Internet Security Policy for Organisations

An exploratory investigation of the use of an Internet security policy to manage the Internet security problem for organisations (1996 – 2000)

A thesis submitted in fulfillment of the requirements for the award of the degree

Doctor of Philosophy

From

Monash University

by Sharman Lichtenstein
B. Sc. (Hons) (First class) (University of Melbourne)
M.Sc (University of Melbourne)

School of Information Management and Systems

The original PhD thesis which was passed at examination identified the companies studied in the research project. This version of the thesis has been modified from the original, for public release.

Please cite as:

Lichtenstein, S. (2001) *Internet security policy for organisations*, PhD thesis (public version), Monash University, Melbourne, Australia.

This thesis is dedicated to my late mother and father:

Eugenia Blashki
Arnold Roy Blashki, MBE

Table of Contents

Abstract

Companies now routinely use the Internet for performing business activities. Accidental and deliberate misuse and abuse of the Internet by internal employees as well as external parties, combined with a notoriously vulnerable global Internet infrastructure and a lack of Internet regulation, has seen the emergence of an Internet security problem for organisations. In this thesis, I explore this problem, and its management via an organisational Internet security policy.

As the best managerial solutions for all forms of information security have been shown to be holistic ones, I have constructed an holistic framework to guide the handling of factors, development and content in Internet security policy for organisations—in particular, for businesses. In order to achieve this, I have brought together a number of different topic areas—electronic commerce, Internet risks for organisations, Internet security management within organisations, and the highly sensitive human issues associated with Internet usage and policy-setting.

This Thesis is structured into five sub-projects comprising the research programme:

(i) *Theoretical Analysis* is concerned with theory-building. It explores the theoretical aspects of Internet security policy by identifying and drawing together the many and varied holistic factors which influence the policy. It develops an initial framework for Internet security policy, composed of sub-models for the factors, development and content of the policy.

(ii) *Preliminary Analysis* explores influential factors and elements in Internet security policy in order to gain indicative support for the proposed framework. It achieves this via two mini case studies.

(iii) *In-Depth Analysis* complements the Preliminary Analysis by providing the detailed empirical understanding necessary to consolidate the proposed framework. It achieves this via four detailed case studies.

(iv) *Theory Validation* tests the proposed framework by drawing on the interactions between interested parties brought together in a focus group to discuss the framework and its usefulness. A revised framework is then presented.

(v) *Conclusion* sums up the findings, draws conclusions, and suggests future research.

The results of this research project highlight a serious Internet security problem for Australian businesses, and suggest that a similar situation exists outside Australia. The research suggests that Internet security policies for organisations are a much needed and potentially useful managerial measure for controlling the growing problem of Internet security, but that there are many complex and sometimes controversial issues to be handled in setting an effective policy. This research clearly provides a sound starting point, via the framework presented, for companies wishing to develop and implement effective organisational Internet security policies.

Declaration

This thesis is submitted in accordance with the regulations of Monash University in partial fulfillment of the requirements for the award of a Doctor of Philosophy. It does not incorporate any material previously published or written by another person except where due reference is made in the text. The work described in this thesis is original work and has not been previously submitted for a degree or diploma in any university.

Sharman Lichtenstein
June, 2000

Acknowledgments

First and foremost, I would like to thank my supervisor, Professor Paula Swatman, for her unswerving faith in my ability to complete this PhD research. Her loyalty, commitment, faith, friendship and support, over the past four years of trials, tribulations and hard work, have been truly remarkable. Her advice and direction in my research effort and topic have been invaluable throughout the project, and I cannot thank her enough.

Many other people have contributed to my research project: The Head of the School of Informations Management and Systems, Professor David Arnott, for supporting my research activities, providing advice, granting study leave to write most of this thesis, and being understanding during my lean times; the four anonymous case study organisations and their personnel (who must also remain anonymous here for confidentiality reasons) who kindly granted me time for the case interviews; the five focus group participants (who also chose to remain anonymous) and the focus group moderator, Dr Craig Parker, all of whom kindly spent several hours one evening evaluating my research; the many students who participated in the preliminary case research; the experts who contributed via research discussions and reviews: Dr Frada Burstein, Dr Jussi Leiwo, Dr Michael Bloch, Judge Don Smalley, Dr Mark Newsome, Professor Michael Bieber, Dr Gerhard Wittig, Andrew Kotulic, Dr Danni Fowler, Dr Simpson Poon, Professor Kai Rannenberg, many unknown referees, journal editors Kevin Fitzgerald, Professor Rob Kling, Paul Spencer, Professor Eleanor Wynn, Professor David Schwartz, and John Meyer; HICSS 97 conference organizers Professor Bill Blanning and Mr Dave King; Sergeant Steve Schmidt of the Australian Defence Force, who granted me an interview; research students Kelvin Ho, Mark Richmond and Steve Mellor, for contributing their opinions on related topics; Rob Lewis, for his model-presentation expertise; and many others too numerous to mention.

There are some special people in my life who have encouraged and supported my research efforts over these last four years: my Cheers pals Mary Sahs, LaRose Karr, Joe Griggs, Shelley Volk, Marcia Sacks, Sally Larwood, Mike Whitney, Dick Wood, Kat Grandy, Linda Allison, Pat Mangum, Glenda Kay White, Chris White, Sally Larwood, Brad Thomson, Peter Macinnis; Internet buddies George and Cynthia Naanes, Dr Tom Zebovitz, Jeff Ratzlaff (dec); academic colleagues Dr Doug Hamilton, Professor Don Schauder and Carey Butler; my brother and sister-in-law, Adrian and Bonnie Blashki; cousins Eda and Geoff Slonim; and last but not least, Jon Paul Gauthier for his love and belief in me.

A special thanks to those loved ones who have kept my flame of hope for this research alive: my two adored daughters, Jasmine and Ilana, my mother Eugenie Blashki, and my deceased father, Arnold Blashki, MBE, who would have dearly loved to have seen this work completed, and to whom this thesis is dedicated.

List of Figures

List of Tables

Chapter 1
Introduction

"Ah, but a man's reach should exceed his grasp. Or what's a heaven for?"

(Robert Browning)

As we enter the new millennium, the Internet has emerged as a key business technology, enabling a myriad of exciting business opportunities. However, the Internet has also brought with it a host of serious concerns for businesses, most notably—an Internet security problem. When I commenced this research project four years ago, I recognized that organisations were not taking adequate steps to manage their Internet security problem. This realisation eventually impelled me to explore the use of an *organisational Internet security policy* as a critical managerial remedy.

This thesis aims to assist businesses in managing their Internet security problem, through providing guidance in the production of an effective organisational Internet security policy. I construct and test a framework to guide the development, content and issues in Internet security policy for commercial organisations, building the framework on a foundation composed of a number of different topic areas—electronic commerce and its reliance upon the Internet, Internet risks for organisations, Internet security management and information security management within organisations, and the highly sensitive human issues associated with Internet usage and policy-setting in business.

In this opening Chapter, I describe the background to the project (see Figure 1-1, which clarifies the issues involved) by examining how the enthusiastic uptake of the Internet globally by businesses has led to an Internet security problem for business, and the need for organisational solutions. I then introduce the research problem for this project. At the Chapter's end, I outline the remainder of the thesis.

1.1 Background to the project

1.1.1 Introduction to the Internet

In the 1970's, the Internet—a technological tool which has since become part of many people's everyday lives—appeared on the global scene. Because it enabled ready global access to people, data, software, documents and multimedia, the Internet's potential was swiftly recognised by organisations and individuals throughout the world, and now it is difficult to imagine life without it. What precisely is the Internet? The Internet is a global network, comprising regional, private, government, business and education networks—employed for conducting business, sharing and managing information, research, communication and collaboration, and access to applications (Forcht *et al*., 1997; Mathieu and Woodard, 1995; Zwass, 1999). Global uptake of the Internet has been dramatic, with some 200 million people using the World Wide Web (the Web) at the commencement of this millennium (Zakon, 2000).

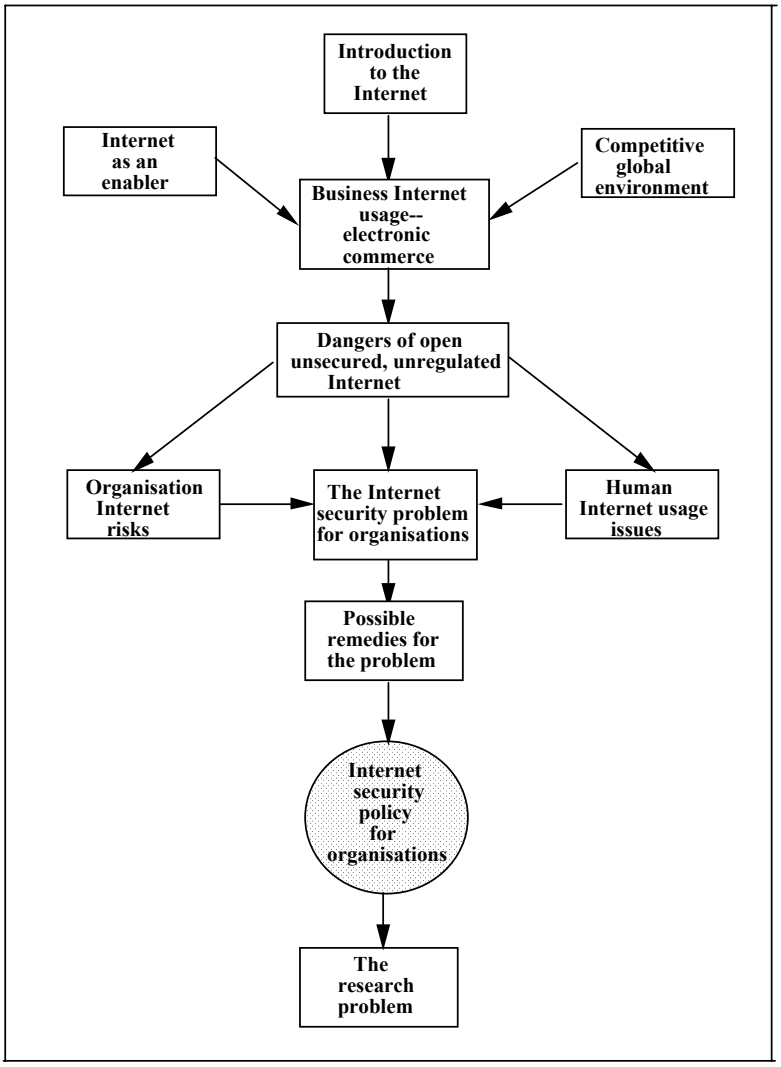

Figure 1-1 A schematic representation of the background to this project - and introducing the research problem

Although the Internet is unlikely to be the ultimate model or technology for future national or global infrastructures, current usage statistics and forecasts suggest that the Internet represents a significant stage in the evolution of future infrastructures, and is hence an excellent focus for research.

1.1.2 Business usage of the Internet

1.1.2.1 Introduction to electronic commerce

Today, businesses face a highly competitive global business environment in which it is increasingly difficult to obtain a strategic advantage. Information technology (IT) can be employed to secure this advantage (Boar, 1994; Blili and Raymond, 1993; King *et al*., 1988; Porter and Millar, 1985), with the

Internet being an important example, improving the speed, accessibility and timeliness of information and communications (Fink *et al*., 1997; Poon and Swatman, 1995; Prakash, 1996).

A major reason why the Internet has been so readily adopted by businesses is the power of the Web. Together, the Internet and the Web have enabled electronic commerce—*e-commerce*—as an accepted mode of business operation (Kalakota and Whinston, 1996; Zwass, 1999).

"The Internet has become the driver for E-commerce thanks to the invention of the World Wide Web as a principal means of sharing information. The Web has turned the Internet into a global, distributed, and hyperlinked multimedia database."[1]
(Zwass, 1996)

There are a plethora of definitions for e-commerce in the literature. For example:

"E-commerce is the sharing of business information, maintaining business relationships, and conducting business transactions by means of telecommunications networks."
(Zwass, 1999)

Another definition of e-commerce is aimed at two objectives:
"*the use of information and communication technologies to network economic activities and processes in order to*
(i) reduce information-related transaction costs or
(ii) gain a strategic information advantage"
(Garcia, 1997, p. 18)
The Internet can reduce transaction costs by enabling speedy and ready access to information and people resources globally, and can provide a strategic information advantage by enabling

"design and deliberate strategic deployment of linkages and networks among cooperating firms intended to achieve joint, strategic goals to gain competitive advantage."
(Wigand, 1997, p. 3)

---

[1] I point out to the reader that unless a phrase followed by a reference is enclosed by quotation marks, the phrase is my own paraphrasing of the work of the author, and not a direct quote. Hence, in this case the phrase is a direct quote.

1.1.2.2 Business use of the Internet

Businesses have aimed for both the above objectives, employing the Internet for promotion, sales, improved customer service and the creation of alliances and networks (Baskerville and Smithson, 1995; Feher and Towell, 1997; Nouwens and Bouwman, 1995; Poon and Swatman, 1995; Timmers, 1998; Zwass, 1996; 1999).

There are many signs of the acceptance of e-commerce into global business life:

The major software and computer companies—including Microsoft Corp., Netscape Communications Corp., Cisco Systems Inc. and Intel Corp.—have focused on Internet-based products to enable e-commerce, while international and national bodies have been heavily involved in its promotion and regulation (for example, OECD, 1997; 1999; EC, 1997; The White House, 1999; UNCITRAL, 1996).

Businesses have reported successful e-commerce endeavours, and experts are predicting increased online trade. Indeed, the White House (1999) estimates that the total value of goods and services traded over the Internet by 2003 will be in excess of $1.4 trillion. Although business-to-consumer e-commerce has been the major e-commerce focus to date, business-to-business (B2B) e-commerce is now regarded as an important and fast-growing segment (Gartner Group, 2000).

Interestingly, recent evidence indicates Internet users increasingly prefer online purchasing to traditional shopping methods. For example, Carvajal (2000) reported a US-based Andersen Consulting survey revealing that 47% of book purchases by Internet users were purchased online, compared with purchases via stores (37%) and catalogues (16%). (Note that the survey did not poll non-Internet users.) The online purchase picture is not all glowing, however, with some 40% of the 500-plus respondents complaining of their Internet shopping experiences, citing out-of-stock items, difficult-to-navigate sites and assorted problems. Indeed, nine out of ten shoppers abandoned Internet shopping trolleys before completing their purchases, suggesting there is room for improvement in e-commerce web sites.

On the Australian e-commerce scene, there has been a dramatic increase in activity in recent times. Australian online retail spending in 1999 amounted to over $920 million, compared with only $250 million in 1998 (www.consult, 2000). Some 3.8 million Australian online purchasers are expected by the end of 2000, representing a significant 20% of the Australian market (www.consult, 2000). There were more than 54,000 commercial Australian Web sites by mid-1998 (Cochrane, 1998), representing 6% of Australian businesses—with a further 16% planning to establish a Web site over the following twelve months, according to the Australian Bureau of Statistics (ABS, 1999).

There are many successful Australian e-commerce endeavours, such as the Melbourne-based boots and leather goods retailer, The Stitching Horse Bootery, which sells world-renown R M Williams boots. This

merchant is making significant profits from its customer-service-oriented Web site, garnering many overseas sales and satisfied customers. Another success story is Lovittools, a Melbourne-based tools manufacturer profiting remarkably well from Web sales, with one Asian hit in 1997 producing sales in excess of $2 million. Online department stores are now beginning to appear, for example the highly successful dstore (http://www.dstore.com.au).

1.1.2.3 Justifying the Internet investment

Looking back, it is hardly surprising that the initial, tumultuous period of Internet use was characterised by an optimistic rush to "seize the opportunity", accompanied by little, if any, planning. However, since the need to assure increased business value from information technology (IT) investments was recognized (for example, an Australian survey of major IT management concerns in 1992 highlighted its importance (Broadbent *et al*., 1995)), we can no longer expect companies to blindly embrace the Internet without first justifying the proposed investment (Bernstein *et al*., 1996; Senn, 1996). Senn has suggested that an *Internet business case* should identify points of success—for example, potential customer contacts—and answer two key questions: "What will the company gain?" and "How will success be measured?"

Experts have attempted to identify and categorize value-adding business uses of the Internet (for example, Bloch *et al*., 1996; Cockburn and Wilson, 1996; Cronin *et al*., 1994; Feher and Towell, 1997; Hoffman *et al*., 1995; Lawrence *et al*., 1996; Poon and Swatman, 1995; Timmers, 1998; Vadapalli and Ramamurthy, 1997; Wigand, 1997). These articulated benefits could be useful in the preparation of Internet business cases, although they must, of course, be pitted against Internet costs, including setup, operational, and recovery costs from security incidents and disasters.

1.1.2.4 Estimating the business value of the Internet

Nonetheless, companies putting forward Internet business cases are finding it difficult to estimate anticipated gains in business value, as:

- existing e-commerce applications have emerged relatively recently, and therefore cannot provide reliable figures,
- online buying patterns are still fairly fluid (Tedeschi, 2000), and
- limited empirical research in this area has been conducted to date.

Furthermore, a veritable minefield for businesses when using available figures is the inconsistent terminology that dominates the area, with terms such as *Internet commerce* and *e-business* having crept into the vocabulary. A salient example of the reigning confusion is the plethora of definitions in existence for the term *e-commerce*. For this very reason, the U.S. Census Bureau has produced a set of definitions

in preparation for the collection of more accurate electronic commerce data from businesses (Mesenbourg, 1999).

Experts have attempted to assist businesses in assessing e-commerce business value by developing methodologies for this purpose (for example, Van Heck and van Bon, 1997), but these have not yet been proven to produce reliable results (hardly surprising, given the abovementioned problems).

Interestingly, some experts have claimed that anticipated e-commerce business value is not being realised (for example, Loveman, 1994). One contribution to unrealised business value may be a lack of rigorous Internet planning and management, leading to ineffective Internet use and reduced benefits.

1.1.2.5 Lack of Internet planning guidelines

Due to the speed of Internet diffusion globally, there has been until recently a dearth of Internet planning guidelines for organisations. Emerging guidelines, to which I have contributed via several publications associated with this research project, now recommend (*inter alia*):

- the preparation of a business case for Internet connectivity;
- the development of an Internet strategy which directs usage towards the alignment of business processes with business objectives;
- the development of policies to underpin Internet management; and
- an overall Internet security management programme

(Bernstein *et al*., 1996; Bloch *et al*., 1996; Brockway, 1996; Cronin *et al*., 1994; Giglio, 1998; Guttman and Bagwill, 1997; Lawrence *et al*., 1996; Lichtenstein, 1996a; Lichtenstein and Swatman, 1997a; 1997b; Logan and Logan, 1996; Miers and Hutton, 1996; Poon and Swatman, 1995; 1996; Segev *et al*., 1998; Quelch and Klein, 1996).
Use of such guidelines may well lead to significant gains in e-commerce business value.

Due to the already-substantial investment in the Internet, the positive statistics in its favour to date, and the enthusiasm shown for it by organisations and individuals around the world, it appears that e-commerce is here to stay.

Unfortunately, not all Internet news is good news. As Forcht *et al*. (1997) cautioned:

"The Internet is both a valuable resource and a potential liability."
(Forcht *et al*., 1997, p. 27)

1.1.3 The dangers of an open, unsecured and unregulated Internet

1.1.3.1 Costs of an anarchic and chaotic Internet

Companies using the Internet for e-commerce have had to face the fact that they are dealing with a medium not originally designed for business purposes. The traditional role of the Internet as an open medium for free, uncensored communication and the exchange of information (Berman and Weitzner, 1997) does not suit companies, which expect a regulated business environment (Spar and Bussgang, 1996). Zwass (1996) pointed to the Internet's "absence of centralised control and consequent organic growth combined with limited security, reliability and bandwidth". Schwartau (1996) labelled the Internet "anarchic and chaotic".

The Internet has always exhibited security flaws. As an evolving tool, its dynamic state continues to open up ever-more security vulnerabilities—hardly an environment conducive to the conduct of e-commerce, characterised by financial transactions and other sensitive business negotiations. The open and unsecured state of the Internet infrastructure has led to significant business concerns, as I discuss in the following section.

1.1.3.2 Business concerns about the Internet

Difficult questions are being asked of the Internet infrastructure by companies, in an attempt to shape the Internet to suit their needs as well as reduce costs. (These questions are also, as it happens, being asked by other sectors of the community for other, equally important reasons.)

- Internet content is sometimes of a dubious nature—should such material be freely available to all and sundry, or should Internet authorities and recognized groups provide content regulation?
- Some people communicate messages widely regarded as offensive across mailing lists—should these messages be allowed through, or can the infrastructure withhold or modify them?
- Many Web sites are collecting personal information about site visitors for unspecified purposes—should this be permitted, or can sites be forced by the infrastructure to specify intended uses?
- Credit card details are being requested across the Internet—are such data safe from the prying eyes of people for whom they were not intended?
- What are the guarantees on the confidentiality, integrity, authenticity. non-repudiation and availability of information sent and received?
- How is it that credit-card details can be retrieved by hackers from corporate databases?
- How is it that major institutions (for example, the Pentagon, reported in Neumann, 1998a) and major Web sites (for example, Yahoo!, Buy.com, eBay and Etrade, reported in Ross, 2000) are being hacked relentlessly?
- Which country's laws are relevant when using the Internet?

These and other equally serious concerns have led companies to question the openness and lack of security inherent in Internet usage, and to seek changes and solutions. One panacea companies have clung to is the prospect of national and international regulations, typically in the form of laws. I discuss Internet regulation in the next section.

Internet regulation is a very important and large topic area in its own right. Therefore, in the interests of keeping this thesis to a manageable size, I will only be providing an overview of the area.

1.1.3.3 Regulation of the Internet infrastructure

The Internet organisational structure is a loosely coupled coalition of organisations and activities, lacking a central management structure and possessing rules and protocols for connection to its backbone communication system and for communicating via the network. However, for the remainder of the Internet community, there is a noticeable shortage of regulation.

Various national Internet laws are already in existence worldwide, as the following examples illustrate. In the UK there are the Electronic Communications Bill and the Data Protection Act 1998 (Baker & McKenzie, 1999), in China and Singapore there are various Internet laws (Davis, 1998), while in the U.S. there are the Communications Decency Act 1995 and the Children's Internet Protection Act 1999 (both of which constitute controversial content regulation).

Interestingly, controversy has accompanied many Internet regulation attempts, highlighting various sensitive issues associated with Internet usage. For example, an American working party released a report in March, 2000, recommending changes to existing laws in order to enable effective tracking of cyber criminals (U.S. Department of Justice, 2000). The prospect of law enforcement agencies tracking people on the Internet is a thorny issue in the U.S. Hence, the report has outraged many Americans.

The Australian regulatory situation is of particular interest in this research project. An initial Senate Select Committee report on Internet issues focused on regulatory issues (Sinclair, 1996a). In September, 1997, the Australian Federal Government established a committee to continue to investigate the impact of the Internet, after the previous committee recommended controversial regulations (Sinclair, 1997b). The Australian Competition and Consumer Commission then proposed measures for dealing with the risks of e-commerce, in response to a dramatic increase in complaints involving transjurisdictional issues (ACCC, 1997).

In 1998, Ministers supported a proposal for an Australian model law based on that of the UN (UNCITRAL, 1996), for the facilitation of e-commerce (Williams, 1998). The resulting Electronic Transactions Bill (discussed in Chapter 3) was approved by the Australian Parliament in November, 1999

(AGD, 1999a). A private sector Privacy Act is about to be legislated (AGD, 1999b; Williams, 2000), while a contentious content regulation law involving the reporting of offensive sites—the Broadcasting Services Amendment (Online Services) Act 1999—came into force in early 2000 (AGD, 1999c). Australian dissidents have been baiting authorities by reporting numerous sites, in order to prove the impracticality of the law.

International bodies have also been active in developing regulations, examples being the United Nations model law (UNCITRAL, 1996) and the OECD guidelines for consumer protection in e-commerce (OECD, 1999).

National regulations for Internet service providers (ISP) have been suggested (for example, TechMedia, 1997; Mitton, 1997a). International ISP regulation could be problematic, as illustrated by Westphal and Towell's (1998) survey of 510 ISPs in 40 countries, the results of which indicated that with so much cultural diversity in the world, ISP regulation would be difficult to implement.

Other regulatory solutions have been proposed. Von Solms (1997) suggested companies be certified as satisfactorily adhering to global Internet regulations. A business would then only permit adequately certified companies to connect to its networks and engage in e-commerce. Davis (1998) pointed out that the Internet effectively operates only according to the laws of the country with the least level of regulation, as the material and activities of that country cannot be controlled by the other countries involved. Von Solms' suggestion above would counter this limitation.

As I have indicated in this section, there is progress world-wide in regulation for the Internet infrastructure. However the business concerns about the Internet, expressed in Section 1.1.3.2, are still pressing. These concerns highlight the Internet security problem for organisations, which I elaborate on in the next section.

1.1.4 The Internet security problem for organisations

Although companies undoubtedly wish to encourage e-commerce and open access across the Internet, they also need to protect their information resources, corporate images, the rights and needs of their internal Internet users, and the interests of external parties. Companies also need to remain law-abiding, and avoid liability in their Internet usage. Hence, companies seek a high level of Internet security. *Internet security for an organisation* can be defined as:

"the protection of the confidentiality, integrity and availability of the organisation's information resources, and the protection of the organisation's image, reputation, finance and viability, from accidental misuse or deliberate attack via Internet connectivity."
(Lichtenstein and Swatman, 1997b)

Escalating Internet vulnerabilities and risks, a lack of guidance in Internet use, and the paucity of regulations at levels ranging from organisational through to global, have led to a serious Internet security problem for organisations—one which is not going to disappear in the foreseeable future.

Neumann commented on the future of computer network security (which is strongly linked to Internet security):

"New information security vulnerabilities are being introduced with each new system released. As a result, supposedly secure systems are penetrable. The risks are still ubiquitous, and are likely to remain so. Anyone who tells you they can develop an infrastructure that avoids or contains the risks is simply not familiar with the realities of computer-communication system security and the foibles of real human beings."
(Neumann, 1997a)

Since its beginnings in the 1970's, the Internet has exhibited multifarious vulnerabilities—in its underlying communications network and nodes, Internet protocols, network administration and host systems (Bhimani, 1996; Doddrell, 1995; Ford and Baum, 1997; Garfinkel and Spafford, 1997; Ghosh, 1998; Nemzow, 1999). Hackers, competitors, disgruntled employees and ex-employees continue to exploit and attack the Internet's ever-changing vulnerabilities, resulting in damage, disruption and uncertainty—a sad indication of the changed nature of the Internet environment from collegial and trustworthy to competitive and hostile (Doddrell, 1995; Neumann, 1996).

Neumann highlighted the vulnerability of the Internet for critical applications, when commenting on the U.S. National Information Infrastructure (NII) (which is based on the Internet):

"The infrastructure may be good enough for low-risk applications, but it is not good enough for high-risk applications such as protection of sensitive corporate and national data, preservation of privacy, large-scale financial transactions over the Internet, and life-critical systems."
(Neumann, 1996b)
In order to highlight the severity of the Internet security problem for organisations, in Sections 1.1.4.1 – 1.1.4.5 I examine: Internet attacks and their impact on e-commerce, internal Internet misuse and abuse, and the need to maximise Internet benefits while minimising security risk.

1.1.4.1 Internet attacks

The increasing vulnerability of the Internet infrastructure to attack from the outside is well recognised. It has been a key finding in surveys of computer crime and security issues in organisations (see, for example, Cockburn and Wilson, 1996; CSI, 2000; 1999a; 1999b; Dinnie, 1999; Ernst & Young, 1996;

NCC, 1996). In a CSI/FBI survey of computer crime and security issues in American companies, 59% of the over-600 respondents reported the Internet as a source of frequent attack over the previous twelve months (CSI, 2000). Disturbingly, Internet attacks had risen steadily over the previous four years.

Recent, well-publicised Internet incidents have raised public awareness regarding the vulnerability of the Internet to attack. Distributed denial-of-service attacks occurred at Yahoo!, Buy.com, eBay and E*Trade Web sites in February, 2000, serving as a warning of impending high-impact attacks (Pethia *et al*., 2000; Reuters, 2000; Ross, 2000). The penetration of major U.S. institutions, including the Department of Defense, NASA, the Pentagon, CIA, Rome Laboratories and Citibank, has highlighted the seriousness of the hacking threat (Branigin, 1991; Denning and Denning, 1998; GAO, 1996; Mitton, 1997b; Neumann, 1996a; 1997a; 1998a). Horrendous virus incidents such as the recent Love Bug virus, which hit some 45 million users and caused an estimated $4 billion in damages (CNN, 2000; The Age, 2000a), and the Melissa virus, which caused an estimated $80 million in damages in 1999 (Kabay, 1999; NYTimes, 1999), are increasingly prevalent, damaging and difficult to control. Accounts of Internet credit card fraud abound—for example, the case of Carlos Felipe Salgado Jr, who hacked into company databases to extract details of 100,000 credit card holders, then attempted to sell the information for $260,000 (Cooper, 1997; CSI, 1997b; Mitton, 1997b).

World leaders and authority figures have reacted to the increasing frequency and severity of Internet attacks. U.S. President Clinton met with industry and security experts after the February, 2000, denial-of-service attacks on major Web sites, to express concern over the vulnerability of the U.S. corporations to Internet attacks, as well as seek solutions (Ross, 2000), while U.S. Attorney-General Janet Reno called for a global Internet law enforcement force to detect and track criminal activity (Greene, 2000). Australian Attorney-General Darryl Williams warned companies to protect themselves against the Internet dangers via use of recognized standards, rather than relying solely on Government legislation (Williams, 2000).

Reasons for increasing Internet attacks include: evolving Internet attack technology in an open-source environment, the plethora of Internet-connected systems with weak security, complex software written by ill-trained programmers, inexorable user demand for new software features rather than added safety, inadequate laws internationally, difficulty in apprehending and prosecuting cyber criminals (particularly across jurisdictions), and a lack of broad community action (Pethia *et al*., 2000). Benjamin *et al*. (1998) noted that the use of standard Internet interfaces and protocols has facilitated initial access, whilst the widespread use of standard databases, software and hardware and easily obtainable hacker tools has facilitated the deeper penetration of systems.

Undoubtedly, the onset of e-commerce has also been a factor in the increasing attacks.

1.1.4.2 E-commerce motivation for attacks

With the advent of e-commerce came new motives for Internet attacks, a salient example being Internet espionage—the interception of sensitive corporate data in transit by competitors and criminals, and the hacking of corporate databases (McClearn, 2000). Most of the 500-plus respondents in a survey of U.S. companies' computer security breaches in 1997, perceived corporate competitors to be a likely source of attack, with over 50% of respondents believing that the information sought in recent attacks would be useful to corporate competitors (CSI, 1997a). Furthermore, with vulnerable online purchasing systems and the visible collection and new accessibility of sensitive and often unprotected financial information, Internet fraud has run rampant (Baker, 1999; KPMG Forensic Accounting, 1998). Neumann (2000) estimates current losses from Internet credit-card fraud at around $1 billion per annum.

1.1.4.3 Impact of Internet attacks on the future of e-commerce

Inevitably, there have been ramifications for e-commerce from the well-reported inadequacies of Internet and e-commerce security. 25% of respondents in GVU's 10th WWW User Survey reported an unwillingness to transmit credit card details over the net, while 60% had serious e-commerce security concerns (GVU, 1998). A number of experts have emphasised the need for trust between computers, people and organisations for successful Internet operation and e-commerce (Hoffman *et al*., 1999; Khare and Rifkin, 1997). Such trust is at present unjustified.

Gray (1996) summarised the lack of Internet robustness for e-commerce as: a lack of security, slow response time, high cost of bandwidth and lack of reliability. Bhimani (1996) specified the requirements for a robust e-commerce security solution as an assurance of the confidentiality and integrity of transactions, non-repudiation by involved parties, and parcelling of aspects of individual transactions (for example, the authentication aspect) for added security.

Improved security is a major goal for new e-commerce technologies such as emerging digital payment systems (Gallegos, 1998; Garceau *et al*., 1998). For example, Reichenbach *et al.* (2000) describe a scheme that allows each consumer to uniquely specify his/her security requirements for a digital payment system; the scheme then recommends the digital payment system matching the consumer's security requirements.

Thus far, I have focused on external Internet attacks, in order to highlight the Internet security problem for businesses. However, Internet security issues may also stem from inside a company—as I discuss in the next section.

1.1.4.4 Internal Internet misuse and abuse

Companies have been increasingly alarmed over risks originating from their own, trusted employees (CSI, 2000; Marsan, 2000). Many employees granted connection to the Internet for valid business reasons, have been misusing or abusing the resource, either from a lack of awareness of the Internet's insecurities, a lack of awareness of valid, value-adding business Internet usages, or purely from malicious intent. One of the more notorious company concerns is excessive use of the Internet for non-business purposes, as indicated by recent surveys and news reports.

In CSI's (2000) survey of U.S. computer crime and security, 79% of over 600 responding companies reported employee abuse of Internet privileges (including downloading pornography, pirating software, and inappropriate email use).

Every Internet-connected company is now well-aware of employees spending work time surfing the Internet for personal purposes, exchanging personal email, downloading games, images and non-work-related software, shopping, banking, checking stock prices, using chat groups and corresponding with non-work-related mailing lists. I have reported some early empirical studies in Lichtenstein and Swatman (1997a; 1997b) and Lichtenstein (1998), indicating that these practices are commonplace and problematic.

In a recent survey, one in three workers spent at least 25 minutes in personal Internet use, one in ten workers had observed colleagues accessing adult sites, and one in three workers had observed colleagues confronted for surfing abuse (Marsan, 2000).

There are even Internet risks to the employees themselves, an important example being loss of privacy via company logging and monitoring of email and urls of visited sites, and collection of personal data by external web servers through forms at sites visited and tracking cookies stored on employee computers (Attaran and VanLaar, 1999; EPIC, 1997a; 1997c; 1998a; Miller, 1997; Wang et *al*., 1998; Weisband and Reinig, 1995). Another example is unsolicited (junk) email, which is both a nuisance and time-waster for employees (Erickson, 1996; Marsan, 2000; Pathak, 2000).

1.1.4.5 Maximising Internet benefits

Another concern for companies is that employees may not be using the Internet effectively for business activities, perhaps due to a lack of awareness of its intended business usage, or perhaps due to overly restrictive usage or security. Ineffective Internet business usage, although not regarded as a security problem, nonetheless works against the eventual success of the Internet within the company.

An important objective in Internet usage is to maximise the benefits while minimising restrictivity and risk.

(Hsieh *et al*., 1996)

In the next section, I examine another aspect of the Internet security problem—the human issues it raises.

1.1.5 The Internet security problem for organisations—the human issues

Companies engaged in e-commerce need to concern themselves with the needs, behaviour and actions of their employees in Internet usage and security (as well as the security-related needs, behaviour and actions of consumers and other parties with whom they interact). Hsieh *et al*. (1996) suggested that individual Internet users be charged with behaving ethically and responsibly in Internet usage. Constraining and monitoring Internet use, in order to assure responsible employee behaviour, is regarded by many as an infringement of personal Internet rights and freedoms. Benjamin *et al*. (1998) noted that security measures adopted by companies must be operationally acceptable to the parties involved in order to promote loyal adherence; hence it is important to find solutions which will be acceptable to employee and employer alike.

Controversial human issues which must be faced by companies attempting to regulate employee Internet usage include the following perceived rights (Lichtenstein, 1996b):

- *employee right to non-business Internet use in the workplace*

Many employees believe they should be free at work to surf the Internet for non-business purposes, subscribe to non-business mailing lists, exchange personal email, and download games, images and software for personal use. The issue is problematic, as the following two instances illustrate. The first case occurred several years ago, when a large, Finnish telecommunications company attempted to disable employee Internet access by its employees due to excessive non-business usage—the employees protested vehemently, and the Internet connection had to be reinstated. In the second example, Asian countries identified concerns about non-business Internet use as a major factor in the decision as to whether or not to adopt the Internet (Tan and Thompson, 1998).

- *the right to freedom of speech*

"the Internet may fairly be regarded as a never-ending worldwide conversation. The government may not, through the CDA (Communications Decency Act) interrupt the conversation. As the most

participatory form of mass speech yet developed, the Internet deserves the highest protection from government intrusion"
(reported from court hearing: ALA vs. U.S. Dept of Justice, Federal court in Philadelphia, U.S., cited in Berman and Weitzner, 1997, p. 83).

Berman and Weitzner (1997) pointed to the uniqueness of the Internet in comparison with other broadcast media such as radio and television, and highlighted its value as a medium for "uncensored free speech, free flow of ideas and democratic discourse". In accordance with this view, many employees believe in their right to freely exchange opinions via the Internet, and may strongly resist any attempt by their company to interfere with this right.

- *the right to freedom of information*

In GVU's 7th WWW User Survey, respondents cited censorship as the main Internet issue (Pitkow and Kehoe, 1997). Internet censorship (although since overtaken by privacy as the number one Internet concern) has remained a high priority ever since. Attempts to filter Internet content via regulation and other means have met with resistance from those who believe that people should be given the opportunity to view freely whatever material is available (Neumann and Weinstein, 1999). Employees may resist attempts by companies to filter access to selected web sites, and/or selected incoming emails.

- *the right to privacy*

"*the right to be left alone—the most comprehensive of rights,*
and the right most valued by a free people"
(Justice Louis Brandeis, Olmstead v. U.S., 1928)

Internet users frequently cite the inadequacy of personal privacy on the Internet as a major concern (Clarke, 1999; EPIC, 1997c; 1998a; 1999; GVU, 1998; Hoffman *et al*., 1999). In GVU's 10th WWW User Survey, over 65% of respondents reported not trusting Web sites collecting so-called demographic information to use that information fairly, while over 71% called for new Internet privacy laws (GVU, 1998). Indeed, companies are often reluctant to post Web privacy statements that explain their collection and use of site-visitor information. The privacy issue is critical to e-commerce success (Hoffman *et al*., 1999).

Many people believe in their right to private Internet communications and accesses, while maintaining a level of anonymity. An opposing viewpoint focuses on those people who use anonymous net communication facilities (eg anonymous email) to avoid accountability in their net behaviour. Companies usually insist on a level of employee accountability in their Internet communications, which may supercede privacy rights.

Indeed, it is obvious from considering the various human issues discussed above, that there are many controversial and conflicting Internet security requirements for the different parties involved in e-commerce. As an example of a promising partial solution, experts in the area have developed a security concept called *multilateral security*, which takes into account the different security requirements of all the different security stakeholders in open communication systems, by allowing each user to define his/her own security requirements (Müller and Rannenberg, 1999a; 1999b; Rannenberg *et al*., 1999; Reichenbach *et al.,* 1997).

1.2 The Internet security problem for organisations—some organisational remedies

Thus far, I have described the diffusion of the Internet into business, and highlighted the dangers of the open, unsecured, and unregulated Internet infrastructure for businesses engaged in e-commerce. In particular, I have identified the existence of an Internet security problem for organisations, who face attacks through their Internet connection from the hostile outside world, as well as misuse and abuse from their own, trusted employees. I have pointed out how sensitive some of the human issues are in Internet security, and the necessity for addressing these issues in any solutions.

The Internet security problem has been earmarked for serious attention:

"The security concern is perhaps the most serious obstacle to consumer-oriented E-commerce."
(Zwass, 1996)

"one of the major inhibitors for e-commerce on the Internet is security and privacy issues"
(Mehta, 2000, p. 32)

Experts around the world are constantly working on improving the security of the Internet infrastructure, with plans for international and national regulations (as overviewed in Section 1.1.3.3), platforms, secure digital payment systems, improved encryption and other technical mechanisms. However, this does not excuse an organisation from taking its own steps to protect itself.

Whatever various groups and individuals may decide to do towards creating solutions in the future, it is never too soon for each organisation to take individual responsibility for protecting itself and its employees from the dangers of an open, unsecured and unregulated Internet.

Hence, this relatively new Internet security problem for organisations demands *organisational solutions*, in the form of:

- *Internet security philosophies, methodologies and guidelines* (see, for example, Bernstein *et al*., 1996; Garfinkel and Spafford, 1997; Kyas, 1997; Lichtenstein, 1996c; 1997a; Müller and Rannenberg, 1999a; 1999b; Nemzow, 1999; NIST, 1996a; Pethia *et al*., 2000; Rannenberg *et al*., 1999; Wood, 1997b);

- *managerial measures* such as organisational security policies, procedures and audits (see, for example, Bernstein *et al*., 1996; Gaskin, 1998; Gassman, 1998; Guttman and Bagwill, 1997; Heard, 1996; Lichtenstein, 1996a; 1997a; 1998; Lichtenstein and Swatman, 1997a; 1997b; Overly, 1999; Pethia *et al*., 1991);

- *Internet security tools and technologies*, including emerging fundamental protocols such as IPSec; firewalls, digital certificates, digital signatures, PKI, digital payment systems, privacy seals and trustmarks, emerging platforms (eg PICS, P3P), intrusion detection systems (IDS) and security management technology (see, for example, Denning, 1996; Edwards, 1996; Ghosh, 1998; Kyas, 1997; Reichenbach *et al*., 2000; Sutterfield and Schell, 1997; SRI, 1997; Wack and Carnahan, 1995);

- *Internet security assurance organisations*, such as TRUSTe (Benassi, 1999; TRUSTe, 2000) and Verisign.

The number of Internet security incidents occurring worldwide, despite the availability and deployment within businesses of highly touted Internet security technologies, suggests that improvements in managerial Internet security measures are needed. This observation goes hand in hand with reports highlighting the need for improvements in organisational information security management—see, for example, GAO (1998). Where the Internet is deployed for e-commerce, the META Group (1999) noted:

"*Companies should not overlook the managerial processes that govern and administer secure EC infrastructure*."

Fennelly (1999) remarked:

"*the biggest security hole in an infrastructure is management*."

Accordingly, a company should develop an Internet security management programme, comprising measures which address organisational Internet risks and other Internet security concerns (Bernstein *et al*., 1996; Lichtenstein, 1996a; 1996c; 1997a; 1998; Lichtenstein and Swatman, 1997a; 1997b). Such measures range from policies and procedures through to technological controls (Doddrell, 1995).

Wood (1995) and many others have stressed that management instructions, such as policies, procedures and standards, are considered critical to providing information security, as they are aimed at controlling the decisive human factor. In particular, the organisational information security policy[2] has long been recognised as underpinning information security management (Bayuk, 1996; Bernstein *et al*., 1996; GAO, 1998; NIST, 1994a; Olson and Abrams, 1995; Olnes, 1994; Warman, 1992; Wood, 1995; 1997a). This policy consists of various types of policies: system-specific, program-specific and issue-specific (Guttman and Bagwill, 1997).

The *Internet security policy* is an issue-specific policy (Guttman and Bagwill, 1997; RiskWatch, 1999) forming the cornerstone of the Internet security management programme (Bernstein *et al*., 1996; Guttman and Bagwill, 1997; Lichtenstein, 1996c; 1997a). Due to limited empirical research in the area of Internet security policy, its newly-recognised importance, and other reasons which I discuss later in this Chapter,

I have chosen to focus on the Internet security policy for an organisation, in this research project.

1.2.1 Internet security policy for an organisation

An *Internet security policy for an organisation* can be defined as:

the medium by which Internet security requirements for the organisation are specified, and the means by which guidance and rules are provided to Internet participants within the business.
(Lichtenstein, 1996c; 1997a)

The policy defines the organisation's Internet security requirements, which are then mapped to secure e-commerce processes and infrastructure, defining new technology requirements and revising security management processes as a result (META Group, 2000). The policy includes a set of Internet usage regulations for the organisation's employees (typically called an *Internet acceptable usage policy*—IAUP).

An *Internet security policy for an organisation* has four main objectives:

- to specify Internet security requirements for the organisation;
- to provide guidance and rules to employees concerning Internet usage issues;
- to protect the company from legal liability in Internet usage; and
- to maximise effective business Internet usage while minimising risk and restrictivity;

[2] The term "security policy" is often used to denote a low-level technical policy composed of sets of rules enforced by the system's technical controls, as well as its management and operational controls (Guttman and Bagwill, 1997). However in this thesis, the term "security policy" denotes its other commonly used meaning: the organisation's overall information security guidelines and decisions.

The importance of such a policy was first remarked as follows:

"there must be a clear statement of the local (Internet) security policy, and this policy must be communicated to the users and other relevant parties. The policy should be on file and available to users at all times, and should be communicated to users as part of providing access to the system."
(Pethia *et al*., 1991)

Nevertheless, many organisations with Internet connection lack an Internet security policy (although many have established Internet acceptable usage policies (IAUP)). Instead, companies have implemented technical security mechanisms such as firewalls as a knee-jerk reaction to the Internet security problem, without first specifying their Internet security requirements via a policy (Beker, 1994).

The importance of the Internet security policy and its sub-policies (particularly the IAUP), in managing the Internet security problem, has recently been recognised (Bernstein *et al*., 1996; Gaskin, 1998; Gassman, 1998; Giglio, 1998; Guttman and Bagwill, 1997; Heard, 1996; Lichtenstein, 1996c; 1997a; McMillan, 1996; Overly, 1999; Wood, 1997b). Indeed, Elron Software's recent Internet usage study revealed that 68% of companies had IAUP's, with around 60% possessing email policies (Marsan, 2000). However, few companies possess encompassing Internet security policies, while existing IAUP's have not been developed from researched sets of guidelines.

1.2.2 The research problem

There are many intriguing questions which need answers in this topic area: What risks do an organisation and its employees face when using the Internet in the workplace, and how can these risks be addressed by an Internet security policy? What consititutes acceptable Internet business usage and unacceptable Internet business usages, and how can we specify these within an Internet security policy? How can the policy promote effective Internet usage? How can the policy protect the company from legal liability? How can the policy address employee rights, freedoms and needs? How can the policy reflect new thinking in information security for modern, adaptive organisations (see, for example, Lichtenstein, 1995a; 1995b; 1996d; 1996e), or the concept of multilateral security, where security requirements for all the parties involved are fulfilled (Müller and Rannenberg, 1999a; 1999b; Rannenberg *et al*., 1999)?

A particularly important question to ask is: Is it possible to develop an *holistic* Internet security policy—one in which organisational, contextual and human issues are given equal consideration to technical issues—in line with current holistic thinking in information security and Internet security (see, for example, Brunnstein, 1997; Hartmann, 1995; Hitchings, 1995; KPMG Forensic Accounting, 1998; Lichtenstein, 1996a; 1996b; 1997a; NIST, 1996b; NRC, 1991; OECD, 1992; Warman, 1992; Williams, 2000; Yngstrom, 1995)? As Neumann (1997a) mandates:

"It is absolutely fundamental that security must be addressed as a systemic problem."

Still more questions present themselves: Can we produce guidelines for the issues and content of an Internet security policy? How does such a policy fit into the organisational infrastructure? How does a company develop such a policy?

To date, very little guidance has been provided for the development, content and factors influencing Internet security policies for organisations, or their key sub-policy, the Internet acceptable usage policy (IAUP) (Bernstein *et al*., 1996; FNC, 1995a; 1995b; FNC, 1996; Gaskin, 1998; Gassman, 1998; Ghosh, 1998; Guttman and Bagwill, 1997; Heard, 1996; IETF, 1991; McMillan, 1996; Lichtenstein, 1996a; 1996b; 1996c; 1997a; 1998; Lichtenstein and Swatman, 1997a; 1997b; Pethia *et al*., 1991; Wood, 1997b). However at this stage, the limited amount of advice available has shortcomings, as will be discussed below—and as one would expect for a topic still in its infancy. This research project is designed to add to the limited body of knowledge in this area.

1.2.3 Research rationale

1.2.3.1 First research rationale

Existing guidelines for Internet security policy for organisations were not developed from empirical evidence (for example, the guidelines of Guttman and Bagwill, 1997), but rather were based on professional expertise which, although not a recognised research method, may yet yield meritorious results. One justification for developing *new* guidelines is the fact that I will be adopting an empirical approach to building and validating guidelines. Hence, my proposed guidelines will make a qualitatively different contribution to those already in existence.

1.2.3.2 Second research rationale

I have critiqued existing Internet security policy guidelines in Chapter 3. This critique illustrates that existing guidelines have some, but not all, of the desired characteristics for guidelines for Internet security policy for organisations. *I suggest that existing guidelines exhibit one or more of the following limitations* (presented in order of most important to least important):

- lack of an holistic perspective to Internet security;
- incomplete or missing coverage of:
  - factors to be considered in policy development;
  - framework for policy development;
  - content outline for policy;
- *ad hoc* and incomplete coverage of Internet risks;

- lack of a risk assessment process for determining significant Internet risks;
- inadequate, nonspecific or missing treatment of important and sensitive human issues in Internet security and usage;
- omission of reference to any corporate Internet strategy, infrastructure, or management programme;
- *ad hoc* specification of acceptable, value-adding Internet usages;
- highly general sub-policies that are never made specific;
- ambiguous sub-policies;
- lack of empirical derivation of the guidelines;
- lack of empirical validation of the effectiveness of the guidelines;
- lack of agreement between the various guidelines.

I am aiming to develop a set of guidelines for Internet security policy which overcomes these limitations, and will therefore constitute an improvement over existing guidelines.

1.2.3.3 Third research rationale

Now that more companies possess selected Internet policies (particularly IAUPs), recent evidence has revealed that the policies developed thus far have been ineffective in managing the risks (Marsan, 2000). This presents a compelling reason for developing improved guidelines for an Internet security policy.

1.3. Project definition

1.3.1 Research question

This thesis describes the investigation of improved organisational management of the Internet security problem through an effective, holistic Internet security policy. The research question on which I have based this project is therefore:

Can an holistic set of guidelines for Internet security policy for organisations be developed?

In order to answer this question effectively, it is necessary to answer the following subsidiary research questions:

1. What are the factors influencing effective Internet security policy for an organisation?

Existing Internet security policies have not been developed from recognised theory, and are typically incomplete. The policies do not take into account the many and varied contributing factors which

influence the area, and this is reflected in their incompleteness. These factors hence need to be established.

2. Is an holistic approach to an Internet security policy more effective than the piecemeal approach adopted to date?

This research project adopts an holistic perspective in line with current thinking in information security, in order to identify a comprehensive set of influential factors whose consideration will result in complete and effective policy.

3. Can a framework be specified for the development, issues and content in effective Internet security policy for organisations?

To date, there have been few (and limited) attempts to offer guidelines for Internet security policy for organisations, none of which have been based on sound research techniques—I have sought to develop such a framework, using established, empirically-based research methods.

1.3.2 Project scope

In this thesis, I report work which focuses on the use of an Internet security policy for managing the Internet security problem for organisations. This project:

- provides an exploratory analysis of the factors which influence effective Internet security policy for organisations;
- analyses current Australian (and limited American) practices in the management of the Internet security problem, focusing on management via an Internet security policy; and
- develops a conceptual framework for the issues, development and content in effective Internet security policy for organisations.

1.3.3 Research constraints

Below, I discuss three limitations to this research project.

- There are many different subtopics included in the overall topic "Internet security policy for organisations", including consideration of various kinds of current and planned information infrastructures (national and international), sensitive human issues in Internet usage such as employee rights and freedoms (including the broad areas of privacy, censorship and intellectual copyright), and a wide range of technical measures such as firewalls and encryption. Clearly, it would be impossible for any one thesis to deal in an adequate manner with all the subtopics involved, as the scope of each is so large. Therefore, in this thesis, while I refer to these subtopics, I

essentially concentrate on the management of the Internet security problem through use of an organisational Internet security policy.

- This research project has almost exclusively involved empirical research conducted within Australia, and therefore has an Australian focus. The results may not therefore be generalisable to other countries, but are, however, *indicative* of the current situation worldwide.

- The research methods used are qualitative and hence not generalisable, although indicative of the current situation. Clearly, further work will be required to confirm the findings of this project, and to ensure that the framework can be applied across all sectors of industry, and internationally.

1.4 Research contribution

This thesis provides an academic analysis of a subject of highly topical interest—the management of the Internet security problem for organisations, and makes a contribution to both theory and practice.

In theoretical terms, the research project:

- adds to knowledge in an emerging research area;
- develops an holistic approach to a hitherto fragmented approach to Internet policy for organisations;
- adds substantively to existing theory in Internet security policy for organisations;
- provides important empirical evidence of the growing seriousness of the Internet security problem for Australian organisations, and the need to manage it via a policy as well as other security measures; and
- identifies issues which will be useful for the development of all kinds of information security policies.

In practical terms, the research project:

- produces guidelines for use by practitioners in the development of an Internet security policy for an organisation;
- provides a framework which could be useful to practitioners for the development of all kinds of information security policies; and
- raises commercial and managerial awareness of the growing importance of the Internet security problem for organisations, and its management via an Internet security policy and associated Internet security management programme.

1.5 Outline of thesis

The thesis is structured into five parts which analyse the area of Internet security policy from a number of complementary perspectives, followed by a conclusion which presents the findings of the research project, and outlines possibilities for further work.

Part I—Theoretical Analysis contains the theoretical foundations upon which the framework for Internet security policy will be based, and is composed of two Chapters:

- Chapter 2 explains the Research Design chosen for this project—analysing the possible methods for the work at hand, and selecting the most appropriate methods.
- Chapter 3 presents a contextual analysis of Internet security policy by identifying and drawing together the various factors which influence the policy, from existing literature, and presents an outline of a three-component framework for Internet security policy for organisations, as well as a model of one of these components—the factors which influence the policy.
- Chapter 4 uses the results of Chapter 3 to construct the two remaining component models for the content and development of the policy, and proposes a final, overall framework for the policy, clearly indicating all three components (factors, content and development) and their respective models.

Part II—Preliminary Analysis analyses two mini case studies to explore influential factors and elements, and compares these with the proposed framework. The two mini case studies focus on the employee perspective of the issues.

- Chapter 5 describes and analyses two mini case studies at Monash University, drawing conclusions for the proposed framework. Monash University was willing for the research results from the cases to be openly published.

Part III—In-Depth Analysis complements Part II by providing the depth of understanding necessary for further exploring the proposed framework through four detailed case studies, and performing a cross-case analysis. *The companies studied chose to remain anonymous for security reasons, and hence, I have used nom de plumes*.

- Chapter 6 describes and analyses a detailed case study of a large Australian medical research establishment: Medical Science Research Institute.
- Chapter 7 describes and analyses a detailed case study of a large Australian travel company: Flyway Australia.
- Chapter 8 describes and analyses a detailed case study of a large Australian retail company: Aus-Retail Ltd.
- Chapter 9 describes and analyses a detailed case study of a large American oil company: USEnergy Petroleum Company.
- Chapter 10 performs a cross-case analysis of the detailed case studies, and presents the findings.

Part IV—Theory Validation tests the proposed framework by drawing on the interactions between interested Australian parties brought together in a focus group to discuss the usefulness of the framework. This part also presents a revised framework.

- Chapter 11 describes and analyses the focus group interactions, and presents the revised framework.

Part V—Conclusion

- Chapter 12 sums up the arguments and findings from the previous work, draws conclusions and implications, and suggests future research directions.

Part I

Theoretical Analysis

Chapter 2
Research methodology

"*The important thing is not to stop questioning*."

(Albert Einstein)

In the previous Chapter, I introduced the research topic—Internet security policy for organisations—and proposed my research question and subsidiary research questions (Section 1.3.1). In this Chapter, I summarise the four research sub-projects which comprise the research programme, and discuss the selection of the most appropriate research methods for the programme.

At this point, I wish to point out that, due to personal reasons, there was a delay of ten months between the conduct of my planned, final piece of research—a focus group, held in June, 1998—and the resumption of this research project in April, 1999. I felt that during this ten month period, the research I had conducted earlier may have lost its currency, and hence decided to add a further piece of research—an additional case study, conducted in May, 1999, to test the continuing relevance of my earlier findings.

This Chapter firstly presents an introduction to information systems research (Section 2.1), then describes the research design (programme) selected for this research, concentrating on illuminating the four individual research sub-projects (Section 2.2). I then discuss alternative research methods for the sub-projects, justify the research methods chosen and overview research procedures (Section 2.3). In Section 2.4, I describe the procedures for research quality assurance. In Section 2.5, I discuss the relevance of the research design for the project's intended audience, and in Section 2.6, I conclude the Chapter.

2.1 Introduction to information systems research

A great deal of work has been carried out in information systems research over the last decade, and a number of interesting research approaches have been proposed (Galliers, 1992; Klein *et al*., 1991a; Lee *et al.*, 1997, Mumford *et al.*, 1985, Orlikowski and Baroudi, 1991).

As information systems is regarded by many as a social science (Galliers, 1992; Klein *et al*., 1991b; Parker *et al*., 1994; Shanks *et al*., 1993), social science research methods may be applicable. Indeed, Bjorn-Anderson (1982) stated:

For better or for worse, it [information systems] must be seen as a social science discipline.

Information systems is typically regarded as an applied discipline (Arnott and Shanks, 1993; Parker *et al*., 1994). Researchers in information systems must therefore contribute to professional practice by providing the necessary new knowledge for improved practice. In this research project, improvements in the management of Internet security for companies—via an Internet security policy—are sought. Empirical research in information security management has been scarce (Baskerville, 1994), and hence the impact of this project's results should be considerable. As my intention is for companies to apply the

developed framework which this project aims to produce (in accordance with recommendations of Benbasat and Zmud, 1999), I must consider research methods which produce results that can be used in practice.

In the following section, I discuss the research design, which I chose after careful consideration (see Section 2.3) for this research project.

2.2 Research design

Galliers (1991) and Neuman (1994) describe a research cycle of three stages: *theory building*, *theory testing* and *theory refinement*. During theory building, exploration of the research domain enables development of a theory (for example, a model or framework). During theory testing, the theory is tested for validity in some way(s). During theory refinement, the original theory is refined in light of the results of theory testing. The last two stages are repeated until the theory is complete and has been fully verified.

Scholarship is a necessary aspect of the first and third stages (Shanks *et al*., 1993), scholarship being the investigation and integration of existing knowledge from relevant domains, with due analysis. The knowledge is obtained via a search of relevant literature and other useful sources such as conferences, seminars, anecdotes, email, Internet mailing lists and discourse with individuals and groups. The aim of such scholarship is to develop insights which can assist in formulating, or refining, a theory.

To set the scene for explaining the research design chosen, I restate below the research question originally stated in Section 1.3.1:

Can an holistic set of guidelines for Internet security policy for organisations be developed?

To answer this question, three subsidiary questions were postulated:

1. What are the factors influencing effective Internet security policy for organisations?

2. Is an holistic approach to an Internet security policy more effective than the piecemeal approach adopted to date?

3. Can a framework be specified for the development, issues and content in effective Internet security policy for organisations?

The *research design* for this project was adapted from the research cycle described above. It is illustrated in Figure 2-1 and discussed below.

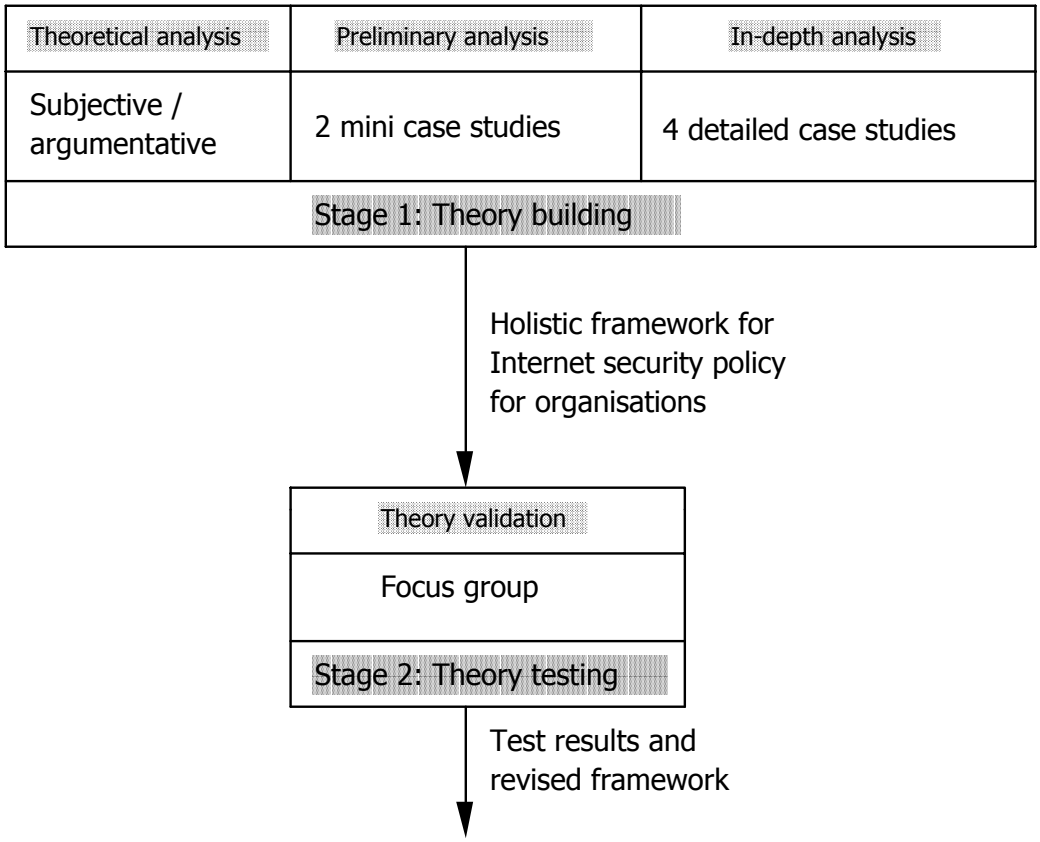

Figure 2-1 Research design

In this research design, the research project is composed of *four sub-projects*:

Stage 1: Theory building

(i) Theoretical analysis: primarily concerned with exploring the topic using the *subjective / argumentative research method* (Galliers, 1992): exploration of various domains within existing literature, attendance at conferences and seminars, presentations at conferences and seminars, anecdotal evidence, email and Internet mailing lists, Web site materials and discourse with groups and individuals, in order to build an initial holistic framework for Internet security policy in organisations;

(ii) Preliminary analysis: concerned with further exploration of the topic through *two mini case studies*, in order to provide early support for the initial framework; and

(iii) In-depth analysis: concerned with further, detailed exploration and description of the topic through *four detailed case studies*, in order to consolidate the framework through providing much-needed depth.

The main domains explored during Stage 1 are: information security, information management, Internet usage, e-commerce, Internet security and information technology.

Stage 2: **Theory testing**

(iv)*Theory validation:* the framework is tested via a *focus group*, and the knowledge thus gained is analysed and used to revise the proposed framework.

2.3 Selection of research methods

In this section, I justify the choice of research methods for Stage 1 and Stage 2, already previewed in the previous section (and shown in Figure 2-1).

2.3.1 Quantitative and qualitative research methods

All information systems research methods can be categorised as quantitative or qualitative (Myers, 1997).

Quantitative research methods use standardised measures so that various perspectives and human experiences can be slotted into prespecified categories, while qualitative research methods permit the study of selected issues in depth without the restrictions of predetermined categories of analysis (Galliers, 1992).

Klein *et al*. (1991a) point out the benefits of each approach. The advantage of quantitative research is that it is possible to obtain and present broad generalised results concisely. The measuring instrument is of prime importance (for example, a survey questionnaire). The advantage of qualitative research is that it produces a rich picture—in-depth, detailed, information—about a smaller set of situations, thus increasing understanding but limiting generalisability. The researcher him/herself is the instrument of measurement.

As Internet security policy is a relatively new research area, there are no agreed-upon, predetermined variables to measure. Therefore related broad issues—such as Internet risks for companies—should be studied in depth, in order to explore this topic.

Hence, I favour qualitative research methods for this research project.

2.3.2 Positivist, interpretivist and critical research approaches

As information systems is a newcomer to the social science scene, research methods for information systems research have, until recently, been selected from those considered appropriate in the past. Chua (1986), and Orlikowski and Baroudi (1991), classified research as positivist, interpretivist, or critical. Myers (1997) suggested that qualitative research can also be positivist, interpretivist or critical.

Positivist research approaches presume an objective physical and social world which exists independently of people—a world whose nature can be measured (Galliers, 1992). These approaches utilise quantitative research methods. Interpretivist approaches assume that reality is a construct of the meaning that people apply to it, and that society cannot be exploited independently of the individuals who contribute to it (Galliers, 1992). Critical research assumes that social reality is constrained by social, cultural and political circumstances, and aims to be emancipatory (Myers, 1997).

Parker *et al*. (1994) noted that although there was a move toward positivist methods in information systems research over the period 1968–1988 (for example, surveys) in information system research, methodologists have argued for an increase in interpretivist methods. According to Jonsson (1991), social reality can only ever be interpreted (as distinct from being objectively analysed). Furthermore, interpretivist research is suited to formative research, such as this relatively new topic area.

As Internet security policy is heavily human-reliant and in its formative stages, I favour the use of interpretivist approaches for this research project.

2.3.3 Exploratory, explanatory and descriptive research methods

Neuman (1994) classifies research methods as *exploratory, explanatory and descriptive*. Exploratory research explores an issue in order to establish a mental picture of what is occurring, and in order to generate ideas and develop theories. Descriptive research presents a narrative profile of the specific details of a situation, thereby inspiring new explanations within a topic area.

Stage 1 of this project is exploratory in that existing literature and other sources are explored as part of scholarship, and aspects of the topic are explored via the two mini case studies and the four large case studies, in order to build a holistic framework of Internet security policy for organisations. *Stage 1 is also descriptive* in that it describes existing Internet influences and existing Internet security policy for organisations via the two mini case studies and the four major case studies, in the process highlighting the need for Internet security policy and comprehensive, holistic guidelines.

2.3.4 Alternative research methods for Stage 1

Stage 1 produces as an outcome the framework specified in the primary research question stated in Section 2.2.

2.3.4.1 Subjective/argumentative

In 1996, when this project commenced, there was a very limited body of literature available concerning Internet usage in companies or its management. In addition, the topic of Internet security was mainly described from a technical viewpoint (for example, information concerning how to build firewalls (Bryan, 1995)). *Most importantly, there was also a lack of academically researched theory on the topic of Internet security policy for organisations.*

Hence, after experiencing some frustration at the lack of existing literature in the topic area, I recognized the need to search within literature for related domains, including information security, information management, Internet usage, electronic commerce, Internet security and information technology, *in order to develop an appropriate intellectual framework from which I could then explore the topic area using empirical research methods.*

I then needed to find out if experts in information systems research supported this approach. I found two key pieces of support:
Firstly,

"when methods [high in data integrity] *are used to investigate research topics about which theoretical development is scant or uncertain, research often is inefficient or misleading. Either the power of deductive methods is under-utilised, or theory and/or method are prematurely pressed into service when their underlying assumptions cannot be met"*
(Bonoma, 1985)

Secondly, Galliers included subjective/argumentative research as a research method in his revised taxonomy of information systems research methods, saying:

[Subjective/argumentative research] "*is included because, in the right hands, this kind of creative process makes a valuable contribution to the building of theories which can subsequently be tested by more formal means. Its strengths lie in the creation of new ideas and insights. Its weaknesses arise from the unstructured, subjective nature of the process"*
(Galliers, 1992)

Hence, I chose the subjective/argumentative research method to develop an initial intellectual framework from which to proceed with further theory building. This method makes heavy use of scholarship (Shanks *et al*., 1993) to source and draw together available knowledge in a number of domains (as indicated above) in order to form a cohesive, comprehensive framework.

Using the subjective/argumentative research method in the area of Internet security required the input of much empirical data reported in various online press publications, which provided many real-life cases of Internet security incidents and associated warnings and remedies.

Hence, the subjective/argumentative research method, as I employed it, was partly empirical in nature.

The fact that the research topic covered a number of varied and complex domains, combined with the difficult and complex intellectual task of constructing an intellectual framework from the information found, meant that the subjective/argumentative sub-project formed a large and significant component of this research project, and is itself a significant contribution to existing theory in this area.

There are additional research methods available for use in Stage 1 (theory-building) which I should consider in order to further explore the topic area and refine the initial framework built from subjective / argumentative research. Three candidate methods are evaluated below, in order to determine the usefulness of each method for Stage 1 of this project. I have considered both quantitative and qualitative methods. The three methods evaluated are: *laboratory experiment, survey and case study.*

2.3.4.2 Laboratory experiment

This *quantitative* research method enables investigation of the causal relationship between controlled variables for alternative exploration (Galliers, 1991) via an experiment conducted using scientific procedures. Variables are measured via quantitative analytical techniques (Shanks *et al*., 1993). Experimental approaches are high quality approaches, but they suffer from several disadvantages: the extent to which results can be generalised to cover real world situations as a result of over-simplification of the experimental situation, and the isolation of such environments from most of the variables that exist in the real world (Neuman, 1994).

Considering that Internet security policy for organisations has many as yet undetermined real world variables affecting it, such as global Internet standards, and national and international laws, it is not possible to completely identify, simulate or simplify realistically the many complex variables. The results that would be obtained from experimentally setting up an Internet-connected environment and simulating an indeterminate set of Internet security risks, in order to determine all the holistic factors

influencing Internet security policy, would certainly lack validity. Furthermore, the resources required to simulate the full range of Internet risks (including viruses, hacking, etc), were not available to this researcher.

Hence, a laboratory experiment was not deemed to be a suitable research method for use in Stage 1.

2.3.4.3 Survey

A survey involves exploring an area by collecting and analysing data from a representative sample of a population (Galliers, 1991; Neuman, 1994, Shanks *et al*., 1993). Analysis of survey data is performed either qualitatively or quantitatively. Surveys can be viewed as "snapshots" of existing practices at a given point in time (Neuman, 1994), and are a very popular *quantitative* information systems research method (Shanks *et al*., 1993).

At the time of commencement of this research project, in 1996, the existing population of Australian companies with significant Internet diffusion and usage was still fairly low (though growing), with most companies either having chosen to commence their foray into Internet usage via an Intranet only (with correspondingly limited application to this research project) *or* with only select, privileged employees (typically managers) being granted Internet access. Hence, a survey would have had limited numbers to sample, as expected for a topic area still in its infancy.

The variables to be measured by a survey for this topic were very hazy in the early years of this project (1996, 1997), and would have needed to be determined. It was important to explore those companies which had, at that stage, more fully embraced the Internet, via in-depth study, in order to uncover these variables.

It also needs to be recognised that each company has been experimenting in these early years of Internet use, and has been basically "doing its own thing". Hence, it would have been very difficult to compare company responses to given survey questions (as they would be likely to be very different).

Hence, I did not choose a survey as an appropriate method for Stage 1.

2.3.4.4 Case study

A case study is used to explore or describe or explain a particular issue within a specified unit of study (Benbasat *et al*., 1987; Shanks *et al*., 1993; Yin, 1994), and is a *qualitative* research method. Walsham (1993) recommends case studies for interpretivist information systems research.

A case study typically requires detailed study of an individual organisation or group of organisations. Data collected are analysed *qualitatively*, yielding a rich picture of what is happening with respect to the issue investigated.

A key aspect of the research question is the concept: *holistic*. Rouse and Dick (1994) state that:

"there is a need for qualitative research techniques to capture holistic real-world answers to real-world problems in a way that is not possible in a quantitative context."

Qualitative research methods for exploratory information systems research (such as the case study research method) are also strongly supported by Cash and Lawrence (1989), Klein *et al*. (1991) and Mumford *et al*. (1985).

Benbasat *et al*. (1987) justify a case study for information systems research in the following three ways.

(i) A case study enables the study of an information system in its natural setting, learning from state-of-the-art practice, and generation of theories from practice.

(ii) A case study enables the answering of "how" and "why" questions. Questions such as "How do national and international laws pertaining to the Internet, influence the Internet security policy for a company?" are critical to determining whether laws are one of the factors influencing policy (see subsidiary research question 1 in Section 2.2).

(iii) A case study is an appropriate method for investigating an as-yet largely unresearched area—which this research area undeniably is.

Aside from the above additional reasons for selecting a case study research method, Bonoma (1995) suggested that case studies are useful where a

"phenomenon is broad and complex, where the existing body of knowledge is insufficient to permit the posing of causal questions, and when a phenomenon cannot be studied outside the context in which it occurs."

This research topic is, indeed, "broad and complex", with many factors (identified in this research project) that may influence the Internet security policy. There is currently limited knowledge in the area, and it is difficult to study the topic without viewing the Internet environment within a given organisation.

Furthermore, Yin (1994) states that case studies are especially useful when the researcher is attempting to answer a "how" or "why" questions over which (s)he has little control. The research question "Can an

holistic set of guidelines for Internet security policy for organisations be developed?" is essentially a "how can?" question, again supporting use of the case study method.

Finally, a case study may capture reality in greater detail, analysing a greater number of variables than is possible with other research methods (Galliers, 1991). It is indeed desirable to identify and study in detail a comprehensive range of factors influencing Internet security policy.

It is appropriate, then, to select the case study research method to explore the research topic and build the initial framework (Stage 1).

2.3.4.5 Multiple case studies or single case study

The next decision to make is whether to use a single case study or multiple case studies.

Benbasat *et al.* (1987) suggested that

"multiple case designs are desirable when the intent of the research is description, theory-building or theory-testing... Multiple case studies allow for cross-case analysis and the extension of theory. Of course, multiple cases yield more general results (than single cases)"

In Stage 1, I am using the case study approach for theory-building, favouring immediately the choice of multiple cases. Furthermore, with such different approaches to Internet adoption and usage within different companies in these early days of the Internet, several cases are required in order to gather sufficiently broad-ranging, cross-industry data to generalise in order to develop a theory at all. Cross-case analysis is also obviously desirable to highlight any trends, patterns or differences, which should be represented in the theory. Hence, according to Benbasat *et al.*'s (1987) advice (cited above), 'multiple cases' appears to be a better choice than 'single case'.

A few additional words on this choice are in order. Given that I have chosen not to conduct a survey, one analysis alone would not give sufficiently broad coverage of the current scene and needs in this topic area. A single case in this relatively young area may (in fact, would almost certainly) yield highly biased and unrepresentative results—Galliers (1992) warned of the difficulty in generalising from a single case study. Therefore, it seems wisest in this project to choose multiple cases over a single case study method.

More support for multiple cases is provided by Yin (1994), who suggests that

"multiple case studies have distinct advantages and disadvantages in comparison to single-case designs...a major insight is to consider multiple cases as one would consider multiple experiments - that is, to follow a 'replication' logic. This is far different from a mistaken analogy in the past, which

incorrectly considered multiple cases to be similar to the multiple respondents in a survey (or to the multiple subjects within an experiment) - that is, to follow a 'sampling' logic"
(Yin, 1994).

Yin also gave advice for when it is appropriate to select a single case study:

- where the organisation concerned can be considered a critical case;
- where an extreme or unique case can be identified; or
- where the organisation can be considered a revelatory case.

None of the above conditions could be met by any organisation in these early days of Internet use within companies.

I therefore decided on a multiple case study approach.

2.3.4.6 Unit of analysis, number and selection of cases

By studying the research question, one can best determine the unit of analysis (Benbasat *et al*., 1987). In order to gather sufficient data to develop theory for all sizes of companies in the future (including large organisations), and in order for the theory to accurately reflect the detail of security problems which substantial and complex Internet usage might lead to, I have selected *a medium-to-large company with substantial Internet connection and usage*, as the unit of analysis.

There were certain considerations in making decisions regarding the number of cases. Firstly, I needed to investigate a variety of different industry sectors to assure a general enough theory. As this research project aims to develop something quite large and complex in scope (a holistic set of guidelines for Internet security policy), *each case could involve an enormous amount of data collection and analysis*. Hence, I could not be over-ambitious in deciding upon the number of cases. I needed *two* readily accessible mini cases to support the hope that my theory was "on the right track", to be followed by as many detailed case studies as would enable me to build a rich and broad enough picture of the topic area in order to generalise and develop a credible theory. As each detailed case study would require a significant amount of data to be collected and analysed, I chose to investigate *three* detailed cases (which, as I mentioned earlier, was later supplemented by an additional case, making *four* detailed cases).

Another consideration was the desire to collect data from both the major types of stakeholders in Internet security policy—the employer (company) and the employees (Internet users). In the two mini cases, I gathered data from employee representatives, while in the four detailed case studies, I gathered data from employer representatives.

In all, I investigated SIX cases, representing five different industry sectors: educational, retail, travel, energy and scientific research.

2.3.4.7 Data collection

There are a number of data collection techniques which are useful for case studies (Benbasat *et al*., 1987). Yin (1994) names six sources of case study evidence: documentation, archival records, interviews, direct observation, participant-observation, and physical artefacts. To fulfil construct validity and reliability requirements, I needed to use multiple sources of evidence. I gathered my data via printed questionnaires and semi-structured interviews using open and closed questions as well as existing documentation—as I describe in the Chapters that present each case study.

2.3.4.8 Data analysis

Case data analysis involves

"examining, categorising, tabulating or otherwise recombining evidence to invoke the initial propositions of a case study"
(Yin, 1994)

Yin discusses two possible strategies for data analysis: *relying on theoretical propositions* and *developing a case description*. *Relying on theoretical propositions* is where the original objectives and design of the case study are based on propositions which reflect the research question(s) and/or hypotheses as well as scholarship and insight. The propositions focus attention on the relevant data to be analysed, and the way in which that data should be analysed. *Developing a case description* is only useful where there are no theoretical propositions.

Yin also suggests a variety of case data analysis techniques, from which I have selected *pattern-matching*. This technique involves comparing case study results with initial theory—in this project, the initial theory is the initial framework developed through scholarship (as I describe in Chapters 3 and 4). I *interpret* case data, as suggested by Yin, in order to carry out this pattern-matching.

2.3.5 Inductive and deductive research approaches

Neuman (1994) discusses two alternative research approaches—inductive and deductive. The inductive approach is useful for theory-building, where one commences with a research question and collects data to use as a basis for theories or hypotheses. The deductive approach is useful for theory-testing—where the theory already exists, and data are collected to confirm or deny it. In Stage 1, I employ both

scholarship and case study research as inductive research methods. In Stage 2, theory-testing, I need to investigate deductive research methods, as discussed in the next section.

2.3.6 Alternative research methods for Stage 2

Stage 2 involves testing the developed framework for validity. I have already selected scholarship and case study research to build the framework, and I require a different research method for *triangulation* purposes. I considered a survey impractical, as there were not enough organisations at the time exhibiting extensive Internet usage, for such a survey to prove viable or valid. One method which did, however, appear both viable and valid, was the well-known market-research method—*focus group*.

2.3.6.1 Focus group

(Chartwell Bass, 1998; Decision Analyst, 1998; Morgan, 1988; Nucifora, 1997)

Focus groups consist of panel discussions between six to twelve people who represent a specific target audience. The semi-structured focus group discussions are led by a *moderator*. These panels provide forums for discourse, exchange of ideas and feedback—as well as generating valuable qualitative research information representing critical client interests (Morgan, 1988).

Commonly employed as a market research method, focus groups typically yield ideas for new products, packaging, advertising, and consumer habits. Organisations can also use focus groups to determine what customers think about their policies, programs and services, as well as to investigate attitudes and ideas for new ways of doing business (Chartwell Bass, 1998). Focus groups are often used in market research to screen new concepts, that is:

Focus groups may be used to test the validity of ideas.

In Stage 2, the validity of a proposed framework is to be tested; a focus group may be useful for this.

Focus groups facilitate conversation in a relaxed, unstressful atmosphere. A properly run focus group allows the moderator to tap real feelings and issues (Morgan, 1988). Furthermore, a focus group is an ideal exploratory technique (Decision Analyst, 1998). In this project's relatively new topic area, there has not yet been much opportunity for experts to explore the related issues. These issues can be brought to the surface by a skilled moderator, and perhaps some consensus reached.

There are those who criticise focus groups (Nucifora, 1997). Firstly, they are not recommended for forming conclusive opinions or go/no decision-making (note, this project is not concerned with conclusive opinions or decisions). Second, the moderator must maintain control of the forum so that dominant personalities do not sway the group, and so that the timid get a chance to speak up (Nucifora,

1997). Third, it is all too easy for participants to "play into the hands of the stakeholder" by agreeing with ideas that they may not believe in reality. (The last two objections can be overcome by use of a skilled moderator.) Fourth, focus groups do not provide projectable estimates on their own, although used in conjunction with other methods—such as surveys or case studies—they can provide useful information (as is the case in this project). Hence, there is no good reason for *not* using a focus group for this project.

However, while focus groups are a well-known market research method, how widely used are they in information systems research?

Focus groups are, in fact, increasingly being used in information systems research (for example, Hasan and Tibbits, 1999). Because it is possible and feasible to locate and congregate a small number of employees, practitioners and experts in IT, Internet workplace use, Internet management and Internet security, to constitute a valid focus group to test the framework developed in Stage 1,

I have selected a focus group as the research method for Stage 2.

2.3.6.2 Focus group procedures

The key to a successful focus group research is the *moderator*. The person leading the focus group must be highly knowledgeable about the subject matter being discussed, as well as being a good conversationalist. What is required is thoughtful, skilled, knowledgeable, information-gathering. The best moderators are very smooth, non-threatening, and thinkers who lead the group. It is a difficult role to play. Hence, I selected an academic in the area of electronic commerce who is an excellent conversationalist, facilitator, explainer, has thorough knowledge of the area, and has a cool head.

The sample group of *participants* should be recruited from the target audience through a random selection process, rather than a "tainted", biased group of friends, colleagues, relatives, etc. I identified and recruited a panel comprised of representatives of employees, and practitioners and experts in IT, Internet management and Internet security. The participants were recruited by telephone, with elimination of those potential participants who displayed any biases that might prevent them from giving fair and honest responses to issues raised.

I followed up this initial phone call with mailing out of:
(i) a confirmation letter to each accepted participant, stating the time, date, location and various directions;
(ii) a form to be completed by each participant, providing information about the participant; and

(iii) the focus group objectives (refer Chapter 11). (Focus groups can yield richer and more insightful information if participants have enough time beforehand to reflect on the issues (Decision Analyst, 1998)).

The moderator reviewed the participant-suppled details before the session, to obtain information about the composition of the group and the nature of the participants.

The focus group took place as a one and a half hour session in June, 1998. I provided a document at the beginning of the session, containing the topics, issues and models to be discussed at the session. A free flow of ideas was facilitated by the moderator. The moderator also ensured that the focus group was best used to reveal pertinent information—as I was more interested in the "whys", rather than the "how muches" or "how oftens." The meeting was video-recorded, and I analysed the knowledge thus obtained, as will be described in Chapter 11.

2.4 Quality assurance for research design

Yin (1994) discusses criteria for assuring quality in research design: *construct validity, internal validity, external validity and reliability.* Below, I explain each criterion, and discuss how I employ it to assure the quality of my research design.

- *construct validity* establishes correct operational measures for the concepts under study.

The research design which I have selected increases construct validity in that I collect multiple sources of evidence, and review draft case reports by key people.

- *internal validity* is concerned with data analysis, establishing a causal relationship wherein certain conditions lead to other conditions.

Internal validity is an inappropriate concept for descriptive or exploratory case studies, and I have therefore excluded this criterion from my research design.

- *external validity* is concerned with the establishment of a domain to which the findings of the study can be generalised.

Because my research design includes studies of companies in a variety of industry segments, I can generalise the theory to companies in a range of industry segments.

- *reliability* is concerned with demonstrating that the procedures of a study can be repeated, producing the same results, in order to minimise errors and biases.

With the use of a recognised case study protocol in my research design, I am able to establish the reliability of results by documenting procedures and problems.

2.5 Relevance

Benbasat and Zmud (1999) highlighted the importance of relevance in information systems research. Research must have a purpose, as well as a target audience for whom it will prove useful (Shanks *et al*., 1993). The research question was stated in Chapter 1 and restated in Section 2.2. The audience who will find the research outcome of most use are companies planning or already embracing the Internet for business purposes, and academics researching this area or related areas. The research methods selected involve IT security practitioners, employer representatives (relevant managers), employees and potential employees (the final year computing/accounting students in the educational industry sector that was studied).

2.6 Conclusion

In this Chapter, I have introduced and fully justified the research design chosen for this project—as illustrated in Figure 2-1—with appropriate regard for the sage advice of a number of leading researchers in information systems research, put forward over the last decade or so.

With this research design in place, I am now ready to describe the *theoretical analysis*—my efforts in *subjective / argumentative research*—wherein I build an initial intellectual framework for Internet security policy for organisations, from the vast and diverse sources available in various domains. I describe this research in Chapters 3 and 4 which follow.

Chapter 3

Internet Security Policy in Perspective—a Contextual Analysis

"if we wait for the moment when everything,
absolutely everything is ready, we shall never begin."
(Ivan Turgenev)

3.1 Introduction

In Chapter 1, I introduced the need for guidelines in Internet security policy for organisations. In Chapter 2, I discussed and justified the research methodology selected for this research project.

In this Chapter and the next, I use the subjective/argumentative research method (Galliers, 1992) to build an initial framework for Internet security policy for organisations. To clarify these two Chapters, I have included a diagram of the issues involved in building the framework (Figure 3-1).

An overview of this Chapter now follows. In Section 3.2, I provide a background to existing guidelines for organisational Internet security policies, highlighting the limitations of current guidelines. In Section 3.3, I propose an outline for a framework for Internet security policy for organisations, composed of three components: factors, content and development. In Section 3.4, I propose a model for the factors component of the outline framework, and explore this model and a number of component models, by identifying and describing the many and varied factors that will influence the formation and composition of the Internet security policy—a genuinely holistic approach. In Section 3.5, I summarise the research embodied in the Chapter, and draw conclusions.

It is important to note here that it is the factors I identify in *this* Chapter (Chapter 3) which form the basis for the *following* Chapter's suggested guidelines for the content of the Internet security policy and suggested guidelines for the development of the policy.

I also remind the reader at this point that unless a phrase followed by a reference is encapsulated by quotation marks, the phrase is my own paraphrasing of the work of the author, and not a direct quote. For direct quotes, page numbers are given unless the reference is an online reference.

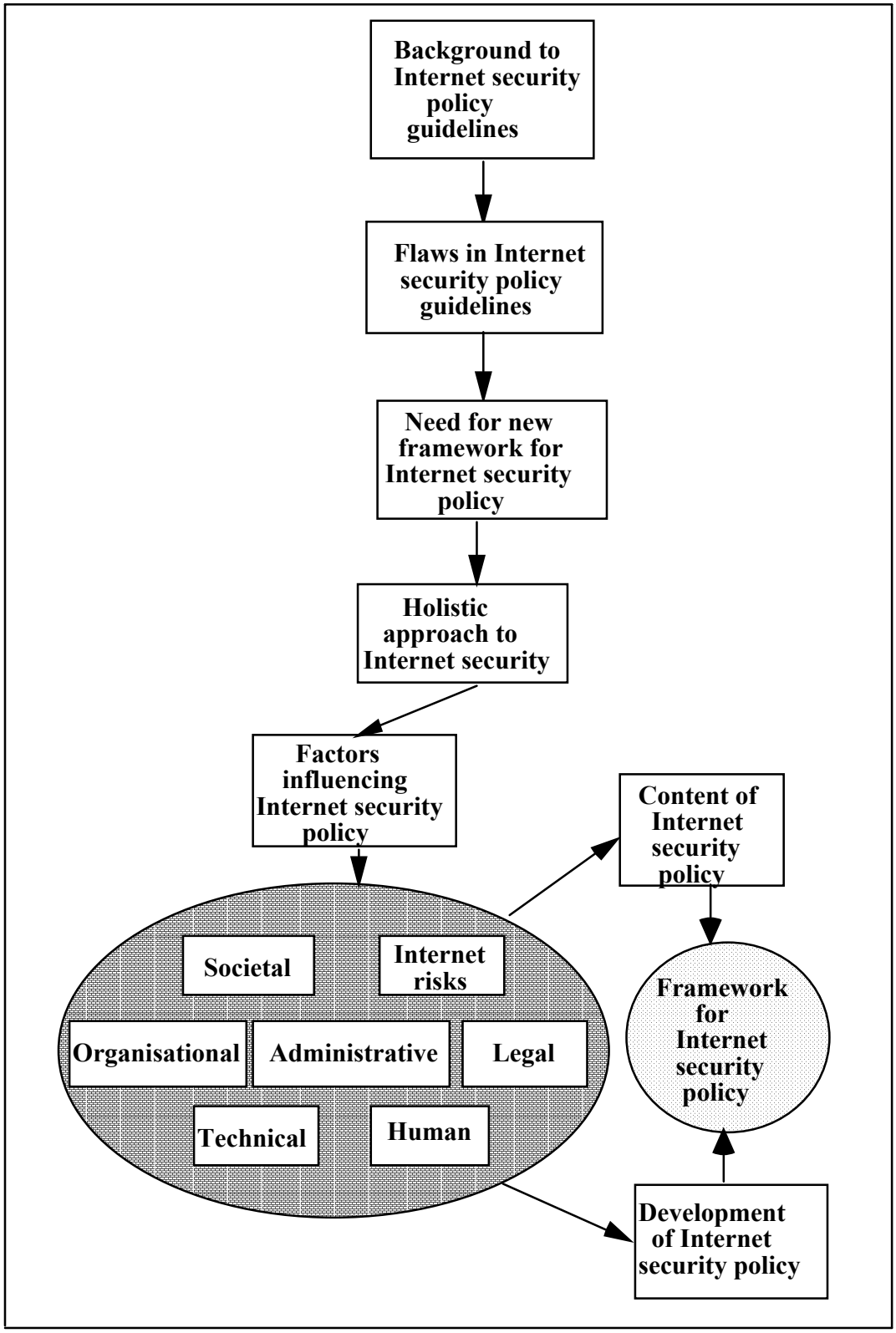

Figure 3-1 — Internet security policy in context

3.2 Background to existing Internet security policy guidelines for organisations

In this section, I remind the reader of the role of an organisational Internet security policy in Internet security management, then critique existing guidelines, in order to highlight the need for new, improved guidelines.

3.2.1 Introduction to Internet security policies for organisations

An organisational Internet security policy, and associated procedures, should be the media by which Internet security guidance and rules are provided to the various types of Internet participants, all of whom have their own individual security interests. Within a company, participants include owners, administrative managers, system managers, third parties (for example, clients) and employees.

The Internet security policy is the cornerstone of an Internet security management programme (Bernstein *et al*., 1996; Guttman and Bagwill, 1997; Lichtenstein and Swatman, 1997a; 1997b). The Internet acceptable use policy (IAUP) is an important sub-policy, informing the users of conditions of Internet use. Procedures are developed from the Internet security policy, and technologies selected, in order to implement the policy.

As I pointed out in Chapter 1, companies have, up till now, largely overlooked the need for Internet security policy, although encouragingly, some organisations are beginning to produce such policies. Nonetheless, current organisational Internet security policies appear to be largely Internet acceptable usage policies (IAUP), for example, the IAUP of ALIA (2000).

Clearly, as I stated in Chapter 1, the following advice should now be heeded by *all* Internet-connected companies:

"there must be a clear statement of the local (Internet) security policy, and this policy must be communicated to the users and other relevant parties. The policy should be on file and available to users at all times, and should be communicated to users as part of providing access to the system"
(Pethia *et al*., 1991 (online reference))

In the next section, I overview existing guidelines for organisational Internet security policy.

3.2.2 Existing guidelines in Internet security policy

To date, very little guidance for Internet security policies has been available. The earliest guidelines were produced by Pethia *et al*. (1991) and IETF (1991). Pethia *et al*. discussed policy for the entire Internet

community, including a recommendation that organisations specify: policies which make employees responsible and accountable for understanding and following security rules, policies for ensuring that employees used available mechanisms to protect their systems, and site-specific policies.

Later, the Internet Engineering Task Force (IETF, 1991) specified six basic guidelines for Internet security policies for Internet user communities:

- assure individual accountability;
- employ available security mechanisms;
- maintain security of host computers;
- provide computers that embody security controls;
- cooperate in providing security; and
- seek technical improvements.

Branstad *et al*.'s (1995) sample Internet security policy for the NREN (National Research and Education Network) adhered to the IETF guidelines, and included sections briefly defining objectives, scope, applicability, threats and vulnerabilities, principles, and allocation of responsibilities, for the NREN Internet participant organisations.

The U.S. National Performance Review's report on information technology (NPR, 1993) commissioned the development of a Federal framework for Internet security (FNC, 1995a), leading to the development of a Federal Information Security Plan (FISP) (FNC, 1995b). Specific actions in the plan addressed the need for guidelines for developing Internet security policy. The FISP policy-related actions initially recommended the development of broad Internet security policies to be issued through established channels such as Federal Information Processing Standards (FIPS), to be followed by the development of community-specific policies by the various participants in the Internet community.

One outcome of this planning was the U.S. National Institute of Standards and Technology's (NIST) technical guide for Internet security policy (Guttman and Bagwill, 1997). Several other sets of guidelines for Internet security policy for organisations, or IAUPs for organisations, have also been produced (Bernstein *et al*., 1996; Gaskin, 1998; Gassman, 1998; Heard, 1996; IETF, 1991; McMillan, 1996; Pethia *et al*., 1991), and guidelines for organisational electronic commerce policies have begun to appear (for example, Oliver, 1997).

3.2.3 Inadequacies in existing guidelines—the need for new guidelines

In Chapter 1, I introduced the limitations of existing guidelines for Internet security policy for organisations. Below, I review and expand on my earlier remarks, prior to the construction of my new framework.

As stated in Chapter 1, existing guidelines for Internet security policy were not developed from empirical evidence, but rather were based on professional expertise which, although not a recognised research method, may still yield valuable results. One research justification for my development of *new* guidelines is the fact that I am building a framework from *empirical studies*. Hence, my framework will make a different and valuable contribution to those guidelines already existing.

In Chapter 1, I also suggested that existing guidelines (Bernstein *et al*., 1996; Gaskin, 1998; Gassman, 1998; Guttman and Bagwill, 1997; Heard, 1996; IETF, 1991; McMillan, 1996; Pethia *et al*., 1991) are inherently limited. Below, I present a critique of Heard's (1996) guidelines, as an illustration of the problems with current guidelines.

Heard (1996) suggested an outline for Internet security policy content which included:

- definitions of terms;
- purpose of policy;
- scope of policy;
- provision of Internet services;
- Internet security plan;
- related procedures, including:
  - monitoring and sanctions;
  - prohibited Internet software;
  - downloading policy;
  - advice of firewall existence;
  - Internet service provider (ISP) use; and
- other applicable policies (eg IAUP).

Heard (1996) suggested an outline for IAUP content which included:

- definitions of terms;
- purpose of policy;
- scope of policy;
- ethics policy;
- business-only Internet access policy;
- copyright and licensing policy;
- business confidentiality policy;
- responsibilities policy, including monitoring duties of supervisors, and awareness and compliance duties of employees;
- list of acceptable uses: business use, approved postings unless accompanied by disclaimer;

- examples of unacceptable uses: non-business use, unsolicited advertising, propagation of malicious software, unauthorised external access, harassing postings;
- permitted non-business usage: no-cost use, outside working hours use, non-embarrassing use; and
- sanctions on noncompliance.

There are several shortcomings evident in the above outlines. First, there is no discernible connection between the two policies—yet they should be related. The IAUP specifies Internet acceptable usage requirements for employees; these are a subset of the organisation's overall Internet security requirements. Hence, the IAUP should form part of, and be consistent with, the Internet security policy. Second, the outlines do not address a comprehensive range of individual Internet risks. For example, the risk of denial-of-service is not mentioned (nor is any other specific risk). Third, the outlines do not include actions to be taken by employees should externally caused risks occur—for example, if a virus is detected. Employees are merely warned not to be the *source* of malicious code. Fourth, the outlines do not take an holistic approach—for example, there are many laws which an employee should be made aware of, apart from copyright and licensing laws. Other important issues such as Internet awareness procedures are only referred to "in passing".

Each existing set of guidelines for Internet security policy exhibits a selection of the following comprehensive list of shortcomings (presented in order of most important to least important) (I repeat the list already provided in Section 1.2.3.2 below, in order to emphasise the need for new guidelines):

- lack of an holistic perspective to Internet security;
- incomplete or missing coverage of:
  - factors to be considered in policy development;
  - framework for policy development;
  - content outline for policy;
- *ad hoc* and incomplete coverage of Internet risks;
- lack of a risk assessment process for determining significant Internet risks;
- inadequate, nonspecific or missing treatment of important and sensitive human issues in Internet security and usage;
- omission of reference to any corporate Internet strategy, infrastructure, or management programme;
- *ad hoc* specification of acceptable value-adding Internet usages;
- highly general sub-policies that are never made specific;
- ambiguous sub-policies;
- lack of empirical derivation of the guidelines;
- lack of empirical validation of the effectiveness of the guidelines;
- lack of agreement between the various guidelines.

I am aiming to develop a set of guidelines for Internet security policy that overcomes the above inadequacies, and will therefore constitute an improvement over existing guidelines.

3.3 Holistic guidelines for Internet security policy for organisations

This section establishes the concept of a set of holistic guidelines for Internet security policy for organisations, and proposes a three-component outline model for the guidelines.

3.3.1 An holistic approach to information security, Internet security and Internet security policy

Systems theory states that the behaviour of a system's interacting parts, when viewed as a whole, differs from the behaviour of the individual parts studied in isolation (Von Bertalanffy, 1956). Holism is defined as "the tendency in nature to produce wholes from the ordered grouping of units" (OED, 1992). Systems theory thus incorporates the notion of holism. The popular interpretation of holism is a study of the broad, all-encompassing picture, rather than a consideration of the individual components alone.

Information security may be viewed as a collection of interacting components, with the overall collection exhibiting information security properties (for example, rigidity) which are not necessarily observed in the individual components. Thus, information security satisfies formal and informal definitions of holism. With information security being a weak-link phenomenon, its design needs to be multi-dimensional (NRC, 1991), addressing a broad range of issues including computer security, systems analysis and design methods, manual information systems, managerial information security issues (for example, security policies) and societal and ethical issues (Baskerville, 1988). One of NIST's (1996b) principles for secure systems is that computer security needs a comprehensive and integrated approach.

Other examples of holistic information security perspectives are:

• The OECD's information security guidelines (OECD, 1992), which relate to many diverse aspects: people, their rights and their responsibilities; viewpoints (multidisciplinary, interorganisational, and intraorganisational); technical, administrative, organisational, operational, commercial, educational and legal aspects; the cooperation of parties; and the integration of the parts to form a coherent information security system.

• Organisational information security policies, which should take into account the organisation's information security philosophy, national policy, international standards, political issues, relevant organisational policies, implementation platform limitations, and relevant ethical, legal and privacy issues (Olson and Abrams, 1995).

There is a common theme to all holistic perspectives of information security: the non technical issues should be considered equally with the technical issues.

Many more holistic views of information security have been described (for example, Brunnstein, 1997; Hitchings, 1995; Lichtenstein, 1996d; Litchko, 1999; Warman, 1992; Yngstrom, 1995).

Some authors have stressed the need for holistic approaches for developing, evaluating, and managing information security (Hartmann, 1995; Kaspersen, 1992; Rannenberg; 1994; Yngstrom, 1995), while others have recommended holistic perspectives for specific domains of information security, with calls for a holistic perspective for the domain of Internet security (FNC, 1995b; Lichtenstein, 1996c; 1997a). A major thrust of the FNC's (1995b) FISP plan for Internet security was, indeed, the recommendation for:

"*a holistic approach to Internet security, in which physical, human and technical issues would be taken into account*." (FNC, 1995b)

Thus it is important that any set of guidelines for Internet security policy reflect an holistic approach.

An holistic approach to Internet security policy for organisations requires initially identifying in detail the diverse issues (factors) that should be taken into account—indeed, this is one of the research questions for this project (Section 1.3.1, Question 1)—then specifying a framework for the content of the policy and a method for developing the policy, based on these diverse factors.

3.3.2 Three components of Internet security policy guidelines

I therefore propose a three-component set of guidelines for Internet security policy for organisations—as illustrated in Figure 3-2.

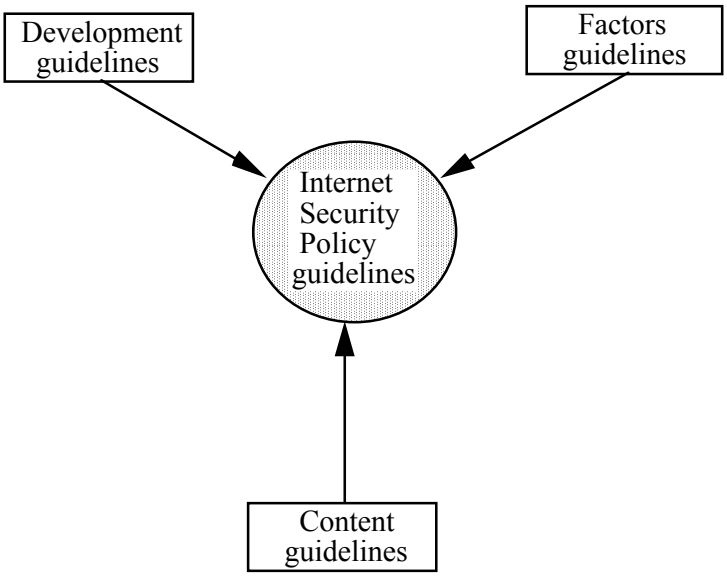

Figure 3-2 The three components of guidelines for Internet security policy

Section 3.4 identifies the diverse factors that influence Internet security policy for organisations, and presents a model of these factors. Note that guidelines for the content of the policy and for developing the policy, as well as the detailed final framework for Internet security policy, are all presented in Chapter 4.

3.4 Factors in Internet security policy for organisations

3.4.1 A model for factors in Internet security policy

Yngstrom (1995) divided holistic information security issues into *managerial*, *administrative*, *legal*, *technical* and *human* issues. Another eminent researcher, Warman (1992), determined in a 1991 survey of one hundred British companies those factors considered most important in developing computer security policy. The factors that Warman identified were, in order of most important to least important: *perceived threats*, *organisational objectives*, *end user considerations*, *calculated risk*, *management preferences*, and *consultancy advice*. Warman's and Yngstrom's holistic information security classification schemes can be extended to Internet security policy. (I have selected Warman's and Yngstrom's schemes as they are representative of existing holistic information security schemes.)

Hence, I have combined Yngstrom's and Warman's work in the factor classification scheme illustrated in Figure 3-3, omitting only *consultancy advice*, which Warman pointed out was deemed by companies to be of little importance, and adding *societal* factors, as I consider that organisational usage of a global tool as far-reaching and pervasive as the Internet, impacts on the entire global society. My proposed scheme

is introduced and justified briefly below, and expounded at greater length in the remainder of this Chapter.

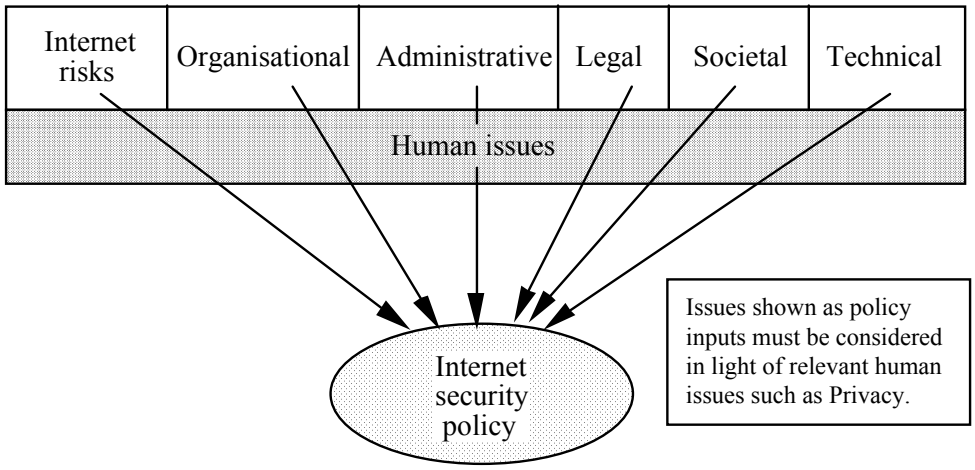

Figure 3-3 Factors in Internet security policy

3.4.1.1 Societal issues

Undeniably, global society is affected by a company's Internet connectivity. For example, a company's interactions with other cultures should take into account any differences between the cultures concerned. Another consideration will be that any global, national, and industry-specific Internet regulations and standards must be adhered to. I discuss societal issues in Internet security policy in Section 3.4.2.

3.4.1.2 Internet risks

(*Perceived threat* (Warman) and *calculated risk* (Yngstrom))

I have combined *perceived threats* and *calculated risk* into *Internet risks* which are initially identified, then assessed via a risk assessment process (Faroughi and Perkins, 1996) in order to determine the most significant Internet risks. Warman (1992) described *perceived threats* as those publicised by the media, thus raising company awareness of their existence. However, a better way to inform companies is for the company to have a guide to all possible Internet risks, to assist in identifying the significant risks.

Risk assessment considers internal and external risks, risks occurring at any of the company network's external access points, and the level of sensitivity and value of corporate data at risk (Faroughi and Perkins, 1996). 'Risk' can be defined as 'a measurable result of the realisation of a vulnerability' (Ekenberk and Danielson, 1995). Calculations of risk can be carried out using estimates of likelihood and impact, historical statistics of actual breaches, available security experts' professional opinions (Baskerville, 1988) or other methods (see Bernstein *et al*., 1996). I present a model of Internet risks for use by companies as a tool for Internet risk assessment, in Section 3.4.3 (Figure 3-5).

3.4.1.3 Organisational issues

(*managerial* (Yngstrom) and *organisational objectives* (Warman) and *management preferences* (Warman))

There are many organisational issues affecting the Internet security policy. For example, those usages of the Internet which are considered valid by the company and therefore acceptable should be clearly articulated. These usages should be aligned with organisational objectives in order to maximise benefits to the company (Brockway, 1996; Guttman and Bagwill, 1997; Lawrence *et al*., 1996; Logan, 1995; Logan and Logan, 1996; Miers and Hutton, 1996; Poon and Swatman, 1995; 1996). I discuss organisational issues in Section 3.4.4.

3.4.1.4 Administrative issues

(*administrative* (Yngstrom))

Administrative and operational tasks need to be considered and defined. For example, procedures for applying, monitoring and auditing Internet security policies are required (Branstad *et al*., 1995; Guttman and Bagwill, 1997). The feasibility of such tasks (for example, are there sufficient resources to carry them out?) will, to some extent, influence related policies within the Internet security policy. I discuss administrative issues in Section 3.4.5.

3.4.1.5 Legal issues

(*legal* (Yngstrom))

Relevant laws such as those dealing with the intellectual property rights of companies and employees in materials published on the Web, will need to be taken into account when setting Internet security policy (Guttman and Bagwill, 1997). I discuss legal issues in Section 3.4.6.

3.4.1.6 Technical issues

(*technical* (Yngstrom))

There are technical constraints which will affect the outcome of the Internet security policy, for example, available workstation technology places constraints on the Internet services which the workstations will be reasonably able to utilise. The company must also consider what it is willing to spend on additional technologies to improve Internet security, and formulate a policy which to a large extent foreshadows the acquisition of these technologies (D'Alotto, 1996). If there has already been an investment made, for example in a firewall, the company can devise a policy to use this investment to mitigate Internet risks. I discuss technical issues in Section 3.4.7.

3.4.1.7 Human issues

(*end user considerations* (Warman) and *human issues* (Yngstrom))

Human issues such as "freedom of Internet use", “privacy” and “censorship” are illustrative of the personal concerns which the end users, in this case, employees, will have in Internet security and usage. It is worth noting here that what may seem best from an organisational and managerial viewpoint may not seem best from the employees' perspective. For example, while the company may wish to prohibit all non-business Internet usage, many employees will see this as an unfair restriction. Similarly, what may appear best from the employees' or organisation's perspective may not be best from a societal perspective. Rannenberg *et al*. (1999) address this need for accommodating different levels of security in their concept of multilateral security, in which users may define their own level of security.

I have argued above that it is important for companies when developing policy to have at hand a model of the human issues in Internet security policy, to assist them in making reasoned decisions about sensitive issues such as restriction of Internet usage. I present a model of human issues in Internet security policy in Section 3.4.8.

Finally, I argue that each of the non-human factors may lead to human issues to be considered by the policy. For example, a proposal for a company firewall (a technical issue) may lead employees to be concerned about: the nature of access controls to be enforced by the firewall (Internet usage restrictions), the logging activities planned for the firewall (infringement of privacy rights) and planned monitoring of the logs (infringement of privacy rights).

As the human element is deemed to be the most critical factor in maintaining strong information security (Warman, 1992; Wood, 1995), the Internet security policy must be developed while considering each of the other factors in terms of the relevant human issues.

The above philosophy is reflected in the model of factors shown in Figure 3-3. In each of the following sections discussing various factors, I highlight the *human issue conflicts* raised by the conflicting needs of global and national society, individual companies and individual employees.

In the remainder of Section 3.4, I introduce and discuss the various factors. As I discuss each factor, I illustrate conflicts by means of boxes which appear as:

Conflict:

and I indicate useful Internet security policy content by means of boxes which appear as:

I now proceed to investigate each of the factors: societal, Internet risks, organisational issues, administrative issues, legal issues, technical issues and human issues, in depth.

3.4.2 Societal issues in Internet security policy

One of NIST's (1996b) eight principles for secure systems is: "Systems owners have security responsibilities outside their own organisations", while another is, "Computer security is constrained by societal factors." Extending these two principles to Internet-based systems, companies need to meet the needs of global society, in the level of Internet security they provide.

The following needs must be considered by the Internet security policy: adequate Internet availability, high personal and company ethics, recognition of cultural differences in global communications, adherence to global, national and industry standards and regulations (for example, Australia's recently revised AS/NZS 4444 standards for Information security management—Code of practice for information security management, 1999), conformance to netiquette (Internet communication standards), a degree of censorship, and privacy.

In this section, I first highlight the conflicts between societal needs in Internet security, and company and individual needs in Internet security, then discuss two specific societal issues—ethics and culture—in order to illustrate societal influences on Internet security policy.

3.4.2.1 Conflicts

Societal needs in organisational Internet security policy often conflict with organisational and individual needs, as illustrated in Figure 3-4.

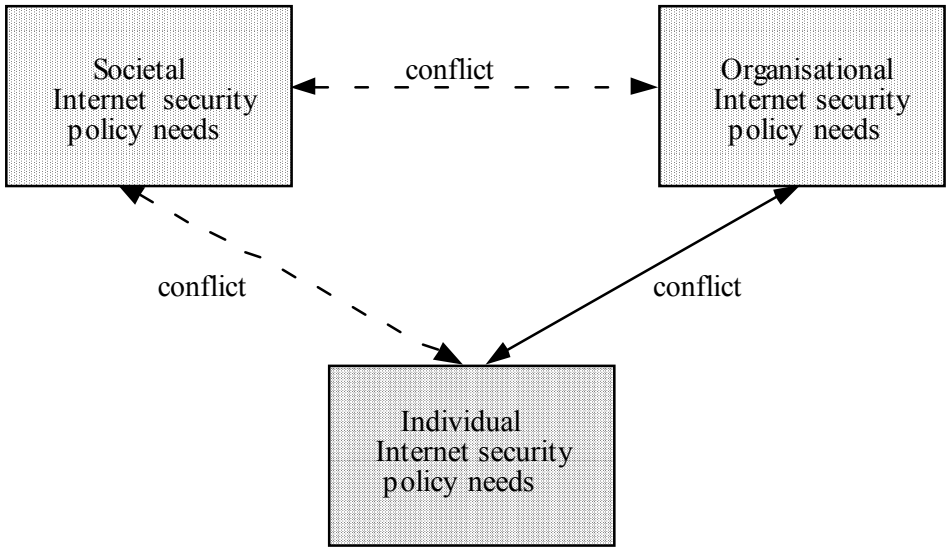

Figure 3-4 Societal, organisational and individual needs in Internet security policy

I will be concentrating on the conflicts between *organisational and individual needs in Internet security policy* for the most part in this thesis although, because of its importance, I include below a brief introduction to the conflicts between society and the organisation, and society and the individual.

Many societal Internet usage demands clash with company needs. An example controversy is presented by weak cryptography schemes (which may be employed by Internet security technologies). These are designed so that the data processed by technologies using these protocols can *easily* be decrypted by the owner companies and law enforcement agencies—by enabling *easy* retrieval of hidden keys from their "safe" hiding places. This is desirable from both the employer *and* law enforcement agency perspectives, as they don't have to worry unduly about "losing" the keys (and hence access to the data). It also means however, that hostile external parties may retrieve the keys from their perhaps “unsafe" hiding places—a societal problem in that the data privacy and confidentiality of data thus encrypted are under continual threat of compromise.

Many societal Internet usage demands clash with individual needs. For example, an individual's manner of expressing him/herself on the Internet may be at odds with society's expectations of politeness. The recipient of an email message in one culture may regard a message as offensive when it was deemed inoffensive by its author.

I now discuss two societal issues in Internet security, to illustrate the effect of societal issues on policy.

3.4.2.2 Ethics

A sense of ethics within a global society should be expected in Internet usage. Politeness, honesty, fairness, trust, willingness to share with and assist others, are all examples of society's ethical expectations in Internet dealings. A statement to this effect in the Internet security policy is desirable.

A key example of an ethical issue is *netiquette*, a set of Internet communication standards for Internet politeness (Highland, 1996). Many attempts have been made to standardise netiquette (Scheuermann and Taylor, 1997).

An organisation may wish to vary netiquette to suit its own culture, with variations being documented within the Internet security policy.

3.4.2.3 Culture

Internet business collaboration is enabled by open email, groupware, discussion groups, address and phone look-up, audio and video services, plus network-transparent calendaring and scheduling. Nance *et al*. (1995) and Kaye and Little (1996) highlighted the need for organisations to understand the different global cultures with which they collaborate technologically. These cultural differences impinge upon individual ethical behaviour and the effectiveness of the collaboration.

Individual cultures may differ in their acceptance of the authority behind a policy (Condon *et al*., 1985). Some cultures obey laws and policies quite readily, while others require active enforcement and sanctions as added inducements. Cultural issues gain significance whenever interaction between people of different cultures takes place. "Language barriers, nonverbal communication, overscrutinization, socialization and intimacy, and interpersonal synchrony" were all identified by Nance *et al*. (1995) as problematic issues in global, computer-mediated communication, leading to possible misinterpretation and error. Despite difficulties which may be encountered in attempting to provide comprehensive and effective solutions to multicultural problems within an Internet security policy, some guidance is advisable.

The Internet security policy can advise of standards and regulations to be followed in Internet usage, as well as advice to employees regarding cultural, ethical and other global society needs in Internet communication.

3.4.3 Internet risks for organisations

In this section, I develop a model of the Internet risks for organisations, which should be addressed by the Internet security policy. I define *Internet risks* to include not only traditional *security risks* to the

confidentiality and integrity of information, and the availability of the Internet resource and company systems, but also *business exposure risks* to the business itself (such as damaged company image from a low quality Web site), and *personal risks* (such as employee harassment from abusive email).

Several models of Internet risks have already been proposed (for example, Bernstein *et al*., 1996; Faroughi and Perkins, 1996; Wood, 1997b), although these models typically focus on gaining the understanding of technical personnel such as network administrators and security technologists, rather than the understanding of senior business managers, business unit managers, security analysts and employees. Existing models are also incomplete. As an example of my concerns, consider Wood's (1997b) scheme and my critique of it, below.

Wood's guidelines present a model of *Internet risks*, categorised into:

- fraud and embezzlement;
- service interruption or degradation;
- data integrity corruption;
- confidential information disclosure;
- privacy violation;
- sabotage or vandalism (including viruses);
- errors or omissions;
- unauthorised system usage; and
- intellectual property law violations.

Some criticisms of this model are:

(i) 'Errors or omissions' and 'privacy violation' are too broad. For example, what does each such risk type cover? How does an 'error' occur? How is privacy violated?

(ii)Where are well-recognized security risks such as 'hacking', in this scheme? 'Hacking' could be covered by either 'unauthorised system usage', 'sabotage or vandalism' or 'data integrity corruption', for example.

(iii)Where are well-recognized business exposure risks such as 'inappropriate email' and 'non-business usage' in this scheme? They would have to be included implicitly within 'service interruption or degradation' and 'privacy violation', rather than being explicitly specified.

I have developed an Internet risks model which presents a non-technical perspective of Internet risks, and includes a comprehensive set of internal, external, deliberate and accidental risks.

The Internet risk types to which an organisation may be exposed through Internet usage are illustrated by the model in Figure 3-5. I compiled this model from previous findings (notably, Bernstein *et al*., 1996; Cheswick and Bellovin, 2000; Cooper, 1995; Denning, 1996; Faroughi and Perkins, 1996; FNC, 1995a;

Guttman and Bagwill, 1997; Hsieh *et al*., 1996; Neumann, 1997d; NIST, 1994b; 1996a; Stallings, 1995; Wood, 1997b). It should be noted here that this model is not intended to be a detailed, low-level taxonomy of Internet risks for an organisation, but rather a high-level tool for assisting companies in locating and identifying their significant Internet risks—which should ultimately be addressed by the Internet security policy.

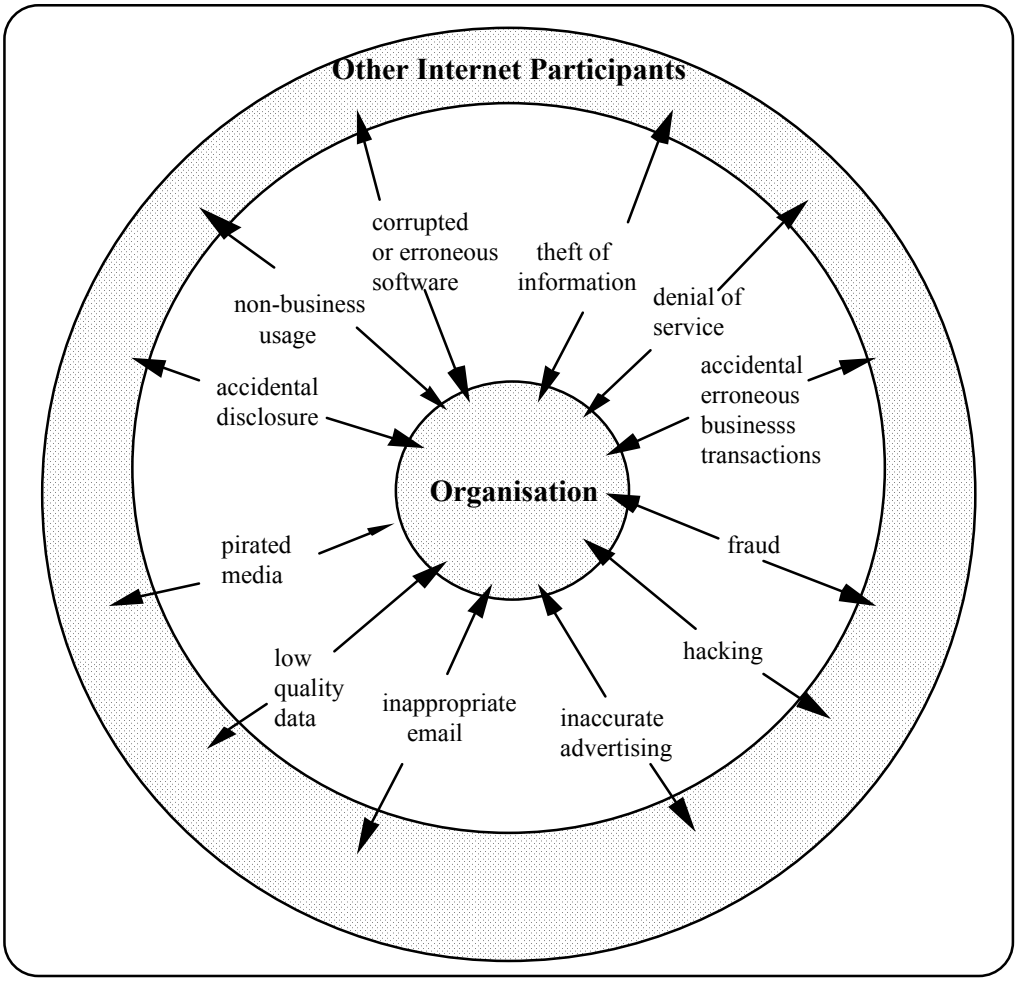

Figure 3-5 Internet risks for an organisation

The central circle denotes an organisation with Internet connection. The outer ring labelled 'Other Internet Participants' denotes other members of the Internet community with whom the organisation communicates via the Internet. The spokes of the wheel portray Internet risks which can emanate from within the organisation and affect other Internet participants, or which can emanate from other Internet participants and affect the organisation. Each spoke represents a different type of Internet risk.

I also include here Table 3.1 for explanatory purposes only *(Table 3.1 is not part of the proposed framework*), linking Internet risk types to their possible impacts and to selected technical countermeasures for reducing the risks. I remind the reader that this research project focuses on the use of

a nontechnical control, the Internet security policy, as a security measure. Hence, the technical controls listed in Table 3.1 are not discussed any further at this juncture, although they are briefly mentioned in Section 3.4.7 (when introducing the effect of technical constraints on Internet security policy).

After viewing Figure 3-5 and the explanatory table, Table 3.1, the reader is invited to learn more about these risks, and how they may be addressed within the Internet security policy, in the ensuing discussion (Sections 3.4.3.1 to 3.4.3.13).

Internet risk type	**Possible impacts**	**Technical countermeasures**
Accidental disclosure (See Section 3.4.3.1)	loss of data confidentiality; loss of privacy; financial damage; loss of competitive advantage; embarrassed employees	privacy-enhanced email (PEM, PGP); encryption; anonymous email services; text filters
Accidental erroneous busines transactions (eg corrupted electronic messages, misdirected email) (See Section 3.4.3.2)	loss of data confidentiality; loss of stored data integrity; loss of message integrity; embarrassed employees	message authentication; message digests; automated verification of send address(es) by mailers; overt mapping of aliases by mailers
Corrupted or erroneous software (eg viruses) (See Section 3.4.3.3)	corrupted or buggy software on system; spreading infections (eg viruses); disruption to work; harmful to employee morale; corrupted hard disk or other strange happenings	firewalls prohibit access to shareware and other dubious sites; firewall scanning of all email attachments and downloaded software, for viruses; antivirus programs (updated frequently)
Denial-of-service (See Section 3.4.3.4)	Internet traffic delay; total loss of Internet connection; loss of data integrity in Web site content; lost productivity; lost transactions; nuisance to employees.	anonymity of communication via digital signature can prevent selective flooding; increased bandwidth; high-speed lines, eg ISDN PRI service; more powerful PC's and operating systems; resource reservation

Table 3.1 (Part 1) Internet risks, impacts and technical countermeasures

Internet risk type	Possible impacts	Technical countermeasures
Fraud (See Section 3.4.3.5)	financial damage; loss of data integrity; loss of data confidentiality; damaged company image; litigation and resulting financial damage;	encryption; PKI; digital signatures; strong authentication; digital certificates; redundant info stored within message
Hacking (See Section 3.4.3.6)	loss of data confidentiality; loss of data integrity; denial-of-service; financial damage; damaged company image; harmful to employee morale; lost productivity; disruption to work; litigation and resulting financial damage	firewalls; strong authentication; encryption; PKI; secure storage of encryption key; account lockout after successive failed login attempts; unavailable anonymous and guest ftp services; separate servers containing sensitive corporate data; intrusion detection systems; network security management technology
Inaccurate advertising (See Section 3.4.3.7)	damaged company image; litigation, and resulting financial damage	automated disclaimers attached to all emails
Inappropriate email (See Section 3.4.3.8)	employee harassment; lost productivity; Internet traffic delay; litigation, and resulting financial damage; loss of privacy	anti-spam filters; text filters for offensive words
Low quality data (See Section 3.4.3.9)	litigation and resulting financial damage	content regulation software; site filtering by firewalls, filter software

Table 3.1 (Part 2) Internet risks, impacts and technical countermeasures

Internet risk type	Possible impacts	Technical countermeasures
Non-business usage (See Section 3.4.3.10)	lost productivity; Internet traffic delays; employee frustration; poor work attitude	filtering, logging and exception reporting by firewalls and proxy servers
Pirated media (See Section 3.4.3.11)	existence of illegal software on company systems; litigation and resulting financial damage; damaged employee and company images	firewalls which block access shareware sites and other similar sites
Theft of information (See Section 3.4.3.12)	loss of data confidentiality; loss of data integrity; loss of competitive advantage; litigation and resulting financial damage	(as for hacking); also digital certificates

Table 3.1 (Part 3) Internet risks, impacts and technical countermeasures

In the following discussion of Figure 3-5, I:

- define each Internet risk type;
- illustrate each Internet risk type by highlighting the most prevalent and damaging Internet risks for that risk type;
- discuss possible impacts of each Internet risk type on the company and its employees;
- highlight conflicts between societal, organisational and employee needs;
- cite real cases of each Internet risk type; and
- discuss possible Internet security policy countermeasures.

Note: Although I point out conflicts between societal, organisational and employee needs in handling each risk, in the following discussion, the main discussion of these issues is reserved for Section 3.4.8 (Human issues).

3.4.3.1 Accidental disclosure

Employees may be incautious in their use of the Internet when communicating possibly confidential business matters, or personal or other sensitive information. Taylor and Resnick (1995) said it all when they advised:

Don't "post anything you wouldn't want to see on the front page of the National Enquirer".
(Taylor and Resnick, 1995, p. 33)

A typical situation is the unintentional inclusion of confidential information within email, Web sites or other postings. A 1998 survey ranked communication of confidential company information by employee email as the number one Internet risk concern for companies (Credit Control, 1998). Alarmingly, a recent study reported 24% of employees receiving confidential email leaks (Marsan, 2000).

LoVerso (1996) described a case of unintentional inclusion of an important FBI url within a posting sent to the Risks mailing list. The seemingly harmless url, http://www.fbi.gov/mostwant/tenlist.htm was included in the posting, thereby unintentionally disclosing the less harmless url, http://www.fbi.gov/mostwant/. In other words, a reader may strip endings off harmless url's legitimately posted to the Internet, and use the derived url's to gain access to possibly confidential information.

The U.S. Department of Energy issued a memorandum in February, 1998, entitled "E-Mail concerns", expressing concern over continual unintentional inclusion of classified information by employees in outbound email (Identity withheld, 1998). Possible snooping for such information in email by external parties, was mentioned in the memo as a matter of concern, and employees were reminded of the Department of Energy's policy of information review for classification prior to dissemination. A warning was issued that, unless the situation improved considerably, text filter software would be employed on firewalls to scan outgoing email for key words and phrases indicating classified information—thereby slowing email down to the level of snail mail. One Australian government military establishment currently requires that its employees label their outgoing email "Security Unclassified". This way, an employee can be held accountable for the level of confidentiality of email.

Suggesting restrictions for employee email content affects an employee's right to freedom of speech, and raises the following conflict:

Conflict:

The needs of society:
protection from unintended public exposure to confidential business information
vs
The needs of the company:
employee email restricted to exclude confidential company information
vs
The needs of the employee:
freedom of speech in email; trust shown by employers

Employee email may be deliberately intercepted internally (eg by managers) or externally (eg by law enforcement agencies) and read, raising a dichotomy between an employee's right to email privacy and the interests of law enforcement agencies and employers (Farrow, 1998; Neumann, 1993):

Conflict:

The needs of society:
law enforcement agencies need to be able to decipher and read the email of suspected law-breakers
vs
The needs of the company:
monitoring employee email to ensure absence of confidential company information and business-only usage;
protection of employee email from external interception
vs
The needs of the employee:
email privacy;
freedom from governmental and company monitoring and surveillance;
reasonable personal email use, and trust shown by employers

Many managers believe that employee email is a company asset, and therefore that they have a right to read it—for tracking worker performance, checking for outgoing confidential or otherwise inappropriate information, or checking for legality (Barker and Gettler, 2000; Carson and Farrant, 2000; Farrow, 1998; Pathak, 2000; Sipior and Ward, 1995; 1999; Weisband and Reinig, 1995).

Employers are now well aware of the increasing liability of companies for employee email content. In a U.S. case, *Davis v. Merrill Lynch, Peirce, Fenner and Smith Inc*, the court held Merrill Lynch liable for the fraud committed by email by one of its employees. The U.S. court found that the company had a responsibility to control outgoing information (Farrow, 1998). U.S. courts have shown acceptance of management's right to read their employees' email. For example, in 1994, in *Shoars v. Epson*,

management rights to read email were upheld by the U.S. court, after a manager was found to be printing and reading employee email (Moulton, 1998). Countries around the world are now dismissing employees for inappropriate emails (for example, Centrelink in Australia recently dismissed six employees (Carson, 2000b)). Furthermore,

---

surveys indicate that a significant proportion of managers read their employees' email.
(Barker and Gettler, 2000; Farrow, 1998; Freehill *et al*., 2000)

However, email monitoring is regarded by many employees as an unethical disregard for privacy. Employers argue that this expectation of employee email privacy is unreasonable (Sipior and Ward, 1995). In addition, system managers sometimes need to sift through (and read?) "presumed lost email" in the inevitable network disasters that occur from time to time. Employees may similarly object to this as an invasion of privacy. Most employees assume their email is private and confidential (Farrow, 1998; Weisband and Reinig, 1995)—obviously an unwise assumption these days.

An interesting turn of events took place in Australia recently, with amendments to a new privacy act providing added protection for the content of employee email (The Age, 2000b). It is too early to determine the level of protection the new act will provide.

Email may not only be read internally, but also be intercepted externally, for example by law enforcement agencies or corporate spies. A salient example was the case of Rodney King, in which email was sent by Los Angeles police officer Laurence Powell to a friend after the Rodney King beating (Weisband and Reinig, 1995). This email was used as evidence in court against Powell. The email stated, "I haven't beaten anybody this bad in a long time".

Possible impacts of the risk of "accidental disclosure" include loss of confidentiality, loss of privacy, employee embarrassment, financial damage and loss of competitive advantage.

The Internet security policy can include advice to employees regarding cautious use of email, by warning employees to double-check the destination address and content prior to despatching their email. Advice can also be given cautioning the employee not to post confidential business information without authorisation by a responsible body, and only to send email to selected, specified types of recipients.

Employees can also be warned that their email is regarded as the property of the business and may be being monitored for compliance with policy. Employees should be advised of the company's email encryption policy, which offers a degree of protection from external email interception. They should also be warned of the rights of law enforcement agencies to read their email, and of the possibility of corporate competitors intercepting and reading employee email. Finally, use of filters and monitoring via firewalls, and appropriate sanctions for abuse, should be advised.

3.4.3.2 Accidental erroneous business transactions

Electronic messages may become corrupted accidentally in transit (for instance, corrupted EDI messages), or companies may accidentally issue transactions incorrectly (a well-known example being the misdirecting of email). Just about every Internet user has accidentally misdirected email at some stage.

In one case, a postgraduate IT student at one Australian university emailed her confidential and highly-sensitive PhD scholarship application for another Australian university to an entire global IT mailing list—not the best way to create a favourable impression at either university.

There are other ways for misdirected email to occur—for example, the silent mapping of aliases by some mailers.

Possible impacts of this risk include loss of transaction confidentiality, loss of data integrity, loss of message integrity, and embarrassed employees in the case of misdirected email.

The Internet security policy can advise employees as to the existence of message integrity technical controls. It can also prescribe steps to back up electronic messages prior to despatching them, and to report and recover from mishaps should they occur. Regarding misdirected email, the policy can advise employees to double-check the send address and content prior to despatching email.

3.4.3.3 Corrupted or erroneous software

There is a risk that an employee may download or provide software containing bugs or malicious code.

In the first case—*malicious code*—not only may such code be obtained accidentally via downloading, but it may also be received within email attachments, or deliberately injected by attackers into systems via hacking or other means (such as through Web browsers, which may provide access to untrustworthy systems or may invoke unproven applications). The major form of malicious code is the virus.

In the second case—*erroneous software*—Borenstein (1996) points out that programs for new Internet services, as well as new versions of existing services, usually contain bugs. Further, there are many amateur individuals and groups making their own, unproven software available for downloading on the Internet. There is even a school of thought that believes that reputable software producers deliberately bug the early releases of their software, then utilise the skills of eager net users to test the software and report all found bugs.

85% of respondent organisations in the CSI/FBI 2000 Computer Crime and Security Survey reported virus attacks (CSI, 2000). Another study revealed that in 1999, viruses cost businesses a staggering $12.1 billion in lost productivity, network downtime and recovery expenses (Noack, 2000). In particular, e-mail-attached viruses devastated the Internet (Kabay, 1999).

E-mail-enabled viruses and worms are now a serious threat to systems everywhere.
(Kabay, 1999)

Some particularly nasty malicious code attacks have attained legendary status, perhaps the most infamous being the Internet "worm" of 1988 (Eisenberg *et al*., 1989). Only recently, the rapidly spreading Love Bug virus attacked an estimated 45 million users (CNN, 2000) and caused $4 billion damage (The Age, 2000a).

A variety of technical and nontechnical antiviral measures are now on the market (Hinde, 1998; Sanford, 1993), the latest being firewall-implemented technologies which scan downloaded software for viruses, strip off email attachments, etc. Nowadays, email attachments containing Microsoft WORD macro viruses are the most common means by which viruses are transmitted (Hinde, 1998).

Possible impacts of 'malicious code and erroneous software' include the existence of corrupted or erroneous software on company systems, disruption to work and poor employee morale. Malicious code may infect other parts of the system, and even other systems within and outside the company in due

course, spreading the damage. There can even be a denial-of-service effect from the clogging up of massive amounts of resources as a virus spreads through systems and entire networks (as happened with the Internet worm)—not to mention the time spent recovering from a virus attack, which alone can cost enormous sums of money through lost productivity. Furthermore:

---

viruses have a terrorising, insidious, even sinister, morale-destroying effect on employees, who are often uncertain and confused as to how to protect their software from viruses.

This effect can be attributed in no small measure to hoax emails announcing perilous viruses, and the rash of follow-up email instructions and advice from many genuine, as well as falsified, sources.

Nevertheless, antiviral procedures can cause frustration to employees, summarised by the following conflict:

Conflict:

The needs of society: global Internet-connected companies desire protection from the spread of viruses vs *The needs of the company:* protect company networks and data from virus presence and impact vs *The needs of the employee:* freedom in downloading software and lack of censorship of email; freedom from self-executed antiviral programs

The Internet security policy can include advice to employees regarding downloading of unproven software that may contain bugs. Employees should be given antiviral policies for: reporting email virus hoaxes, caution in accepting email with attachments or from unknown sources, caution in downloading shareware from the Internet, disallowance of external floppy disk software importing, proper use of company antivirus software, awareness of the existence of any firewall virus scanning, and action to be taken on suspicion or detection of virus presence. The Internet security policy can also inform employees how to obtain the software that they require in ways other than downloading shareware. Finally, use of any other filters and employment of monitoring via firewalls, as well as sanctions for policy abuse, should be advised.

3.4.3.4 Denial-of-service

There is an increasing risk that Internet participants may act as a source or conduit for *deliberate* threats resulting in denial-of-service, either manifested as an Internet traffic delay or complete inability to gain access. Alternately, resource overusage may *accidentally* slow or disable the Internet facility (Schwartau, 1997; 2000).

60% of companies attacked via the Internet in the CSI/FBI 2000 Computer Crime and Security Survey, reported denial-of-service attacks (CSI, 2000).

Deliberate denial-of-service may occur in many ways. Typically, a barrage of hits causes a site to become inaccessible, as in the 1999 FBI web site attack (CNN, 1999) and the distributed denial-of-service attacks of February, 2000, where innocent computers were held hostage in order to render various major web sites—including Yahoo! Buy.com, eBay and Etrade—inaccessible (Ross, 2000). Sometimes flaws in software may be exploited, such as the attack known as "New tear", enabled by flaws in NT 4.0 and Windows '95 (Welsh, 1998).

One classic denial-of-service attack is known as "flooding", where the perpetrator causes excessive traffic (eg email) for a selected customer, or for a randomised customer base, so that genuine traffic is held up, lost, or judged unprocessable by an overloaded server

(Needham, 1994)

Accidental denial-of-service can happen anywhere where there is inadequate bandwidth combined with resource overusage. An example was the Wall Street scramble of October, 1997, noted earlier (Bellovin, 1997), which led to an inability to access critical stock-price sites and inaccurate figures listed on relevant sites. Another case was reported in Neumann (1997c)—a major ISP (America Online, AOL) had an outage in late 1997 lasting two hours, caused by a hardware glitch and complicated by subsequent system wide software problems. During this outage, online users lacked email facilities for several hours, while new users were unable to log in for two hours. Garfinkel (1997) also reported a denial-of-service problem at AOL during October/November, 1997.

Furthermore,

---

accidental denial-of-service is increasingly a result of excessive non-business Internet usage in the workplace (refer Section 3.4.3.10).

This is because the non-business usage consumes bandwidth, at the expense of valid business usage.

A topical dilemma in policymaking is raised by this risk:

Conflict:

The needs of society:
speedy Internet service and traffic movement worldwide
vs
The needs of the company:
undelayed Internet traffic; no denial-of-service; inexpensive bandwidth
vs
The needs of the employee:
unrestricted Internet usage; continuous, speedy Internet traffic; no denial-of-service

As has already been mentioned, accidental denial-of-service may also be facilitated or exacerbated by inadequate bandwidth. Bandwidth is the measure of the capacity of a network—the amount of traffic it can transmit—typically measured in bits per second. The Internet backbone is already saturated and congested due to inadequate bandwidth on many network connections, and with multimedia applications becoming more popular, accidental denial-of-service because of inadequate bandwidth is increasingly a concern.

Possible impacts from 'denial-of-service' include Internet traffic delays, loss of Internet connection, loss of data integrity in site content, lost transactions, lost productivity, and nuisance to employees.

The Internet security policy can include advice to employees not to (over)use the Internet facility at peak times, and not to (over)use it for non-business purposes. Advice as to actions to be taken if "flooding" occurs can be given. Employees should be advised as to steps to take if denied their required Internet access due to Internet traffic delay. Employees should be warned not to cause denial-of-service via flooding or other means, to other Internet participants. Finally, use of filters and/or monitoring for abuse, via firewalls, as well as sanctions for abuse, should be advised.

3.4.3.5 Fraud

Internet participants may fraudulently obtain monies from a company or individuals using the Internet connection.

Computer fraud in general has proven a particularly nasty problem for companies in recent years. A 1997 survey revealed that 57% of international banking and finance companies reported computer abuse in the

previous twelve months (the highest computer misuse statistic reported by all industrial sectors surveyed) (Ashton-Davies, 1997). There was reported growth of over 200% in company computer fraud during the period 1995—1997, with average losses per company being around $30,000 (with some individual losses around $1.5 million) (Ashton-Davies, 1997). One estimate of the rate of growth of computer fraud was 500% per year (Milunovic, 1997b). Milunovic pointed out that, according to the U.S. National Centre for Computer Crime, fraud constituted 44% of all computer crime. (These estimates, of course, include non-Internet as well as Internet fraud.) In CSI/FBI's 1999 survey of computer crime and security in American companies, 14% of respondents reported fraud in the previous year (CSI, 1999a).

Multi-national companies with Web sites are exposing themselves to even greater risks of extortion and fraud, with people now willing to submit personal information to financial and service web sites (KPMG Forensic Accounting, 1998) and with the increased visibility of companies with Internet connection (Milunovic, 1997b). Further,

---

fraud can be committed on a much grander scale, and much faster, via the Internet.

The following four incidents illustrate the vulnerability of the Internet to fraudulent attacks. In the first incident, a hacker group demonstrated to the German media how easily the Internet could be used to subvert online banking transactions by illegally transferring funds from one bank account to another (Mitton, 1997b).

In the second incident, Citibank's electronic money transfer system was hacked into (via the Internet) by Russian hackers, shifting $10 million to various international accounts (Mitton, 1997b). Young Vladimir Levin was sentenced in the U.S. in February, 1998, to three years in prison for his role in this fraudulent incident, and was required to pay Citibank $240,015 in restitution, after having already spent 30 months in a British jail and 6 months in a U.S. jail (the 3 years already served constituted his new sentence) (CNNfn, 1998). Four of his hacker accomplices had earlier pleaded guilty to conspiracy to commit bank fraud.

In the third incident, a Russian hacker released credit card details stolen from online music retailer, CD Universe, via a Web site (Sullivan, 2000).

In the fourth incident, a hacker in Eastern Europe stole 485,000 credit card details from an e-commerce site, then stored the data on a U.S. government web site—where it was eventually discovered during a routine audit (Brunker, 2000). Astonishingly, many of the credit cards thus revealed had not been cancelled by the (notified) financial institutions concerned, who judged the risk of their unauthorised use as unlikely.

In a recent demonstration of the vulnerability of credit card data, MSNBC accessed nearly 2,500 credit card numbers and related personal data, merely by browsing e-commerce Web sites using a commercially available database tool (Sullivan, 2000).

With the imminent arrival of full-scale e-commerce, the risk of fraud is terrifying for companies and customers alike.

E-commerce schemes relying on electronic forms of payment are vulnerable to fraud via forgery, repudiation, misrepresentation (for example, via spoofing), denial-of-service, replaying of transactions and various forms of cheating (Bhimani, 1996; Borenstein, 1996; Cooper *et al*., 1996; Ellison and Schneier, 2000; Hudoklin and Stadler, 1997; Pattison, 1997; Schneier, 1996). The public are well aware of the problem, with 66 percent of respondents in one 1997 study citing credit card fraud as a major online shopping concern (Aldridge *et al*., 1997), and 86% of respondents in a 1998 study citing credit card fraud as the main inhibitor holding them back from involvement in e-commerce (TRUSTe, 1998).

Cooper *et al*. (1996) attribute e-commerce fraud to particular parties in the transaction:

- merchant fraud—committed when a purchaser does not authorise a transaction;
- third-party fraud—committed through the unauthorised use of an account; and
- purchaser fraud—committed when a purchaser buys a product or service but denies doing so, falsely claiming that the purchase was unauthorised.

There are ever more ingenious methods for committing Internet fraud, for example the copying of held digital cash by its owner (Pattison, 1997).

Groups and Web sites provide tips for merchants and consumers, advising how to avoid financial and other types of fraud in Internet use (see, for example, Antifraud.com, 1998; NETrageous, 1998; IFW, 1999a, 1999b).

On an optimistic note, new technologies to tackle the Internet fraud problem are emerging. In particular,

---

public key infrastructure (PKI) is a critical technology for reducing the risks of fraud in e-commerce.

Various schemes have been proposed to provide confidentiality and privacy, message integrity, authentication of parties involved, and non-repudiation, for e-commerce transactions and messages (Bhimani, 1996; Garceau *et al*. 1998; Hudoklin and Stadler, 1997; Liddy, 1996), with the most recent of

these schemes employing PKI technology to enable digital signatures, digital certificates, digital coins and various complex digital payment protocols.

Of concern is that evolving digital payment protocols are inevitably reported as vulnerable (for example, Svigals, 1997). Indeed recently, Ellison and Schneier (2000) warned of risks incurred in using the much-vaunted PKI technology for digital signatures and certificates. Borenstein (1996) cautioned overall against reliance on digital payment protocols, and advised that valuable financial information be stored away from Internet access. Other proposed solutions include e-commerce site security certification (Garceau *et al*., 1998).

A very different type of Internet fraud to that discussed above is the *scamming* of individuals (IFW, 1999a). Online auctions were reported as the major Internet scam in 1998 (IFW, 1999b), but ever-new and inventive scams appear seemingly daily.

Possible impacts of Internet fraud include financial damage, loss of data integrity, loss of data confidentiality, and damaged company image.

The Internet security policy can include advice prohibiting employees from storing sensitive financial information on systems accessible via the Internet. Employees should be cautioned against the dangers of ordering or paying for goods and services over the Internet—particularly the giving out of cleartext personal credit card or business credit card details. Use of encryption for postings, use of filters and monitoring via firewalls, and appropriate sanctions for abuse, should be advised.

3.4.3.6 Hacking

A person or group may gain unauthorised access to an organisation's systems or data either out of curiosity or for a more harmful reason, and may subsequently cause damage. For example, hackers may steal sensitive corporate information (for example, financial data), vandalise Web sites, or "smurf" by flooding victims with data or access attempts (Sandberg, 1998), thereby bringing down networks and causing denial-of-service (as discussed in Section 3.4.3.4 earlier). Financial data stolen by hackers can be used to commit fraud (as discussed in Section 3.4.3.5).

I initially provided evidence pointing to hacking as an extremely serious and increasing security concern worldwide, in Chapter 1. A CSI/FBI survey of 163 companies reported losses of $124 million in 1998 from hacking (Koerner, 1999). A more recent CSI/FBI survey reported that 59% of the responding 643 companies experienced frequent Internet attacks over the previous twelve months (CSI, 2000). Major

U.S. institutions have been penetrated in recent years, for example the Pentagon (Neumann, 1998a); NASA (Branigin, 1991; Finucane, 2000; Neumann, 1997d); the U.S. Army (SINS, 1998); Citibank (Neumann, 1997a; CNNfn, 1998); web sites for the Associated Press, Drudge Report, C-Span and ABC (AP, 1999); web sites for the FBI, White House and Senate (CNN, 1999); the web site for the United States Information Agency (Stout, 1999); and web sites for Yahoo!, Buy.com, eBay and E*trade (Ross, 2000).

In the U.S. National Security Agency's 1997 cyberwar drill exercise, "Eligible Receiver," 35 hackers hired by the NSA broke into 36 of the 40,000 government networks within four days, demonstrating just how vulnerable systems are to hacking (Sullivan, 1999). Another example is:

In 1998, hackers attacked many networks in the US, including 14 of NASA's 15 U.S. sites (Hinde, 1998).

The profile of a hacker has been the subject of much study. Some individual hackers have gained infamy, for instance, Kevin Mitnick (Neumann, 1995) and Robert Morris (Eisenberg *et al*., 1989). Sometimes hackers form powerful collaborations which are difficult to stop, with group names such as Cult of the Dead Cow, and Hacking for Girlies (Koerner, 1999). An interesting trend has been that although in general, hackers tend to be curious network explorers, ex-employees, system crackers and techno-terrorists, an increasing number of hacking attacks are by industrial spies acting for corporate competitors (Hsieh *et al*., 1996; Kovacich, 1998; McClearn, 1999).

Hackers often use programs that are readily available on the Internet as their tools for attack—for example, Black Orifice. Hacker attacks are usually enabled by unauthorised access gained through:

- stealing of user identifiers plus passwords via:
    - unsecured gateways, using ftp or telnet services;
    - eavesdropping via 'sniffer' programs that hunt for user ids and passwords, running at network nodes while information is in transit;
    - password cracking programs; or
    - encryption key cracking;
- spoofing (forging) of IP addresses of a trusted host in order to establish a connection with a victim machine;
- exploiting weaknesses in protocols, systems and browsers to gain unauthorised entry; or
- social engineering, in which people are conned into providing access information (eg passwords)

(above list attributed to Denning, 1996; Schwartau, 2000; Valente, 1996).

Companies must not only act to prevent hacking of their own sites and computers, but also to prevent their own employees from hacking into other companies. This typically necessitates filtering, logging and monitoring of employee Internet accesses. An interesting dilemma is raised by a company monitoring its employees' attempted accesses to known hacker sites, or other suspect unauthorised site access attempts.

Conflict:

The needs of society:
protection from hacking attempts; ability to detect and apprehend hackers

vs

The needs of the company:
attempting to protect external companies from hacking attempts by their own employees, and to protect themselves from liability for hacking damage

vs

The needs of the employee:
trust displayed by employers; freedom of Internet use;
freedom from logging of Internet accesses and monitoring

Non-technical countermeasures include maintaining an up-to-date list of valid users and administrators, limiting the number of super-users, removing all non-essential accounts, reviewing audit logs and installing security patches (Valente, 1996).

Possible impacts of 'hacking' include loss of data confidentiality, loss of data integrity, denial-of-service, financial damage, damaged company image, poor employee morale, lost productivity and disruption to work.

The Internet security policy can include advice prohibiting employees from storing valuable corporate data on systems accessible via the Internet. Employees should be educated about safeguarding their user ids and passwords, especially from social engineering attempts to capture them. Employees should be advised to change their passwords frequently, and never to transmit user ids and passwords in cleartext. Employees should also be informed as to the actions to take if a hacking attempt into the company network is suspected. Employees should be cautioned against attempting unauthorised accesses into external systems, attempting accesses to known hacking sites, and hacking altogether. They should also be informed of related filtering, logging and monitoring.

3.4.3.7 Inaccurate advertising

An organisation or employee may consciously 'advertise' within email, Web sites, or other posting mechanisms, without due authority, in such a way as to appear to represent an official view. The content of this information may be inaccurate, in an organisational context—for example employees may order goods without authority (Woodward, 2000). In one case, a security analyst at a large Australian bank was regularly contributing his own opinions, without a disclaimer, to the Secure Electronic Transactions protocol (SET) mailing list, acting as if his opinions were those of his employer (the bank). He was reprimanded after his exploits were reported, and asked to include a disclaimer with each future posting (source: anecdotal).

Absence of disclaimers on email is causing misrepresentation of official company positions.

Conflict:

The needs of society:
clear distinction between employee opinion and official company position

vs

The needs of the company:
clear distinction between employee opinion and official company position;
freedom from legal liability for employee Internet postings

vs

The needs of the employee:
freedom of Internet speech

Possible impacts of 'inaccurate advertising' include damaged company images, and even litigation.

The Internet security policy can include advice as to acceptable email content—in particular, not to present personal opinion as official company position. Mandatory disclaimers can be advised, if the company so decides. Use of filters and monitoring via firewalls, and appropriate sanctions for abuse, should be advised.

3.4.3.8 Inappropriate email

Companies or employees may send or receive unwanted or unsolicited email (*junk email*), harassing, discriminatory or defamatory email (*flame email*) or excessive unwanted email (*spamming*) (Erickson, 1996; Moulton, 1998; Sipior and Ward, 1999).

Junk email and *flame email* include advertising material, offensive messages and jokes, sexually explicit materials, defamatory statements, chain letters and pornographic images (Moulton, 1998). *Junk email* such as advertising material and chain email wastes recipients' time, not to mention Internet resources. Such email also constitutes a daily annoyance. *Flame email* containing harassing, discriminatory or defamatory statements may incur legal suits (Sipior and Ward, 1999), or employee dismissal (Carson, 2000b). In 1997, Norwich Union was ordered to pay 450,000 English pounds and to apologise for a libellous email to a private health care group (Moulton, 1998).

A 1999 Gartner Group survey reported that some 175 million spam emails were received each week, and that over 90% of Internet users receive junk email each week (Weaver, 1999). 97% of the users reported that they did not appreciate receiving the email.

An issue which arises is how to determine what is offensive Internet email, with differing standards for offensiveness between different cultures.

For example, semi-nude advertising is commonplace and acceptable in France and Brazil, but unacceptable in Saudi Arabia and Iran (Moulton, 1998). Moulton also points out the availability of text-filtering software that scans incoming email for offensive words, 'alarming' an authority on detection.

Conflict:

The needs of society:
email compliance with differing national and cultural standards for communications decency
vs
The needs of the company:
freedom from accusations of inappropriate email; freedom from legal liability; employee protection
vs
The needs of the employee:
freedom of email speech; freedom from receipt of inappropriate email; freedom from legal liability

Spamming (excessive unwanted email) of Internet users is another worrying risk. It is disturbing to learn that many spammed Internet users retaliate against spamming via mail-bombings and denial-of-service "flooding" attacks (Pitkow and Kehoe, 1997). A spam email, when read, can even trigger an unexpected visit to a hostile Web site (Brazil, 1997). Half to three-quarters of all spam email contain forged email addresses for replies, thereby blocking tracking of the sender (Neumann, 1997c).

Mail-bombing is indicative of a decline in civility between Internet participants
(Highland, 1996)

Spamming may also be accidental. Fischer (1998) reported accidental spamming when one thousand members of the U.S. National Association of Broadcasters were spammed with email due to a misconfigured mailing list server.

The Gartner Group 1999 survey estimated a staggering $255 million a year loss due to either junk email or spamming (Weaver, 1999).

One technique to control deliberate spamming is “anti-spam filtering”, where the ISP (through which the spammer manoeuvred) blocks future email from the offending email address for a period of time (for example, a week). It is unknown at this stage just how effective this technique is at preventing further attacks by the spammer. Spammers can get around this technique, for example, by rotating sender addresses (Weaver, 1999). Three out of four respondents in the Gartner Group study believed ISPs should regulate spamming and junk email, and ISPs such as Hotmail, MindSpring and Earthlink are investigating and implementing possible anti-spam techniques (Weaver, 1999).

Possible impacts of "inappropriate email" include employee harassment, employee embarrassment, litigation and resulting financial damage, lost productivity costs, loss of privacy and denial-of-service.

The Internet security policy can include advice to employees as to how to act if they are harassed, spammed, or sent other unwanted or unsolicited email, including reporting the event to a designated authority. Employees should also be warned not to send unwanted, unsolicited, harassing or spam email to others. Use of filters and monitoring via firewalls, and appropriate sanctions for abuse, should be advised.

3.4.3.9 Low quality data

The quality of data being exchanged via the Internet is questionable, in that it may be inaccurate, untimely, inconsistent, dubious, a scam, a harbinger of unfair trading, or merely opinion rather than fact (Mathieu and Woodard, 1995).

(i) Inaccurate data

Inaccurate data may be issued or accessed during Internet usage by a variety of means. Organisations or employees may accidentally issue transactions or postings which contain incorrect data (for example, by inclusion of an inaccurate data field). Another way in which inaccurate data manifests itself is that initially correct information, in the form of business transaction data or communications, may become altered in transit, either deliberately—after eavesdropping (also known as 'sniffing' or 'snooping') followed by alteration, or hacking—or accidentally via imperfect technology (Mathieu and Woodard, 1995; NIST, 1994b). Forged email content as well as impersonation of email send addresses are further manifestations of inaccurate information (NIST, 1994b).

(ii) Untimely data

Outdated (i.e. untimely) information may reside on Web sites, and be taken as gospel by employees. This may be due to a site owner either not bothering to update their site, or losing their Web site access privileges. Sometimes outdated information remains on sites due to an inability to cope with a sudden spate of accesses. For example, in the Wall Street stock market turmoil of October, 1997, NASDAQ Internet trading systems were unable to cope, displaying incorrect last sale prices which were picked up and reported by reliant mutual funds (Bellovin, 1997).

(iii) Inconsistent data

Conflicting versions of data may exist on a corporate system—for example, several differing versions of a database. Employees may accidentally access data from an old version.

(iv) Dubious data

The content of some Web sites is of a restricted or objectionable nature—for example, child pornography sites.

Attempts to regulate the content of Web sites through metadata labelling schemes and associated, complex Protocol for Internet Content Selection (PICS) schemes are being made around the world, so that Internet users may avoid being exposed to offensive Web site content. Software to filter out known dubious site addresses is available (for example, NetNanny, SmartFilter (Moulton, 1998)), and some official bodies are maintaining lists of dubious sites for use by companies in site blocking. Moulton (1998) recommends site blocking of such offensive sites as company policy.

American ISPs were increasingly being found *not liable* for the quality of Internet content which passed through their servers (EPIC, 1997d), however in other countries such as Australia and the UK, ISPs may

be found liable. In Australia, a new law will find Australian web site owners liable for offensive content (ABA, 1999; AGD, 1999c).

Conflict:

The needs of society:
freedom of speech on the Internet
vs
The needs of the company:
only unobjectionable Internet content to be accessible by their employees; business-only Internet usage
vs
The needs of the employee:
freedom of Internet usage; freedom of (access to Internet) information

(v) Scams

Scams to gather personal information about Internet users, or to rake in users' money (fraudulent scams), are increasingly appearing in unsolicited email, on Web sites or in other postings. (Note: Scams were also discussed earlier under 'fraud' (Section 3.4.3.5)). An example scam was the software pirate found selling illegally obtained software over the Internet (Branton, 1997).

59% of respondents in one survey cited merchant illegitimacy on the Internet as a major online shopping concern (Aldridge *et al*., 1997). Due to heavy concern with scams, various initiatives have been taken. For example, in Australia, a special day was organised in 1997 to scan the Internet for scams mounted via Web sites (Sinclair, 1997a). Janal (1998) advises companies how to protect themselves against scams. As discussed under 'fraud' in Section 3.4.3.5 earlier, various parties have set up web sites to help protect consumers against scams (for example, Antifraud.com, 1998).

(vi) Opinion-based data

Subjective opinion, rather than fact, may be transmitted by organisations or individuals, via postings, as mentioned earlier (see Section 3.4.2.7 in this Chapter).

(vii) Site of unfair trading

In response to rapidly rising complaints about possibilities of unfair trading on the Internet, an Australian commission recommended, at a corporate level, that companies be classified as 'quality traders', by exhibiting site features which include corporate service charters, adequate and accurate information provision, corporate complaints handling systems and corporate compliance systems (ACCC, 1997). A September 1997 meeting of Australia's fair trading ministers decided to devote its first national consumer day to Internet-related problems (Sinclair, 1997a).

Possible impacts of this risk include litigation and resulting financial damage, damaged employee morale, financial loss, damaged company image.

The Internet security policy can include advice to employees to validate or verify site content and postings where inaccurate or untimely data are suspected. Employees can be warned to be wary of email received form unknown sources. Employees should also be warned that certain dubious sites have been blocked by firewall or other filtering mechanisms, and that attempts to access such sites are being monitored. A list of sites being blocked should also be published.

3.4.3.10 Non-business usage

There is a risk that employees may use the Internet for non-business activities such as personal surfing of the Internet, Internet relay chatting, downloading games and images, personal use of email, personal use of other tools (for example, videoconferencing), netphones and newsgroups. Many companies are now aware of significant non-business Internet usage, and are warning employees of increased monitoring to control such misuse. There has been increasing company action on non-business Internet usage, for example in October 1999, Xerox Corp fired approximately 40 employees for Internet non-business usage.

A comment about personal email in the workplace, from an experienced U.S. businesswoman, illustrates the non-business use quandary:
"I think that email on the job should be just like any other personal things. Like phone calls. Personal calls should be made on personal time. Of course, there is the occasional emergency call that has to come in. When you are off the clock like lunchtime, should you choose to use your time taking care of personal email, then it should be totally private. I hear that email is the biggest corporate time thief going. That productivity is being seriously affected in the work place. If that is the case, then personal email is certainly the business of employers!" (Allison, 1998).

One Australian employee of a large, well-known company told me in 1998 that he spent at least four hours per day surfing the Internet for personal reasons, and charged that time to the company's clients for legitimate purposes—thereby penalising the clients.

Although the company itself strictly monitored personal usage, this employee worked at a client site where many of the client's employees surfed the Internet for "legitimate" reasons (eg research), and were not monitored. Hence, the remiss employee's personal surfing had gone unmonitored and undetected. His company, however, subsequently broadcast a warning to all employees about non-business Internet usage, warning that email may need to be randomly scanned to check for compliance if non-business email misuse continued, and that monitoring of Internet accesses was being stepped up.

Of increasing concern, then, is the conflict between societal, employee and company needs represented by non-business Internet usage:

Conflict:

The needs of society:
free flow of Internet traffic
vs
The needs of the company:
controlled, business-only employee Internet usage; maximised employee productivity;
legality of Internet usage; effective and efficient Internet business usage;
minimal Internet traffic delay;
vs
The needs of the employee:
unrestricted Internet usage

Possible impacts of 'non-business usage' include lost productivity, Internet traffic delays, and the spreading of a poor work attitude throughout the workplace.

The Internet security policy can include advice to employees of any restrictions regarding non-business Internet usage—typically, total prohibition of, or restricted time limits, on personal use. Use of filters and monitoring via firewalls, and other surveillance methods, as well as appropriate sanctions for abuse, should be advised.

3.4.3.11 Pirated media

An employee may download software or data in breach of copyright or licensing laws. In 1997, software piracy (much of which is achieved by downloading software from the Internet) was estimated at $11 billion per year, and was being condoned by leading figures such as university academics, according to a survey of attitudes to piracy (Lawrence, 1997). Bulletin boards are the most common method for distributing software illegally on the Internet (Saunders Thomas *et al*., 1997).

Some companies are centralising their networks with workstations consisting of dumb terminals rather than PC's. Hence, with all software residing on the central mainframe, employees are not able to download Internet software illegally. This unfortunately slows down worker productivity at the workstations, as each time software is required it must be loaded from the mainframe onto the workstation and then executed.

A conflict arises from the piracy risk:

Conflict:

The needs of society: absence of software piracy vs *The needs of the company:* absence of software piracy; freedom from liability. vs *The needs of the employee:* unrestricted Internet usage; required software unavailable

Possible impacts include the illegal existence of pirated software on the company's systems, legal actions, financial damage from successful legal suits, and sullied employee and company images.

The Internet security policy can include advice to employees not to download software illegally. It can also advise employees how to obtain required software through proper channels. Use of filters and monitoring via firewalls, and appropriate sanctions for abuse, should be advised.

3.4.3.12 Theft of information

Information may be accessed and "stolen" from an organisation via a variety of means, such as hacking into systems and viewing corporate data, eavesdropping at network nodes, copying Web site information without gaining owner permission, and downloading software illicitly (Internet software piracy) (Bernstein *et al*., 1996; Bhimani, 1996; Denning, 1996; EPIC, 1998b; Jackson, 1998; McClearn, 1999).

Theft of financially sensitive data such as credit card details from corporate databases, Internet software piracy, user id and password theft, and theft of other confidential corporate data, are now rife.

(Bhimani, 1996)

A CSI/FBI 1998 study reported information thefts resulting in individual losses between $300 and $25 million US, totalling $300 billion for the year, in the U.S. alone (McClearn, 1999).

Unauthorised data retrieval (theft of information) was listed as one of the top three concerns in a survey of Internet user concerns (Aldridge *et al*., 1997; Internet Security Survey Results, 1996). Data theft via hacking is enabled by means of unauthorised access through FTP, NFS, remote log-in and flaws in

systems software (Bernstein *et al*., 1996). Of increasing concern is the fact that corporate data may be corrupted or deleted once they have been accessed (Bhimani, 1996)—a very damaging type of data theft. A perturbing new concern is that:

---

a rival firm's employees may attempt to view useful information within another firm's systems, without authorization, with the aim of gaining a competitive advantage.

Indeed, an increasing number of industrial spies are acting for such corporate competitors, and are hacking into systems and viewing (hence stealing) strategic information (Hsieh *et al*., 1996; McClearn, 1999). Some experts claim more and more corporate-inspired hacking is being funded by government and business (McClearn, 1999). Jackson (1998) examines how international bodies have been changing the ways in which law protects confidential business information and trade secrets, given the transjurisdictional issues involved.

The Internet security policy can assign data owners responsibility for protecting owned information assets (Bernstein *et al*., 1996). The policy can also prohibit employees from storing valuable corporate data on systems accessible via the Internet. Employees should be advised to safeguard their user ids and passwords—for example, by not transmitting them in cleartext. Employees should be advised regarding safe storage and destruction of information. Employees should be given instructions for reporting suspected theft of information from other companies, in particular, copying of Web site information without permission. Use of encryption for postings, use of filters and monitoring via firewalls, and appropriate sanctions for abuse, should be advised.

3.4.3.13 Summary remarks

Both deliberate and accidental types of risks have been included in the Internet risks model, although the difference between deliberate and accidental is often extremely difficult to determine. For example, Vanbokkelen (1990) remarked that "Security is subjective; one site might view as idle curiosity what another would view as a hostile probe".

I make an observation about the Internet risks model at this point—that there is a significant amount of overlap between the different risk types. For example, “hacking” of financial data may also constitute “fraud” as well as “theft of information”. (As one policy which addresses all these three risk types, I have suggested that employees should be warned not to store valuable information on systems which are accessible via the Internet.) Despite such overlap, I believe each risk type is different enough to warrant separate classification.

Losses from Internet risk occurrences can be severe. I reported many survey results in Section 3.4.3, showing large losses for all kinds of risks.

"The Internet risks described in this section are not going to disappear in the foreseeable future, nor, therefore, are the losses."
(Neumann, 1996).

The Internet risks described in this section, *if assessed as significant for a company*, should be addressed in the company's Internet security policy along the lines that I have suggested for each of the Internet risk types described in this section (Section 3.4.3).

Summary of Internet security policy advice: Employees should be made aware of the significant Internet risks, consequent losses, policies for recommended behaviours, actions, remedies, prohibitions and consequences for misuses and abuses, through the Internet security policy. Companies should also stipulate technical Internet security requirements for addressing significant Internet risks, within the Internet security policy.

3.4.4 Organisational factors in Internet security policy

The Internet security policy will be constrained by organisational factors such as the company's business requirements, internal information security infrastructures, management attitudes and overall information security posture (Sutterfield and Schell, 1997) as summarised in Table 3.2 and elaborated below.

Organisational Factors in Internet Security Policy	Source
Organisational objectives	3.4.4.1
Internet security infrastructure	3.4.4.2
Management commitment	3.4.4.3
Internet security management programme	3.4.4.4
Internet security awareness	3.4.4.5
Policy integration	3.4.4.6
Principles for Internet security and policy	3.4.4.7

Table 3.2 Organisational factors in Internet security policy

3.4.4.1 Organisational objectives

Computer security should support the mission of an organisation, according to NIST's Generally Accepted Principles and Practices for Security Information Technology Systems (NIST, 1996b). Accordingly, an Internet strategy for the company should be developed from the company's *organisational objectives*—a process known as alignment (Brockway, 1996; Lawrence *et al*., 1996; Logan, 1995; Logan and Logan, 1996; Miers *et al*., 1996; Poon and Swatman, 1995; 1996). The Internet strategy should include articulation of intended business usages of the Internet (see Bloch *et al*.'s (1996) business usages below, for example). (Note, some authorities have recommended an e-commerce strategy (rather than an Internet strategy), for example, META Group, 2000).

The Internet strategy can be used as a guide to acceptable Internet business usages, which should form part of the Internet security policy. The acceptable business uses will in turn help define the Internet services—for example, email, ftp and telnet——that are required to support these business uses (Griffiths, 1996). Secure use of each of these services should also be specified in the Internet security policy.

Experts have proposed various classification schemes for business uses of the Internet. For example, Bloch *et al*. (1996) classified ten different business Internet uses by "source of business value":

- improvements in: product promotion, new sales channel, direct savings, time to market, customer service, brand image;
- transformed organisation in: technological and organisational learning, customer relations; and
- redefined activities: new product capabilities, new business models.

Permitted or denied user accesses to internal and external information required to facilitate these business uses must also be defined. The defined accesses can later be permitted or denied via *firewalls*, which filter inbound and outbound accesses according to predefined firewall rules (Griffiths, 1996; D'Alotto, 1996; Drake and Morse, 1996).

Hence, organisational objectives directly influence the Internet security policy, as recommended by Bernstein *et al*. (1996).

The Internet security policy should articulate acceptable and unacceptable business usages of the Internet in line with the Internet strategy and organisational objectives. The policy should also specify the Internet services required to support such usages, and secure use of them, for individual users and user groups. The policy should specify permitted or denied inbound and outbound accesses of various types, for individual users and user groups (for example, to specific Web sites, networks and Internet services).

3.4.4.2 Internet security infrastructure (Internet security plan)

The organisational Internet security infrastructure, which is referred to by some experts as an *Internet security plan*, should include: an Internet security philosophy, an Internet strategy (see Section 3.4.4.1), constitution of the policy development and maintenance team, standards, Internet architecture, storage of corporate data, Internet services and software, and other Internet staffing requirements.

(i) Internet security philosophy

A *philosophy* for Internet security for the company can be based on one of Aldridge *et al*.'s (1997) recommended Internet security postures for governing permitted Internet accesses for employees:

- paranoid: everything forbidden, no connection;
- prudent: everything forbidden except what is explicitly allowed;
- permissive: everything allowed except what is explicitly forbidden; or
- promiscuous: everything allowed.

The Internet security posture adopted will affect the level of restrictivity specified throughout the entire policy.

(ii) Internet strategy

An Internet strategy is not only a statement of the intended business usage of the Internet (see Section 3.4.4.1) but also a statement of the position of the organisational Internet security infrastructure within the overall organisational information security infrastructure. The position of the Internet security policy within the overall company policy infrastructure is an important part of this statement. Guttman and Bagwill (1997) and others (for example, RiskWatch, 1999) recommended that:

The Internet security policy should be a sub-policy of the Corporate information security policy (CISP).

The CISP contains the complete information security requirements for the organisation, in the form of layers of policies (subpolicies) representing progressively more refined and progressively more rule-like policies, addressing different audiences and different aspects of information security (Abrams and Bailey, 1995; Olson and Abrams, 1995). Guttman and Bagwill (1997) classify CISP sub-policies as issue-

specific, system-specific or program-specific, designating the Internet security policy as an issue-specific sub-policy of the CISP.

(iii) Development team

Aldridge *et al*. (1997) discuss use of in-house staff, consultants or outsourcing for the development of Internet security and policy. Time, budget, personnel availability and skill are factors that will influence the constitution of the development team.

(iv) Standards

Information security management standards such as Australia's recently revised AS/ NZS 4444 standards for Information security management—Code of practice for information security management, 1999—can be employed to achieve a higher level of Internet security. Emerging standards or guidelines in Internet security management should also be used. Indeed, a major outcome of this research project is a framework for Internet security policy for companies, which is expected to be of value to an organisation aiming for more effective Internet security management.

(v) Internet architecture, services and software; storage of corporate data

The required Internet configuration must be specified, as suggested by Bernstein *et al*. (1996):

- considering interoperability between planned Internet activities (eg e-commerce), networks used (eg Ethernet), computing platforms (eg UNIX), network tools and standards;
- selecting a sufficiently secure protocol (eg TCP/IP is not the most secure protocol);
- selecting heterogeneous computing platforms;
- determining required security tools (eg RACF);
- determining network architecture;
- determining the location of sensitive business data; and
- determining acceptable network bandwidth.

(vi) Staffing requirements

Staffing requirements for administration and maintenance of the company's Internet infrastructure must be determined. Wilson (1996) discussed the importance of distributing Internet security tasks and responsibilities amongst all kinds of personnel, so that overall responsible behaviour is obtained. He also discussed the importance of a stable base of resources, in order for the infrastructure to function effectively.

Companies need to be aware of any new Internet security infrastructure trends, such as use of centralised networks with dumb terminals as workstations to achieve reduced piracy and virus occurrence.

The Internet security policy should include appropriate details about the Internet security infrastructure—to include the Internet architecture, Internet tools, location of corporate data, Internet security posture, and staffing requirements. Employees can be advised as to proper use of each of the Internet tools, and secure handling of the specific architecture selected.

3.4.4.3 Management commitment

Senior management's commitment to protecting a company's systems has long been considered essential to assuring successful information protection (Bernstein *et al*., 1996; Guttman and Bagwill, 1997; Stanley, 1997; Wilson, 1996). Management commitment was identified by Stanley (1997) as a key information security challenge for the new millennium.

Evidence points to a serious lack of management commitment to information security and Internet security.

Senior management are typically uninterested in information security until a breach occurs (Kwok, 1997; Marro, 1995), and are under-represented in most working parties in information security: In one survey, only 30% of over 150 leading European companies included senior managers as chairpersons of key information security working groups (Stanley, 1997).

Management commitment to information security can, however, be obtained through a variety of tactics, as suggested by Wilson (1996):

- selecting real-world issues that management can understand, then selling them on addressing those issues;
- briefing senior managers about their important contribution to achieving security; and
- referring to legal liabilities in certain situations.

Guttman and Bagwill (1997) state that if a manager is truly convinced about a policy, his/her feelings will filter down to employees through informal channels. Stanley (1997) highlighted the need for research into information security performance metrics which can be used to inform management of a company's existing information security problems. The above ideas can be explored to secure management commitment to Internet security and policy.

The Internet security policy should ideally indicate management commitment to the policy and to Internet security. Management expectations of acceptable employee behaviour in Internet usage should be clearly

articulated in the policy (Moulton, 1998), and should be supported in a variety of ways. For example, adequate resources (eg budget and skilled staff) must be provided by management to properly support the policy (Bernstein *et al*., 1996). A weak link in the managerial chain from top to bottom in a company can seriously affect the policy's chances of success. Hence, the Internet security policy should be introduced to employees in a manner that assures them of unqualified management support—from top to bottom (NIST, 1994a). Senior managers should ideally issue the policy (Bernstein *et al*., 1996), and representative managers should attend policy awareness sessions.

The Internet security policy should clarify management expectations for employee behaviours and actions. It should also include a statement about the various forms of policy support that will be provided by management.

3.4.4.4 Internet security management programme

The Internet security policy is only one component (albeit a key one) of an Internet security management programme, which provides critical support for the policy (Bernstein *et al*., 1996; Lichtenstein and Swatman, 1997a; 1997b). Bayuk's (1996) and Doddrell's (1995) recommendations for an information security programme suggest that an Internet security management programme be composed of policies, procedures, training and awareness activities, access restrictions and monitoring, compliance procedures, an Internet security plan, and a range of Internet security technologies (see also Lichtenstein and Swatman, 1997a; 1997b).

Additional low-cost managerial measures include physically protecting the central corporate data processing and Internet facility, personnel screening, back-up procedures, contingency plans and data recovery (Faroughi and Perkins, 1996; Fried, 1995). Procedures for the correct disposition of sensitive corporate data—ie clearing and purging of unrequired classified data from Internet accessible servers—are required. Regular and thorough Internet access audits can be carried out by identifying all Internet users and conducting an audit trail to determine their accesses over a period, perhaps through using special-purpose software (Faroughi and Perkins, 1996).

Wilson (1996) discussed the importance of distributing Internet security tasks and responsibilities amongst all personnel groups, so that overall responsible behaviour is obtained. He also discussed the importance of a stable base of resources in order for the programme to operate effectively.

The programme must be dynamic, due to a rapidly changing Internet world. Sutterfield and Schell (1997) suggest a process of incremental improvement of the programme:

- implementing a certain level of Internet security;
- monitoring Internet security regularly;
- evaluating Internet security; and

- implementing improvements.

The Internet security policy should include statements about all components of the Internet security management programme. The policy itself is a key component of that programme.

3.4.4.5 Internet security awareness

Information security awareness is essential in any information security approach (GAO, 1998; Stanley, 1997). Internet security awareness for employees is part of such overall awareness.

Employees may refuse to accept accountability for their Internet actions without adequate Internet security awareness activities and measures in place.

As the Internet is a relatively new business tool, employees need a lot of assistance in being made aware of, and understanding, written Internet security policy (including the IAUP), via: Internet security awareness sessions, training sessions, presentations, written materials, screen messages on log-on, videos, strategically placed wall posters, guest speakers, panels and newsletters (Bernstein *et al*., 1996; Guttman and Bagwill, 1997; NIST, 1994a; 1996a; Spurling, 1995). Periodic simulated attacks can also promote awareness (Benjamin *et al*., 1998). At awareness and training sessions, the Internet security policy can be clarified. For example, terms such as "reasonable and prudent precautions" should be explained (Branstad *et al*., 1995).

Educational information disseminated should include plentiful examples of acceptable and unacceptable Internet usages, cautionary messages about downloading unapproved software, protective configuration advice and remedies based on risk loss control or mitigation. Employees should be educated about Internet risks and possible losses to the system, to themselves, or to other Internet participants—risks incurred through either accidental misuse or deliberate abuse (Aldridge *et al*., 1997). Training should emphasise specific employee roles and responsibilities.

Sutterfield and Schell (1997) suggest a stronger awareness approach. They believe in education by initially informing employees about recent and damaging Internet security incidents, break-in statistics and impacts, then drawing employee attention to the relevant policy regulations. Woodward (2000) advises “selling” the policy to employees via awareness sessions, to ensure the policy’s success.

People must be assigned responsibilities for Internet security awareness, including the IT security manager, the IT function, business unit managers, the corporate training function and the human resources department (Bernstein *et al*., 1996).

The Internet security policy can include details of Internet security awareness activities and measures.

3.4.4.6 Policy integration

Complementary information security policies, such as the Corporate information security policy (of which the Internet security policy is a sub-policy) reinforce the Internet security policy, as do standards, guidelines and procedures (for example, procedures for the development of individual employee Web pages). Internet users may also need to conform to relevant ISP policies. The Internet security policy should also be integrated with other relevant organisational policies, such as the organisation's Code of Conduct, in order to ensure consistency between policies, and therefore enhance the policy's chances of success (Guttman and Bagwill, 1997).

Griffiths (1996) noted that other company policies may need to be changed because of the new Internet security policy—for example modem usage policy may need to be centralised to avoid clandestine links to the Internet.

The Internet security policy should be consistent with internal policies, standards and guidelines as well as relevant ISP policies, and should refer employees to all these policies for required compliance.

3.4.4.7 Principles for Internet security and Internet security policy

Bernstein *et al*. (1996) suggest the following characteristics for an Internet security policy:

- *flexibility*: the policy must accommodate future technology changes and new Internet risks, at least in its structure;
- *pertinence*: the policy must reflect the company's current objectives;
- *applicability*: the policy must reflect the company's computing environment;
- *implementability*: the policy should be implementable without too much trouble;
- *timeliness*: the policy should be up to date;
- *cost-effectiveness*: the policy should be cost-effective against the costs of risk occurrences;
- *enforceability*: the policy should be enforceable in the current environment; and
- *integratibility*: the policy should be integrated with other company policies.

It is also important in managing Internet security for modern types of organisations for a company to develop corresponding Internet security. Modern organisations with non-hierarchical and non-bureaucratic structures have been collectively termed "adaptive organisations" (Baskerville, 1988)—by

dint of sharing an important, common characteristic—the ability to adapt rapidly to changing circumstances and requirements.

It has been suggested that information security needs and principles governing adaptive organisations differ from those governing more traditional, bureaucratic types of organisations (Baskerville, 1988; 1997; Lichtenstein, 1995a; 1995b; 1996e). In earlier work, Lichtenstein (1995a; 1995b; 1996e), I developed a set of information security principles for adaptive organisations, which can readily be extended to cover Internet security and policy. For example, Internet security policy should feature *human involvement*, as the latest technological controls may not be able to handle new risks in the rapidly changing Internet environment.

An Internet security policy should exhibit the characteristics of flexibility, pertinence, applicability, implementability, timeliness, cost-effectiveness, enforceability, and integratibility. An Internet security policy for modern organisations should reflect the special information security and Internet security needs and principles which have been determined for such organisations.

3.4.5 Administrative factors in Internet security policy

Administrative and operational tasks need to be considered and defined. Procedures for applying, monitoring, auditing and updating Internet security policies are required (Branstad *et al*., 1995; Faroughi and Perkins, 1996; Guttman and Bagwill, 1997). Procedures are also required for publicising the policy, establishing and maintaining Internet access controls, performing risk assessments, training Internet users and developing contingency plans. Good administration is critical. Network administrators must be a highly skilled team armed with the latest technology, in order to carry out basic services such as intrusion detection, incident response, security evaluation, network mapping and network usage monitoring (Sutterfield and Schell, 1997).

The policies within the Internet security policy should be feasible in light of existing administrative constraints, such as the availability of skilled staff, and resources for implementing the policies as procedures. Procedure definitions or referrals to these should be included, wherever possible.

3.4.6 Legal issues in Internet security policy

An organisation should take into account national and international laws in its policies, to avoid liability in Internet usage and security incidents, and in order that their employees can be duly informed with respect to legal Internet usage. Companies could face major litigation, for example, from temporary shutdowns due to distributed denial-of-service attack such as those that occurred in February, 2000 (Krebs, 2000). Overly (1999) stresses the role of Internet policies in avoiding legal liability.

Legal issues in Internet usage include copyright and licensing, fraud, theft, terrorism, privacy, trademark and trade secrets, legal evidence, jurisdictional issues, and the publication and accessibility of offensive material. Legal issues in Internet use are discussed in Cavazos *et al*. (1994), Foster (1997), O'Connell (1997), Pattison (1997), Saunders Thomas *et al*. (1998) and Smith (1996).

The approach by countries to date has involved countries legislating each separate legal Internet concern with limited international co-ordination. An example Internet law is Australia's new Electronic Transactions Act (AGD, 1999d), which enables business and the public to use electronic communications in interactions with, and legal obligations to, Government agencies. The law attempts to equate electronic transactions with paper document transactions. The law is consistent with the U.N. model law of UNCITRAL (1996), demonstrating an attempt at global standardisation.

Because there are so many differences in Internet laws between countries at present, and so much off shore Internet crime which cannot be prosecuted in the victim's country as a result, US Attorney General Janet Reno recently proposed an online network of international law-enforcement agents to monitor the Internet, and bring international criminals to justice (Greene, 2000). The US Department of Justice (2000a) recently released a report highlighting the need for changes to existing laws, in order to counter global unlawfulness on the Internet, and has also launched a Cybercrime web site for cyber crime awareness and reporting purposes.

The legal issues I discuss here are summarised in Table 3.3 and elaborated below. As mentioned above, this is not a *complete* model of legal factors in Internet security policy. Many other legal issues, though undeniably important, have been omitted here, as not only is the topic very large in its own right, but this thesis is solely concerned with illustrating the impact of Internet legal issues on Internet security policy.

Selected legal factors in Internet Security Policy	Source
Cryptography laws	3.4.6.1
Censorship laws	3.4.6.2
Defamation laws	3.4.6.3
Intellectual property and copyright laws	3.4.6.4
Privacy laws	3.4.6.5
Reliance on content	3.4.6.6
Self-help remedies	3.4.6.7
Transjurisdictional issues	3.4.6.8
Legal liability	3.4.6.9
Contracts	3.4.6.10
Evidence	3.4.6.11

Table 3.3 Selected legal factors in Internet security policy

3.4.6.1 Cryptography laws

Weak encryption technologies for encrypting data, including key escrow and key recovery schemes, were previously legislated by the U.S., in order to enable law enforcement bodies to read data where necessary—thereby constituting a breach of privacy for other countries and communities (Horning *et al*., 1998). This situation has recently been reversed (Clausing, 2000), in line with the European Directive on Electronic Signatures (Baker & McKenzie, 1999).

Companies must be aware of current cryptography laws when setting encryption policy.

3.4.6.2 Censorship laws

The controversial issue of Internet censorship is a human issue as well as a legal issue. In this section, I will be concentrating on the legal aspects of Internet censorship, while in Section 3.4.8.3 I will be focussing on the human aspects.

Censorship laws have been legislated in various countries in order to limit restricted and objectionable material on the Internet.

In particular, such laws are aimed at preventing defamation, access by minors to unsuitable materials, and harassment of individuals. However, many individuals and groups regard censorship laws as counter to democratic principles of "freedom of speech" and "privacy rights", and are providing vigorous opposition. Neely (1995) illustrated these objections by pointing out a powerful public argument for allowing uncensored, private consensual electronic interchanges, such as personal email between boyfriend and girlfriend.

Some countries have recently legislated controversial Internet censorship laws, for example, Australia has the Broadcasting Services Amendment (Online Services) Act 1999. This law aim to prevent adults gaining access to materials deemed unsuitable for either themselves, or minors, in accordance with Australian film and video classification standards. The law has severe ramifications for service providers, who now must not store such content on their servers once the offensive content has been reported to the Australian Broadcasting Authority (ABA) and rated unsuitable.

The Act revolves around industry self regulation via industry-specific Codes of Practice being registered with the ABA. Each industry must write its own "decency" rules and its member companies' Web site content must comply (Hogan and James, 1997). Offensive private email is considered to be already prohibited by the *Crimes Act 1914*, Section 85ZE (Hogan and James, 1997).

In the United States, there not only exists the controversial Communications Decency Act of 1995 (CDA) operating in conjunction with the Telecommunications Act of 1996, which has been overturned several times, but also the new Children's Internet Protection Act 1999.

Despite the U.S. censorship law (CDA), ISPs in the U.S have not yet been held liable for objectionable content on their servers. Their claim that they do not scan content, and cannot be expected to, has been upheld in court.
(EPIC, 1997d)

In fact, the U.S. Supreme Court's June 1997 ruling in favour of the American Civil Liberties Union (ACLU) in *ACLU v. Reno* made a mockery of the CDA. The court ruled that the CDA was an unconstitutional restriction on free speech. The landmark decision was regarded as a victory for "freedom of speech on the Internet", and the future of the CDA was questionable (ACLU, 1997; Beeson *et al*., 1998).

In the U.S., cases continue to be heard which call into question various limitations of the CDA and the related Telecommunications Act of 1996. For example, in the case *Kathleen R. v. City of Livermore*, TechLaw (2000a), a woman has been suing a library for not filtering out pornographic sites that her

young son gained access to via the library computer Internet connection. The defence has argued the library was not liable, as it was acting as a provider or user of an interactive computer service, thereby excusing it from liability under Section 230 of the Telecommunications Act. The case has been ongoing since 1998.

Internet censorship laws could use Internet content classification schemes for feasible monitoring of content. In these kinds of schemes, Web sites are classified either by the Web site publisher or by a third party group. There are various attempts being made to devise and implement such schemes (for example, the PICS platform).

Companies need to keep up to date with the latest censorship laws and content classification schemes, in order to devise an Internet security policy and choose technologies to avoid employer liability.

The policy should inform employees of the existence of selected Internet censorship measures such as checking of internal web site content for appropriateness, company filtering of internal attempted accesses to external objectionable sites, random human scanning of outbound email for objectionable content, or automated scanning of all outbound email for objectionable content.

3.4.6.3 Defamation laws

Companies must ensure that they do not hold defamatory material on their servers, as they will be held liable for such material. Newsgroups hosted by a company's servers may contain defamatory material, leading to company liability—currently a very active area of online litigation (Smith, 1997). If an employee posts email containing defamatory comments, the company may be liable rather than the employee (Farrow, 1998; Moulton, 1998). For example, the State of Indiana in the U.S. did not take action when a supervisor in a particular company sent objectionable email to junior employees in the company, and the company itself was then held liable for the behaviour of the supervisor (Moulton, 1998).

In the *Stratton Oakmont v Prodigy Services* Company case, Prodigy (an online provider) exercised editorial control over the contents of discussion forums and was held liable for some defamatory content (Smith, 1996). To avoid liability, online providers and ISPs have been less willing to moderate content passing through their servers (EPIC, 1997d). In the U.S., online providers continue to be sued, with Section 230 of the Telecommunications Act being called upon to excuse the liability of the provider (for example, *Blumenthal v. Drudge and AOL*, TechLaw (2000b), where AOL paid Drudge to make his online report readily available to AOL subscribers).

In the UK, ISPs may be liable, as in a recent case where a physicist obtained damages from an ISP for defamatory news items left on their server.

3.4.6.4 Intellectual property and copyright laws

Internet intellectual property rights are a critical legal issue (De Zwart, 1997; Foster, 1997; Loundy, 1998; Saunders Thomas *et al*., 1997; Smith, 1996). A significant issue concerns the content of Web site material: Is it copyright-protected? Companies must ensure that they hold copyright permissions for all their Web site material (for example, permissions from all freelance authors whose work is on the site) (Smith, 1996). Further, companies must question the legality of copying information from external Web sites (Foster, 1997; Loundy, 1998).

In most cases, existing laws protect the copyright of Web site information or other postings, whether or not information owners place a copyright statement on their electronic document. However, for safety,

---

companies should always post copyright statements on their Web sites.
(Smith, 1996)

One concern revolves around "what constitutes a reproduction?" For example, do copies of information made by proxy servers or routers constitute reproductions (Foster, 1997)? If so, then if nations legislate their own Internet copyright laws, ISPs may find themselves liable in other countries for their (reproduced) proxy server content (Foster, 1997).

Another copyright issue is that companies must ensure they are copyright-protected for database information accessible via their Internet connection.

3.4.6.5 Privacy laws

The issue of Internet privacy is a human issue as well as a legal issue. In this section I will be concentrating on the legal aspects of Internet privacy, while in Section 3.4.8.2, the focus will be on the human aspects.

Privacy was recently rated the number one human concern in a U.S. survey (EPIC, 1999), and Internet privacy in particular is under the spotlight, with increasing use of the Internet in everyday life. Recent surveys show that Internet users want Internet privacy laws (EPIC, 1997c, 1998a; GVU, 1998).

Internet users are extremely concerned about personal data gathered by Web sites and on firewalls and servers, and the use of this data. They are also concerned about the privacy of their email.

Nations around the world already have privacy laws which are used to regulate information privacy.

Australia's data privacy rights are currently recorded in the Privacy Act (1988), although this does not cover state government bodies or private bodies (Hilvert, 1996). Private bodies are likely to get privacy legislation soon with a proposed Bill (AGD, 1999b)—which has been debated by various experts (for example, Clarke, 2000)—about to be legislated. The UK has enacted the Data Protection Act 1998 (Baker & McKenzie, 1999), while the U.S. has enacted the Electronic Communications Privacy Act of 1986, the Children's Online Privacy Protection Act 1999 and has proposed a host of new online privacy Bills (TechLaw, 2000c).

The U.S. has long resisted government regulation of Internet privacy. Indeed, the Federal Trade Commission (FTC) still holds high hopes for industry self-regulation of consumer Internet privacy. However, if this proves inadequate for the safeguarding of Internet privacy, some proposed online privacy bills may eventually progress to become law (TechLaw, 2000c). Various experts have been urging recently that the U.S. get in line with other countries by regulating Internet privacy (for example, Clarke, 1999).

Regardless of privacy laws, the collection and use of personal information gathered via Web site visits should be stipulated by companies on their Web sites:

Increasingly, companies are including privacy statements on their Web sites.

The TRUSTe organisation (Benassi, 1999; TRUSTe, 2000) recommends the U.S. Dept. of Commerce privacy principles for Web sites to provide good consumer privacy protection (FTC, 1998). TRUSTe reviews the privacy level of Web sites on request. If the privacy of a site passes muster, that site may display the TRUSTe 'Privacy Seal' trustmark.

Email privacy rights are also of concern, and remain a legal grey area (Sipior and Ward, 1995). Most courts have been upholding the employer's right to read email provided and paid for by the employer, despite employee claims to email privacy.

Cross-border personal data flow is another Internet privacy concern. In the European Community, the EU Data Protection directive (EC, 1995) which has operated since October, 1998, prohibits personal information flow from companies located within the Community to countries outside the Community that do not provide 'adequate' information privacy protection. This has been of considerable concern to the U.S., who have had to establish principles in order to allow American companies to trade internationally under the directive (ITA, 1999; Kabay, 1999).

As all company policies must conform to national and global privacy laws (Godwin, 1998), so must the company Internet security policy.

3.4.6.6 Reliance on content

If incorrect information is published on the Web by a company, leading to personal injury or property damage, "due care" must be established to avoid company liability. This suggests routine disclaimers on safety-critical and other relevant Web sites in order to protect companies (Smith, 1996).

3.4.6.7 Self-help remedies

Many Internet users are resorting to self-help remedies in reaction to Internet harassment or other offensive behaviour. Such actions may be illegal (Smith *et al*., 1998). For example, the "flooding" of an offender with excessive traffic in order to cause denial-of-service is usually illegal.

3.4.6.8 Transjurisdictional issues

The Internet is a borderless facility, and countries may well make judgments based on the rationality and intelligibility of other countries' laws. This has been an extremely worrisome concern (Jackson, 1998; O'Connell, 1997).

Businesses need to be aware that they may well be subject to the laws of other countries when accessing customers in those countries (Pattison, 1997). Pattison cited the example of a company using its trademark on a Web site, thereby infringing third-party trade mark registrations in other countries, and suggested as one solution that a company limit its Internet product and service activities to residents of specified countries via web site notification and user consent agreements or contracts.

Some experts have investigated how international bodies have changed the ways law protects businesses from various Internet risks, given the transjurisdictional issues involved (see, for example, Jackson, 1998).

3.4.6.9 Legal liability

Related to transjurisdictional issues is the issue of "who is liable?" for an Internet abuse. For example, regarding a web document, is it the document author, the author's employer, or the ISP publishing the document, who is liable for its content? U.S. cases have favoured excusing ISPs from liability (EPIC, 1997d) in accordance with the Telecommunications Act, 1996, taking the view that if ISPs were required to check the content of all material that passes through them, they would soon decide to go out of business.

As mentioned earlier, the new Australian Broadcasting Services Amendment (Online Services) Act 1999 will hold ISPs liable if they allow illegal off shore site content (that is, illegal according to the new Australian law) that has been reported to the Australian Broadcasting Authority (ABA) to pass through their servers (AGD, 1999c). This onus of responsibility and liability being placed on ISPs has caused controversy in Australia.

Companies should take preventative measures. As mentioned in discussing defamation (Section 3.4.6.3):

Increasingly, companies are being held liable for the unchecked offensive postings of their employees. Companies are now expected to show a response to an issue, or take preventative action to avoid liability.

(Farrow, 1998; Moulton, 1998)

There are ways for companies to avoid legal liability. For example, companies are advised to use Web wrap contracts which bind a Web site user who “signs” the contract—agreeing to the stated terms of Web site use—prior to proceeding further into the site (Smith, 1996). A final warning comes from Foster (1997):

Countries legislating independently may mean that a company may be liable in countries other than that in which the company’s server resides.

(Foster, 1997)

3.4.6.10 Contracts

There is a question as to what constitutes a legally binding contract between purchaser and vendor when an Internet order is placed. For example, if a Web site displays out-of-stock items (the most popular

consumer complaint in a recent survey), the vendor may be in breach of contract (Pattison, 1997). Pattison noted that requests for user acceptance of terms of contract prior to completing an electronic transaction were becoming more common.

3.4.6.11 Evidence

Email is increasingly regarded as a potential source of evidence, as part of an audit trail of legal evidence (Farrow, 1998). Farrow noted that electronic discovery of evidence had become a critical aspect of U.S. litigation, with lawyers who fail to uncover a critical electronic document potentially facing claims for malpractice.

3.4.6.12 Influence of laws on Internet security policy

The Internet security policy should ensure there are policies in place which protect company liability, as well as advise employees of their personal liability in various situations. The policy should also advise employees how they should behave and act in their Internet usage, in order to conform to existing law.

3.4.7 Technical issues in Internet security policy

Technical Internet security mechanisms must be selected, acquired, installed and monitored, in order to implement the security requirements specified in the Internet security policy. Procedures must be specified for this process.

New Internet security technologies are constantly emerging (see Bryan, 1995; Chapman and Zwicky, 1995; Cheswick and Bellovin, 2000; D'Alotto, 1996; Denning, 1996; Edwards, 1996; Faroughi and Perkins, 1996; Kyas, 1997; NIST, 1994b; NIST, 1996a; Olivier and van de Haar, 1997; Siyan and Hare, 1995; Wack and Carnahan, 1995; Wood, 1997b).

It is outside the scope of this research project to describe the many available Internet security technologies. Instead, a brief listing of the major technologies follows.

The Internet security technologies available include greater bandwidth communication lines (for example, using ISDN PRI services), improved workstation capability, firewalls (including routers, gateways and switches—such as the Eagle firewall systems offered by Raptor Systems), proxy servers, tunnelling (virtual private networks), anti-viral tools, cryptography, key management systems, PKI, authentication (especially biometric authentication, intelligent tokens ("smart cards"), digital signatures, single sign-on and third-party authentication), digital certificates, logging and real-time alarms (including intrusion detection systems), automated auditing systems, penetration testing tools (such as Internet Probe Droid), and secure e-commerce software and services. However,

all Internet security technologies are vulnerable to failure (Denning, 1996), supporting once again the claim that nontechnical controls are critical in maintaining security.

Sub-policies for each technology selected are required. Again, it is beyond the scope of this thesis to investigate these sub-policies, as the complexity and scope are significantly large.

For example, Stanley (1997) points out that the issues for encryption policy are enormous (see, for example, Section 3.4.6.1 for an indication of legal aspects to be considered by a company's encryption sub-policy), and that most companies do not understand encryption issues, or management of encryption, or relevant laws or import/export controls.

The Internet security policy should include specification of technical Internet security requirements (examples: firewall technology requirements and encryption requirements).

3.4.8 Human issues in Internet security policy

The importance of the human influence in all spheres of information security is well recognized. Many experts believe that the human issues in information security should be considered just as important as the technical issues (Warman, 1992; Wood, 1995). There are many human issues which may be of concern to an organisation's employees in the Internet security policy, with which they will be expected to comply. From the outset, I inform the reader that human issues in this thesis will be discussed in the context of countries where people have democratic rights.

An important initial remark is made here. I believe that employees are more likely to accept Internet restrictions if they are made policy prior to deploying the Internet, i.e. with forethought, rather than as an afterthought, as people tend to get annoyed in general when available privileges and tools are removed. Hence, decisions reached prior to deploying the Internet may well be different ones to those reached if the Internet is already deployed—with certain privileges already in place.

The model of human issues illustrated in Table 3.4 summarises human issues in Internet security policy. Each issue is discussed below, with related conflicts being highlighted as usual within a *conflict* box.

Human issues in Internet security policy	Source
Freedom of Internet use	3.4.8.1
Privacy	3.4.8.2
Censorship	3.4.8.3
Right to be kept informed	3.4.8.4
Accountability	3.4.8.5
Ownership	3.4.8.6
Ethics	3.4.8.7

Table 3.4 Human issues in Internet security policy

3.4.8.1 Freedom of Internet use

Conflict:

The needs of society:
free flow of Internet traffic internationally, with minimal traffic delay; and
regulated Internet usage (view of commercial bodies) or
unregulated Internet usage (view of many other bodies)

vs

The needs of the company:
optimum workplace productivity;
controlled Internet usage; and
Internet resource availability

vs

The needs of the employee:
unrestricted Internet usage

Employees will expect certain Internet freedoms in the workplace, as illustrated by the traditionally accepted personal usage of the office telephone. In many organisations, employees may feel unduly restricted and may resist if restricted in Internet usage (for example, by being prohibited from non-business Internet usage). Employees may feel that they should be free to send personal email, surf the Internet, download games and images, subscribe to listservers, and so forth—for at least a portion of the day. Cultural patterns will influence the amount and types of Internet use freedom which employees will expect.

The employer, on the other hand, may feel that Internet usage is a privilege rather than a right, and may be interested in restricting usage in order to maximise business usage, minimise lost productivity due to non-business or ineffective usage, and maintain the availability of the Internet resources to the

organisation as a whole. With increasing concerns about non-business usage in the workplace, and consequent losses, employers are now taking a stronger position on this issue. However,

---

it is becoming increasingly difficult to define a usage as personal or business, as communication and collaboration may involve personal exchanges as a cultural expectation. Acceptable and unacceptable usage will thus need to be interpreted by employees and authorities in the context of the organisation's culture.

The Internet security policy must include advice as to what constitutes acceptable and unacceptable Internet usage, including time constraints or other restrictions or conditions of use. The employees should be advised that Internet use is a privilege rather than a right.

3.4.8.2 Privacy

(refer Section 3.4.6.5 for a discussion of the legal issues associated with privacy)

Conflict:

The needs of society:
law enforcement agencies need access to evidence about suspected law-breakers;
freedom of information (about Internet users); individual and company accountability for Internet usage
vs
The needs of the company:
employee accountability for Internet usage; protection of employee privacy from external world.
vs
The needs of the employee:
personal privacy in Internet usage

Data privacy may be defined as "the ability of an individual to control information about oneself, and communications to which the individual is a party", with current data privacy concerns revolving around personal information, transactions and communications (NIIAC, 1995). Another definition of data privacy is “a condition of limited access to identifiable information about individuals” (Smith, 1993, p. 106). Individual privacy has been viewed as a spiritual issue, the invasion of which is an affront to individualism and human dignity (Bloustein, 1964). Mason (1986) referred to privacy as one of the four major ethical issues of our times. Supporting this notion, EPIC (1999) cited a survey reporting personal privacy as the number one American concern.

An employee's right to privacy during Internet usage is particularly important due to global exposure. Internet privacy has been well-remarked by experts as a serious e-commerce concern (Agre and Rotenberg, 1997; TRUSTe, 2000). Furthermore,

---

Internet users consistently cite 'lack of personal privacy' as a major worry.
(Aldridge *et al*., 1997; EPIC, 1997c; 1998a; 1999; GVU, 1998; Pitkow and Kehoe, 1997; Wang *et al*., 1998)

I discuss here four classic user privacy concerns (compiled from Aldridge *et al*., 1997; Hilvert, 1996; Wang *et al*., 1998), to illustrate the nature of the problem. Firstly, servers log every access, IP address, time of download, user's name, URL requested, status of request, size of data transmitted, client the reader is using and sometimes the user's real name and email address. Secondly, e-commerce sites proffer forms for users to complete with personal details, some of which may be sensitive financial data, such as credit card details. Third, personal information about a user is often stored on a user's hard drive by the web server of a site visited, as a "cookie" record, which is subsequently retrieved by web servers of sites visited for tracking the user's behaviour for direct marketing and other purposes. Finally, users are often unaware of uses (such as direct marketing, third party distribution) to which personal information gathered from Web site visits is put.

There is plentiful evidence of user concerns about personal data collected. 41% of a Boston Consulting Group 1997 survey's respondents admitted leaving Web sites when asked to register or provide personal information (BCG, 1997), while 27% falsified information on Web site registration forms (SKYWRITING, 1997).

Employees have another type of user privacy concern. Employees do not wish their Internet accesses to be logged, monitored or surveilled, contrary to employer needs for employee accountability.

Yet another type of privacy concern has centred around proposed weak encryption schemes, which may lead to invasion of the privacy of data stored about third parties, (such as customers) in corporate data accessible via the Internet. Because highly sensitive military information could be disclosed in other countries which could break weak encryption algorithms such as those previously proposed with key escrow and key recovery schemes by the U.S, encrypted technology has been regarded as a form of munition, and IT products employing encryption (including Internet tools employing encryption) have therefore been subject to export controls (Denning, 1996), causing much frustration for IT companies who wished to export products. For a discussion of this issue, see Landau *et al*. (1994). This issue may die down with the recent relaxation of U.S. exported encrypted technology (Clausing, 2000).

There are some new, insidious types of invasions of Internet privacy. For example, Internet users are being encouraged to subscribe to direct marketing services who send them direct marketing email, which the user then reads. The user is later recompensed financially for reading the advertisements in the email. The click-through rate on links in such emails is claimed to be around 60%, far higher than that for banner advertisements on web sites. An example of such a direct marketing service is the Internet company Money for Mail.

What privacy services are users ideally seeking? Six different *Internet user privacy services* to support Internet privacy needs have been defined by researchers:

(i) informational self-determination

Kohl (1995) discussed the right to informational self-determination, namely the need for individuals to be in control of access to personal data about themselves. This right could be extended to Internet concerns, for example, do employees determine who accesses individual site access information logged on firewalls (usually not)?

(ii) *unobservability*

Rannenberg (1994) discussed the right of a user to use a resource or service without other users, especially third parties, being able to observe that the resource or service is being used. In the case of the Internet, this entails an absence of monitoring or surveillance.

(iii) nonrepudiation

Rannenberg (1994) and Kohl (1995) defined this as a user being unable to deny accountability with respect to a particular operation. It is considered a very important privacy requirement for e-commerce success.

(iv) anonymity

Rannenberg (1994) defined this as the right of a user to use a resource or service without disclosing identity. Lee (1996) and Anonymous (1996) noted the use of anonymous remailers to allow user anonymity in email usage. The originator of a message then becomes virtually untraceable. These two authors note the virtues and vices of this facility. They argue that although identification of a speaker assists readers in assessing the truth and accuracy of a posting, anonymity also facilitates impersonation; the originator can pretend to be an authority in order to gain credibility. Further, anonymity facilitates offensive postings, pranks and fraud, particularly in electronic commerce, where accountability may not then be possible. Conversely, anonymity also facilitates freedom of speech, especially for concerned groups such as victims of crimes, and "whistle-blowers". Lee (1996) proposes "visible anonymity" for postings, where a user can view a clue to the anonymous nature of an email message in the message header.

(v) unlinkability

Rannenberg (1994) discussed the right of a user to make multiple uses of resources or services without others being able to link these uses together.

(vi) pseudonymity

Rannenberg (1994) discussed the right of a user to use a resource or service without disclosing identity, yet still being held accountable for that use. Many ISPs offer pseudonymous usage (for example, America Online (AOL))—by maintaining records of the true identities of their customers, so that they can hold that customer accountable for their actions. Another example of the employment of pseudonymity is in emerging intrusion detection systems, where pseudonymous audits are possible (Sobirey *et al*., 1997). Lastly, cryptography can provide pseudonymity for Internet commerce transactions by providing message authentication as well as accountability (Anonymous, 1996).

If any of the above Internet privacy services are available to employees, the employee should be informed within the policy as to how the services are accessible.

Industry and community groups are cooperating in developing various guidelines for Internet privacy protection. Companies can now choose to display privacy statements on their web sites. For example, Citibank exhibits a privacy statement on its home page (Citibank, 2000).

The number of companies displaying privacy statements on their Web sites has grown dramatically in recent years. TRUSTe (1999) and EPIC (1999) cited a survey indicating that in 1998, nearly two-thirds of commercial web sites displayed a privacy statement, although less than 10% of commercial web sites had comprehensive privacy statements consistent with fair information practices. This situation is a significant improvement compared with results of earlier surveys (see EPIC (1997a), reporting a survey of the top 100 Web sites, of which only 17% had privacy statements). Only 12% of Australian sites featured privacy statements in 1999 (Frehill and Hollingdale, 2000).

The Internet security policy must incorporate an *Internet privacy sub-policy* addressing all the above issues.

3.4.8.3 Censorship

(refer Section 3.4.6.2 for a discussion of relevant legal issues)

Societal Internet censorship is aimed at limiting accesses, and limiting production of, restricted and objectionable material on the Internet (via provision of site classification and content regulation schemes, for example), for legality and decency reasons.

Company Internet censorship is aimed at preventing employee non-business Internet usage, as well as access to indecent and criminal Web sites, preventing defamation and harassment of others by their own employees, preventing damage to company image caused by recorded employee accesses to indecent or criminal sites, and preventing leaking of confidential business information by employees in postings to external parties. It is also aimed at preventing employees from accidentally accessing objectionable sites and postings (for example, offensive postings on selected newsgroups). For example, Willing (1998) pointed out the way in which porn companies can abuse inoffensive sites by using almost identical urls for their own site addresses. Unsuspecting searchers are then subjected to the content of porn sites.

Many individuals and groups regard Internet censorship as counter to democratic principles of "freedom of speech" (desire to write email and construct Web sites, for example, free of restrictions) "privacy rights" (desire not to have email read (censored) by company), and "freedom of information" (desire to have access to the complete range of external Internet materials)—and are providing vigorous opposition.

Neely (1995) illustrates these objections by pointing out a powerful public argument for allowing uncensored, private consensual electronic interchanges, such as personal email between boyfriend and girlfriend.

The above conflict is summarised below:

Conflict:

The needs of society:
restricting Internet materials for legality and decency purposes

The needs of the company:
restricting Internet material for legality, decency, confidentiality and company image reasons;
restricting Internet usage to acceptable business usages; and
protection of employees from embarrassing access to objectionable materials

vs

The needs of the employee:
freedom of speech; freedom of information; privacy

The Internet security policy must incorporate an *Internet censorship policy* addressing all the above issues.

3.4.8.4 The right to be kept informed

(refer Section 3.4.4.5 for related discussions on Internet awareness issues)

It is in the interests of society, companies and their employees that employees are kept informed of their Internet usage and security responsibilities. Without adequate awareness activities in place, employees may refuse to accept accountability for their Internet activities. Awareness activities are considered essential to the success of Internet security, as discussed earlier in Section 3.4.4.5.

The Internet security policy must include advice regarding Internet security awareness measures and activities for employees.

3.4.8.5 Accountability

One of NIST's (1996b) principles, accountability, requires that the *Internet roles and responsibilities,* as well as the means for providing the Internet accountability of all parties involved, be made explicit in the Internet security policy.

A company's need to hold employees accountable for their Internet activities as well as for residual system conditions after Internet misuse or abuse, raises the following conflict:

Conflict:

The needs of society: protection of all Internet networks from attacks by company employees; and liability of employee or company to be determinable vs *The needs of the company:* the right to check for policy compliance through records of Internet accesses; avoidance of company liability for external damage through proof of employee-caused harm; and the right to impose sanctions on non-compliance vs *The needs of the employee:* privacy of Internet activity; trust shown by company; and acceptable sanctions on non-compliance

Policies which clarify employee accountability (ie place the blame) are extremely difficult to formulate. For example, data exchanged by employees over the Internet may be of low quality, yet current legal and ethical guidelines for determining liability and accountability for the quality of Internet information are

inadequate (Mathieu *et al*., 1995). In such conditions, how can policies place the blame for low data quality with the employee? Employees will also need to be assured that adequate security services which support true accountability are in place, namely authentication and nonrepudiation:

Authentication: Each employee should be identified and verified by the system.

Nonrepudiation (from Kohl, 1995): An employee should be unable to deny having performed an operation.

Furthermore, employees may refuse to be held accountable for their actions without adequate policy awareness measures.

Visibility of employee Internet activity is a simple, though controversial, method for checking for employee compliance with policy, and thence holding employees accountable for non-compliance. Internet activity visibility involves recording and maintaining a comprehensive, secure history of Internet actions—amounting to *monitoring* and *surveillance*—also both sensitive and controversial actions (Neumann, 1993).

Monitoring and *surveillance* are enabled by technical mechanisms such as *firewall logs* of employee Internet accesses, combined with exception reports from the logs, manual report-checking, video surveillance of the workstation areas in which employees work, and supervisors walking around keeping an eye on employee Internet activity on screen. Analytical surveillance may also be required for detecting and possibly preventing network outages, intruders and misusers, and fraud (Neumann, 1993).

Visibility, monitoring and surveillance are often regarded by employees as unethical infringements of privacy, and symbolic of distrust. Hence, Neumann (1993) advises their careful control due to their high antisocial potential.

Sanctions may also be employed to enforce policy. Employees will wish to know their level of culpability with respect to breaching policy. Sanctions should be clearly defined, and should be acceptable to employees. In order to achieve acceptance, suitable warnings, reprimands, and other punitive measures need to be developed by negotiation with representative employees. Exceptions to policy should always be possible, and the path of action for approval of such exceptions clarified within the policy.

The Internet security policy must include advice which clarifies all aspects of accountability, including clear identification of roles and responsibilities, and the services to be implemented which will support accountability, including the level and degree of logging, monitoring, surveillance and sanctions.

3.4.8.6 Ownership

Employees typically claim ownership of their own postings, and hence expect privacy with respect to these. However, many companies believe that such postings are their property, and claim rights to access the information. It is the companies which are being held liable for such material if found to be illegal (for example, defamatory), and hence at present, the law appears to favour company ownership of Internet material rather than employee ownership (see Sections 3.4.3.1 and 3.4.6). New laws, for example a new Australian Privacy Act, may challenge company ownership rights to employees' personal email. The conflict is summarised below.

Conflict:

The needs of the company: Company ownership of employee postings and Web sites; avoidance of legal liability Vs *The needs of the employee:* Employee ownership of employee postings and web sites; avoidance of legal liability

The Internet security policy must advise employees to put disclaimers on opinion-based or personal email and personal Web sites.

3.4.8.7 Ethics

(refer Section 3.4.2.2 for discussion of ethics as a societal issues)

A sense of ethics within global society should be expected in employee Internet usage (as introduced in Section 3.4.2.2). Politeness, honesty, fairness, trust, willingness to share and assist others, are all examples of society's expectations in Internet dealings. A statement to this effect in the Internet security policy is desirable. (There may already be a company Code of Ethics which will guide the statement.)

For example, our global society emphasises the importance of *netiquette*, a set of Internet communication standards for Internet politeness. Many attempts have been made to standardise netiquette (Highland, 1996), and Scheuermann and Taylor (1997) described the most frequently cited netiquette suggestions. For example: "Think first. Messages can be forwarded or copied. Never write while angry. It may be better to wait a day to think of the possible outcomes before responding in haste." An organisation may wish to vary netiquette to suit its culture, with variations being documented within the Internet security policy.

The Internet security policy should advise employees to adhere to the company's Code of Ethics, as well as specific advice to follow a set of netiquette standards in Internet communications, and guidelines for other recommended ethical behaviours.

3.5 Conclusion

This Chapter has placed Internet security policy for organisations in the context of existing research by surveying related aspects from the following reference fields: information security, information management, Internet usage, electronic commerce, Internet security and information technology. By so doing, I was able to posit a basic, three-component outline for Internet security policy for organisations (Figure 3-2), and then propose, justify and describe in detail a model for *one* of the three components—the factors which influence the policy (Figure 3-3). I describe below how I went about this, and draw conclusions for the development of the remaining two components in Chapter 4.

At the beginning of this Chapter, I found from the literature that existing guidelines for Internet security policy for organisations were deficient in a number of important areas. In particular, an holistic approach to Internet security was missing, guidelines were too general, there was incomplete coverage of prevailing Internet risks, and important human issues were overlooked.

There was clearly a need for new guidelines which overcame these and other deficiencies (see Section 3.2.3). I proposed a three-component outline for guidelines (Figure 3-2), showing the need for (i) guidelines for factors to be considered, (ii) guidelines for policy content, and (iii) guidelines for policy development.

In the remainder of the Chapter, I focused on developing the first of the components, the guidelines for factors, as follows:

I initially proposed a model for the factors in Internet security policy, Figure 3-3, suggesting that the factors fell into the following categories: *Internet risks, organisational, administrative, legal, societal, technical and human issues*. The model clearly indicates that *human issues are the filter through which all other factors must be viewed.*

Within each category of factors, I explored many sources (in particular, existing literature) from the domains of: information security, information management, Internet usage, electronic commerce, Internet security and information technology. In the process:

- I identified many factors in each category, and developed four additional models:
  - conflicts in Internet security policy (Figure 3-4);

- Internet risks for organisations (Figure 3-5);
- organisational factors in Internet security policy (Table 3.2); and
- human issues in Internet security policy (Table 3.4).

- I highlighted *conflicts* which may arise for companies when setting policy to handle identified factors;
- I suggested *advice* which may be given to employees within the policy to address identified factors;
- I suggested sub-policies for the Internet security policy, to address factors;
- I suggested Internet security requirements which may be included in the policy; and
- I confirmed that the initial model for factors (Figure 3-3) was an appropriate first-cut model.

It is clear from the analyses of the various factors in this Chapter that there will be many difficult decisions to be made by security analysts when developing policy, as discussed below.

With respect to the Internet risks to be addressed by the policy, not only are there many such risks to consider, but there are many clever, determined, criminally-minded or unethical people "out there" who are increasingly exploiting the Internet's significant and growing vulnerabilities. Further, company employees are contributing to Internet risks through accidental or deliberate misuse of Internet facilities (for example, excessive non-business usage).

The research also made it clear that different companies face different risks—for example, a financial company such as a bank faces fraud more strongly than an educational institute. Hence, it may be wise to conduct a risk assessment of the Internet risks being faced, at the time of developing the policy. In this way, the most attention can be given to controlling the most significant risks. (The process of risk assessment is, indeed, suggested in Chapter 4 when discussing an approach to policy development.)

This research has clearly signalled that this category of factors (i.e Internet risks) are a key category to address within the policy.

With respect to the organisational factors which influence the Internet security policy, the research suggests that it is imperative that a formal organisational Internet infrastructure guiding all Internet usage and security for the company, be set up. Hence, set policy will be consistent with this formal infrastructure, and further, the infrastructure can be described within the policy itself. Some critical advice for employees to be included in the policy is suggested by this research:

- a set of acceptable Internet business usages that are aligned with organisational objectives;
- an indication of senior management support for the policy; and
- specification of awareness activities which support the policy.
-

A critical Internet security requirement to be included in the policy is suggested by this research:

- an Internet security management programme, for ongoing, organised Internet security management.

With respect to administrative factors in Internet security policy, the research suggests that the policies set must be feasible, and that procedures for implementing them must either be referenced or laid down within the policy document itself.

With respect to legal issues in Internet security policy, the research suggests that companies need to familiarise themselves (and keep up to date) with existing national and international laws before setting policy, and that employees should be warned of illegal Internet usages within the policy itself.

With respect to technical issues within Internet security policy, the research suggests that companies need to be aware of (and keep up to date with) the growing number of excellent, useful Internet security technologies coming onto the market. Knowledge of available technologies can then lead to specifying requirements for these technologies within the policy. However, the research suggests that current and emerging technologies are vulnerable to failure, and companies hence need to proceed with caution when employing them.

With respect to human issues within Internet security policy, the research suggests that policy decisions made regarding other identified factors may negatively affect company employees. Their rights and expectations for each issue need to be considered. For example, employee *accountability* for Internet use must be considered when addressing the following factors in the policy:

- *Internet risks:* For example, Internet use monitoring may be decided upon to check for 'non-business usage', thereby making employees accountable for any non-business usage;
- *organisational factors:* For example, a lack of Internet awareness activities will negatively affect the employees' cooperation with respect to being held accountable for their Internet actions;
- *administrative issues:* For example, procedures being considered for sanctioning employees after misuse may not meet with employee approval, hence compromising the chances of successful employee accountability—sanction procedures must meet with employee approval;
- *legal issues:* For example, deciding to hold employees accountable for the presence of illicit, downloaded software on their workstations implies a statement to this effect must be placed in the policy; and
- *technical issues:* For example, choosing to deploy a firewall for logging employee Internet accesses may be decided upon to provide employee accountability, against employee wishes.

In the next Chapter, I utilise the factors identified in this Chapter, as well as other results of the research described in this Chapter, to construct the two remaining components of the framework for Internet security for organisations: a model for the content of Internet security policy for organisations, and a framework for the development of the policy. I then construct the final overall framework for Internet security policy for organisations, utilising all my developed models.

Chapter 4
First-cut Framework

"*Nam et ipsa scientia potestas est"*

- *Knowledge is power* (Francis Bacon)

In Chapter 3, I constructed an outline framework for Internet security policy (Figure 3-2) consisting of three components: factors, content and development. I suggested a model for the factors component (Figure 3-3), and investigated all categories of factors proposed, through exploring research literature and other sources. In the process, I developed three models for specific categories of factors: Internet risks (Figure 3-5), organisational factors (Table 3.2) and human issues (Table 3.4).

In this Chapter, I draw together all previously identified factors to determine models for the remaining two components of Figure 3-2 (content and development), and finally the overall detailed framework. In Section 4.1, I present and overview an outline for the content of an Internet security policy. In Section 4.2, I present and describe a framework for developing an Internet security policy. In Section 4.3, I present and discuss a detailed overall framework for Internet security policy for organisations incorporating the three main components (factors, content and development) as well as related models.

4.1 Content of Internet security policy for organisations

An organisation's Internet security policy is composed of a series of sub-policies and statements. In this section, I propose the sub-policies and statements shown in Table 4.1 as an outline for the content of an Internet security policy, then briefly describe each component, relating it back to the relevant discussions in Chapter 3.

Internet security policy content	Source
Purpose and scope of policy	4.1.1
Philosophy of policy	4.1.2
Internet security infrastructure	4.1.3
Internet security management programme	4.1.4
Other applicable policies	4.1.5
Internet privacy policy	4.1.6
Internet censorship policy	4.1.7
Internet responsibility and accountability policy	4.1.8
Internet information protection policy	4.1.9
Internet information access policy	4.1.10
Firewall policy	4.1.11
Internet security technology policy	4.1.12
Password policy	4.1.13
Internet acceptable usage policy (IAUP)	4.1.14
Internet publication policy	4.1.15
Email policy	4.1.16
Internet virus policy	4.1.17
Internet audit policy	4.1.18
Internet incident response policy	4.1.19
Internet legal policy	4.1.20
Internet security policy review policy	4.1.21

Table 4.1 Internet security policy for organisations—content

4.1.1 Purpose and scope of policy

The purpose of the Internet security policy must be stated, as well as the range of issues addressed. Heard (1996) suggested the following statements of purpose and scope:

The purpose of this policy is to protect the (organisation's name) network and data from unauthorised access, corruption, or service disruption as a result of Internet usage.

This policy applies to all staff of the (organisation's name) whether they are permanent, temporary, auxiliary, contracted or seconded.

4.1.2 Philosophy of policy

(refer Section 3.4.4.2 for related discussions)

A statement of the Internet security posture adopted should be made: either paranoid, prudent, permissive, or promiscuous, with an explanation of this posture.

4.1.3 Internet security infrastructure (Internet security plan)

(refer Sections 3.4.4.1 and 3.4.4.2 for related discussions)

There should be a policy detailing all aspects of the Internet security infrastructure: an Internet strategy (see Section 3.4.4.1), constitution of the policy development and maintenance team, standards, Internet architecture, storage of corporate data, available Internet services and software, and other staffing requirements.

4.1.4 Internet security management programme

(refer Sections 3.4.4.3, 3.4.4.4 for related discussions)

A description of the components of the Internet security management programme should be given, as well as details of programme reviews and updates. The programme should be composed of policies, procedures, training and awareness activities, access restrictions, monitoring, compliance procedures, an Internet security infrastructure (Internet plan), and a range of Internet security technologies. A statement of management commitment should also be made.

4.1.5 Other applicable policies

(refer Section 3.4.4.6 for related discussions)

A statement referring the reader to other relevant policies should be made (for example, the company Code of Ethics, key subpolicies such as the IAUP, and subsuming policies such as the CISP).

4.1.6 Internet privacy policy

(refer Sections 3.4.6.5 and 3.4.8.2 for related discussions)

Experts recommend an Internet privacy policy for the protection of employer and employee privacy (EPIC, 1999; Griffiths, 1996; Smith, 1993; TRUSTe, 1999). The policy should include details of any Internet privacy services provided (for example, anonymity in Internet activity), technological measures provided (for example, provisions of email encryption facilities), and any necessary infringements of employee privacy (for example, logging of employee Internet activity, and scanning of employee email). Some amount of monitoring will undoubtedly be considered essential by the company for security,

planning and diagnostic reasons. It is ethical to inform employees of the need for such monitoring, exactly what is being monitored, and who has access to that information.

4.1.7 Internet censorship policy

(refer Sections 3.4.6.2 and 3.4.8.3 for related discussions)

A policy advising of any filtering of offensive Internet materials, either into or out of the company, is required.

4.1.8 Internet responsibility and accountability policy

(refer Section 3.4.8.5 for related discussions)

There must be a statement of the Internet security roles and responsibilities of personnel, including network administrators, the IT security manager, the IT function, business unit managers, and other employees. Employee accountability achieved via monitoring, surveillance and sanctions, must be stated.

4.1.9 Internet information protection policy

(refer Sections 3.4.3.5, 3.4.3.6, 3.4.3.12, 3.4.4.4 for related discussions)

This policy should define the corporate data and Web sites which require protection from the outside world. It should also include a policy for storing sensitive data in a safe place, inaccessible to Internet intruders, and for disposing of sensitive corporate data (i.e. clearing and purging of unrequired classified data from Internet-accessible servers). Finally, it should define back-up procedures for backing up sensitive corporate data residing on Internet accessible servers.

4.1.10 Internet information access policy

(refer Sections 3.4.3.5, 3.4.3.6, 3.4.3.9, 3.4.3.12, 3.4.5 for related discussions)

This policy should specify Internet access requirements to internal data and web sites, for different parties (for example, groups of employees, individual employees, suppliers). A policy for requesting Internet access privileges and Internet services is also required. The Internet information access policy is supplemented by the Internet firewall policy.

4.1.11 Firewall policy

The primary function of a firewall is to provide a buffer from external attack.
(Drake and Morse, 1996)

However, a firewall can only implement decisions that are made by the organisation as matters of policy.

(Bryan, 1995)

A statement of the company's Internet connection policy is encoded as a set of rules into a firewall (Griffiths, 1996)—this Internet connection policy forms a foundation for a *firewall policy*.

4.1.11.1 Firewall policy content

I propose a firewall policy composed of the following components, illustrated in Table 4.2.

Internet Firewall Policy Content	**Source**
security boundary statement	(i)
firewall policy stance	(ii)
access method	(iii)
access rules	(iv)
firewall maintenance policy	(v)
firewall new access request policy	(vi)
firewall roles and responsibilities	(vii)

Table 4.2 Firewall policy content

(compiled from Bryan, 1995; D'Alotto, 1996;
Drake and Morse, 1996; and Griffiths, 1996)

(i) security boundary statement (for example: "all internal network nodes and the firewall itself are to be protected by the policy").

(ii) firewall policy stance (for user access to Internet services)

(attributed to Chapman and Zwicky, 1995):

- 'default deny': that which is not expressly permitted is prohibited
- 'default permit': that which is not expressly prohibited is permitted

(most businesses will choose the 'default deny' stance).

(iii) access method

Access can be granted in three ways: by IP address, by account (user identifier plus password) or by strong user authentication (eg biometric device). The first method, granting access by IP address, is a means which is easily subverted either by a person sitting at the PC (and away they go!) or by spoofing the IP address. Also, when a legitimate user moves and gets a new IP address, the firewall rules must be changed accordingly. Hence, either account-based access or strong authentication-based access should be chosen.

(iv) access rules

All firewall technologies require a set of access rules to be defined, permitting and disallowing accesses into and out of the company. Highly granular firewall components set:

- access rules for employees and external parties accessing:
  - Internet services (email, FTP, Telnet, World Wide Web etc.);
  - source and destination subnets, hosts and ports; and also
  - permitted access times for all types of accesses.
- a list of automated defences (i.e. the firewall access rules); and
- a list of procedural defences (for example: "users are not allowed to modify the email program").

For example, a firewall policy may permit the following accesses:

- email in both directions;
- both internal and external hosts are allowed to "ping" the firewall (for connectivity
- testing);
- both incoming and outgoing Domain Name Service (DNS) requests;
- non-anonymous File Transfer Protocol (FTP);
- unrestricted World Wide Web access.

(v) firewall maintenance sub-policy

Firewall policies and the firewalls themselves need maintenance. There should be a firewall maintenance sub-policy, specifying:

- the events to be logged, where the logs are to be stored, and for how long;
- which events are to be "alarmed", and how they are to be alarmed—for instance, by
- sending an email alert to the network administrator when an "alarmed" event occurs;
- who reviews the firewall logs and how often they are reviewed;
- other firewall subpolicies—for example a requirement for automatic virus-scanner software on the firewall;
- firewall report types;
- firewall auditing sub-policy;
- change control sub-policy for changing the firewall configuration.

(vi) firewall new access request policy

This policy references a procedure for employees requesting access to newly available or existing Internet services, and internal data access via the Internet.

(vii) firewall roles and responsibilities

The level of expertise required for administering the firewall must be specified, as well as assignation of personnel to firewall administration (could be inhouse staff, an outsourcer, or a combination of these). The roles and responsibilities of the assigned staff should be specified.

4.1.11.2 Developing the firewall policy

The team which develops the policy should include a network administrator, system administrators, a financial controller, a legal adviser, a management representative and a user representative (Griffiths, 1996).

Integrating the ideas of Griffiths (1996) and D'Alotto (1996), I suggest developing a firewall policy by:

(i) Determining the firewall policy stance for user access to Internet services.
(ii) Determine method for granting access.
(iii) Determining the business needs of users who require Internet use
(eg communicate with customers) (see Section 4.1.9).
(iv) Determining the Internet services for individual users and groups, which will satisfy
the business needs, and hence the access rules.
(v) Assess risks associated with each service. Minimise this set to reduce risk, taking
cost-effectiveness of proposed firewall controls into account.

Note: Griffiths (1996) points out that the risks for different Internet services are not equal. A risk assessment needs to be carried out for each Internet service, listing the risks associated with each service (eg remote login permitted from outside the company into its networks facilitates 'hacking'), the severity of each risk, and existing countermeasures for each risk. The value of the service should then be estimated, and weighed against the costs associated with risk, to determine whether to permit the service access.

(vi) Set firewall maintenance sub-policy.
(vi) Set firewall new access request policy.
(vii) Determining firewall staff roles and responsibilities.

4.1.11.3 Future directions for firewall policies

D'Alotto (1996) pointed out that the access rules for firewall policies are usually written by firewall administrators in highly technical network router protocol languages, and called for a more corporate-friendly modelling tool to be used by policy-makers for modelling Internet access rules for firewalls. Drake and Morse (1996) supported this suggestion, pointing out that most firewall policy-makers have no way to state their policy requirements. Thus, there appears to be common agreement on the need for a high-level access rule modelling tool for use by firewall policy-makers, which can then be communicated to a firewall administrator for translation into the lower level protocol language.

Drake and Morse went a step further, proposing automated configuration of the firewall in conjunction with specification of the firewall policy itself. This would remove the error risk in allowing firewall administrators to compose and implement the rules.

4.1.12 Internet security technology policy

(refer Section 3.4.4.7 for related discussions)

For each Internet security technology required, there should be a separate policy. For example, if encryption is to be used, there should be an encryption policy. The Internet security technology policy also outlines or references procedures for the selection, acquisition, installation and monitoring of the technologies involved.

4.1.13 Password policy

(refer Sections 3.4.3.5, 3.4.3.6, 3.4.3.9, 3.4.3.12 for related discussions)

Employees should maintain the confidentiality of their passwords by a variety of means, and these recommended means should be specified within the password policy. For example, employees may be required to change their passwords at frequent, scheduled intervals.

4.1.14 Internet acceptable usage policy

The Internet acceptable usage policy (IAUP) is a key sub-policy of the Internet security policy. The policy should be disseminated to each requesting Internet user, and the user must sign his/her consent to the conditions of Internet use set out in it (Pethia *et al*., 1991).

Based on earlier discussions in Chapter 3, I propose the following content for an IAUP, illustrated in Table 4.3.

Internet Acceptable Use Policy	Source
purpose and scope of policy	4.1.14.1
ethics policy	4.1.14.2
Internet services policy	4.1.14.3
confidentiality policy	4.1.14.4
acceptable uses	4.1.14.5
unacceptable uses	4.1.14.6
Internet risks	4.1.14.7
legal policy	4.1.14.8
roles and responsibilities	4.1.14.9
privacy	4.1.14.10
accountability	4.1.14.11
monitoring and surveillance	4.1.14.12
sanctions	4.1.14.13
awareness	4.1.14.14
user consent	4.1.14.15

Table 4.3 Internet acceptable use policy content

4.1.14.1 Purpose and scope of the policy

A statement to the effect that the policy is intended to control employee misuse and abuse of the Internet, assist employees in dealing with external misuse and abuse, and maximise effective business use of the Internet, is required. The employee should also be advised that "use of the Internet is a privilege, not a right".

4.1.14.2 Ethics

(refer Sections 3.4.2.2, 3.4.2.3 and 3.4.8.7 for related discussions)

Employees should be instructed to deal with others on the Internet in an ethical manner. Guidelines for fairness, honesty, trust and politeness (for example, reference to netiquette) may be given. Reference to existing company Code of Ethics may be given. Caution may be advised in communicating with people from different cultures.

4.1.14.3 Internet services

(refer Section 3.4.4.1 for related discussions)

For each available Internet service (ftp, telnet, etc), there should be a policy explaining approved, secure use of that service. The employee should be reminded to only use approved Internet services, and only in the recommended manner.

4.1.14.4 Confidentiality

(refer Section 3.4.3.1 for related discussions)

A statement explaining nondisclosure of confidential business information is required. Employees can be referred to designated authorities or other sources for confirmation or denial of the confidentiality of material intended for Internet publication. There are other policies to consider for inclusion here, such as: employee labelling of postings as "unclassified" in order to ensure employee accountability, should a confidential posting be traced to an employee; and also use of routine disclaimers on non-business email.

4.1.14.5 Acceptable uses

(refer Sections 3.4.4.1 and 3.4.8.1 for related discussions)

Employees should be advised to only use the Internet for acceptable business purposes, in acceptable ways, and within acceptable times or time limits. Plentiful and specific examples of acceptable uses should be provided. The employee should be reminded to use only approved software—if additional software is required, a procedure for obtaining it should be referenced.

4.1.14.6 Unacceptable uses

(refer Section 3.4.3 for related discussions)

Lists of unacceptable uses should be provided, including harassment, unauthorised access, providing low quality data, downloading shareware, personal advertising, personal gain, personal surfing, denial-of-service through excessive Internet use, and plagiarism.

4.1.14.7 Internet risks

(refer Section 3.4.3 for related discussions)

For each Internet risk type in Figure 3-5 (hacking etc), there should be a policy explaining approved, secure use of the Internet in order to reduce the risk.

4.1.14.8 Legal policy

(refer Section 3.4.6 for related discussions)

Employees should be cautioned to adhere to relevant national and international laws (for example, intellectual property and copyright laws).

4.1.14.9 Roles and responsibilities

(refer Section 3.4.4.5 for related discussions)

Employees should be advised of their own roles and responsibilities in secure Internet usage, as well as those of other relevant personnel such as network administrators, the IT security manager, the IT function, business unit managers, corporate training function and the human resources department. Employee responsibilities must include reporting of suspicious Internet events to a designated authority.

4.1.14.10 Privacy

(refer Section 3.4.8.2 and 3.4.8.6 for related discussions)

Policy on company provision of Internet privacy services should be specified. Policy on the level of internal monitoring should be specified, with references to the company's Internet accountability and monitoring policies (see Sections 4.1.14.11 and 4.1.14.12). A statement concerning the level of disclosure of incoming and outgoing email, company web sites, and employee site accesses (to internal parties in the organisation) is required.

Employees should also be warned that their activities and personal data may be recorded and misused at external Web sites without their knowledge, and be advised as to what actions to take on visiting Web sites in order to prevent such recording or misuse. Finally, employees should be warned that their email and other postings may not be private externally, as they may be intercepted externally and read without authorisation (for example, by eavesdroppers or corporate spies).

4.1.14.11 Accountability

(refer Section 3.4.8.5 for related discussions)

Employees should be advised that they will be held accountable for their Internet actions, and the means by which this will be enforced—in particular, any monitoring and surveillance policy (see Section 4.1.14.12 below).

4.1.14.12 Monitoring and surveillance

(refer Section 3.4.8.5 for related discussions)

Employees should be advised of the need for monitoring and surveillance to ensure employee accountability for their Internet actions. They should be advised of any monitoring technology used, internal logging of Internet actions, reporting of unusual events, scanning of email, and other monitoring activities.

4.1.14.13 Sanctions

(refer Section 3.4.8.5 for related discussions)

Compliance with policy must be advised, with a note to the effect that employees are expected to comply with both the Spirit and the Letter of the policy. Employees should be advised of the various sanctions which may be applied on noncompliance with policy. These may range from warnings through to dismissal.

4.1.14.14 Awareness

(refer Sections 3.4.4.3, 3.4.4.4, 3.4.4.5, 3.4.8.4 for related discussions)

Employees should be advised of the comprehensive Internet security management programme which supports the IAUP, as well as management commitment to Internet security and its policies, and the full range of awareness activities existing to inform employees of their Internet responsibilities as well as other aspects of the IAUP.

4.1.14.15 User consent

(Pethia *et al*., 1991)

There should be a signed consent form which each employee must sign, agreeing to comply with the IAUP, as a condition of their being granted Internet access.

4.1.15 Publication policy

There should be a policy detailing guidelines for the division, allocation, electronic publication and dissemination of information over the Internet.

4.1.16 Email policy

I propose an *email policy* composed of subpolicies as illustrated in Table 4.4. As I believe the meaning of each component to be self-explanatory, and in the interests of limiting the size of this thesis, I have not

explained each component. The interested reader is referred to the three listed references for further details.

Email Policy
email ownership
acceptable email usage
email privacy
email encryption
email monitoring
email netiquette
emotional email
avoidance of references to third parties
duties to third parties (eg auditors)
external interception of email
email deletion after usage
distribution of email copies
copyright implications of copy distribution
legal issues
enforcement and dissemination of email policy

Table 4.4 Email policy content

(compiled from Barker *et al*., 1995; Denning, 1993; Farrow, 1998)

4.1.17 Internet virus policy

(refer Section 3.4.3.3 for related discussions)

The virus threat is sufficiently important to justify a policy of its own. This policy can specify available antiviral measures as suggested in Section 4.4.4.3, in order to prevent employee promulgation of viruses to others, as well as to detect and eliminate incoming viruses.

4.1.18 Internet audit policy

(refer Section 3.4.4.4 for related discussions)

A policy regarding the auditing of Internet accesses as well as the Internet security policy itself, is required.

4.1.19 Internet incident response policy

Pethia *et al*. (2000) advised organisations to have an Internet incident response plan, in order to deal quickly and effectively with attacks. Contingency plans, back up procedures and disaster recovery steps must be specified (Griffiths, 1996). The incident response policy should also designate a spokesperson to speak with the media, in any media investigation of an Internet incident. Heard (1996) provided guidelines for an Internet incident response plan, addressing the technical and business issues which may arise after an incident. The IETF (1991) described the development of an Internet incident response policy.

4.1.20 Internet legal policy

(refer Section 3.4.6 for related discussions)

A policy should refer Internet users to relevant national and international laws which must be adhered to, for example intellectual property and copyright laws.

4.1.21 Internet security policy review policy

Griffiths (1996) recommends a policy which stipulates the periodicity of reviewing and updating the Internet security policy. The procedure for policy review and update should also be specified or referenced. This procedure may include a risk assessment of new or changed Internet risks.

4.1.22 Summary

In Section 4.1, I have briefly described the component sub-policies and statements which constitute the Internet security policy proposed in Table 4.1. In the process, I proposed three additional models, the Internet firewall policy content model (Table 4.2), the Internet acceptable use policy content model (Table 4.3) and an Email policy content model (Table 4.4), for the relevant sub-policies of the Internet security policy.

Section 4.2 which follows, outlines a method for the development of an Internet security policy, based on the well-known security concept of risk assessment.

4.2 Development of Internet security policy for organisations

The engineering of information security typically comprises four phases (Abrams *et al*., 1995b):

- a requirements definition phase, culminating in a Corporate Information Security Policy containing layers of policies and procedures;
- a design phase, resulting in a set of security mechanisms which implement the requirements;

- an integration phase, which results in the coordinated security system being put in place; and
- a certification or accreditation phase, which results in a certificate of accreditation being produced, if relevant.

Many methods to develop specific types of information security policies have been described (for example, Olnes, 1994). In Section 3.4.4.2, I pointed out that the Internet security policy should be an issue-specific sub-policy of the corporate information security policy (CISP). Therefore ideally the Internet security policy should be developed at the same time as the CISP, that is, during the requirements definition phase. However, most companies already possess a CISP, and must develop the Internet security policy at a later time. *I assume the latter situation exists, in my proposed method.*

A framework in which to develop an organisation's Internet security policy was proposed in Lichtenstein (1996c; 1997a). It is illustrated in Figure 4-1, and explained below.

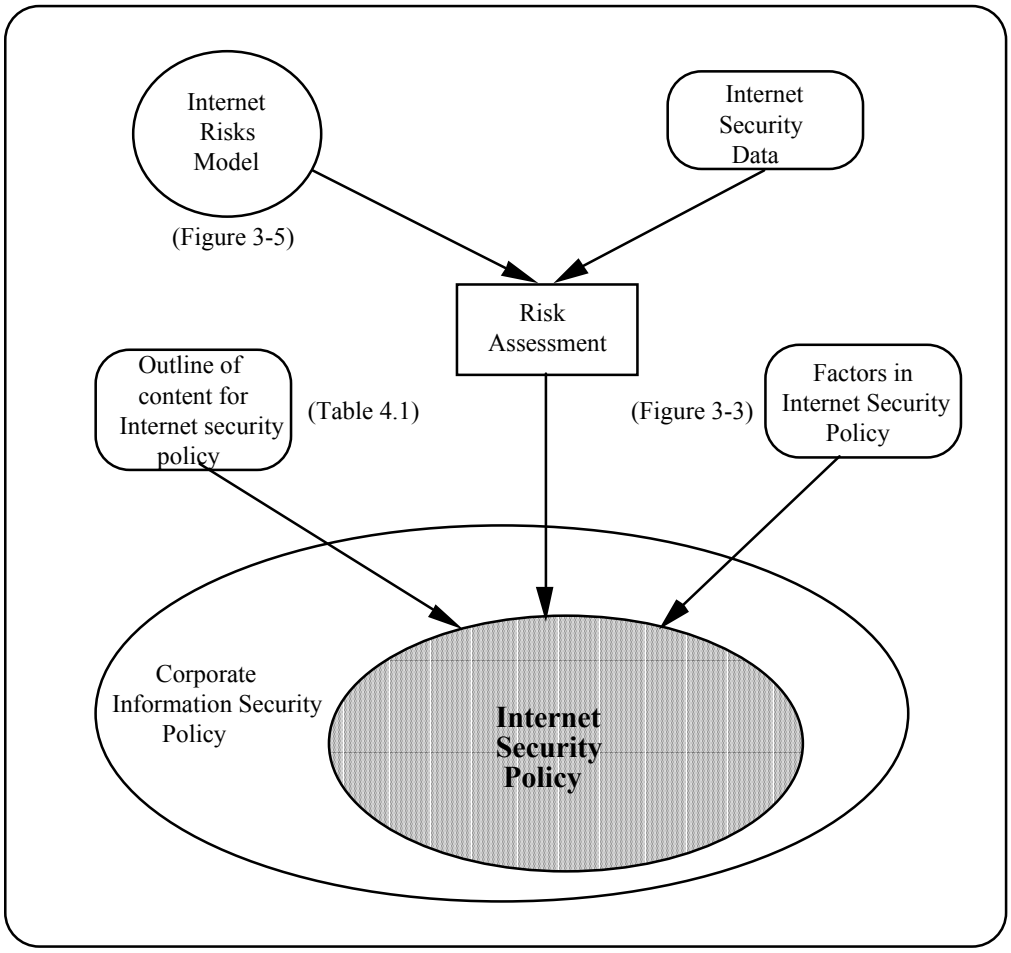

Figure 4-1 Development of Internet security policy for organisations

An explanation of the framework follows. Note that the framework is based on 'risk assessment', a popular technique for identifying information security risks (Baskerville, 1988). I have selected risk assessment based on the recommendations of Bernstein *et al*. (1996), GAO, 1998; Guttman and Bagwill (1997), NIST (1996b) and Stanley (1997). Stanley identified risk assessment as a critical process for improving information security in this new millenium, while NIST (1996b) espoused the principle, “Computer security should be cost-effective”, necessitating a risk assessment process.

The framework shows the Internet risks model (here portrayed by the circle labelled 'Internet risks model', a model that is fully presented in Figure 3-5) in the top left-hand corner. Company-specific Internet data (here portrayed as the curved-corner rectangle labelled 'Internet security data') is shown in the top right-hand corner. The Internet risks model is used in conjunction with the company-specific Internet security data as input into a risk assessment process (here portrayed by the rectangle labelled 'Risk assessment'), in order to determine and prioritise the significant Internet risks for the company.

These risks are then considered, in conjunction with other influential factors in Internet security policy (here portrayed by the curved-corner rectangle labelled 'Factors in Internet security policy', and fully presented in Figure 3-3), in order to construct the Internet security policy itself (here portrayed by the shaded oval labelled 'Internet Security Policy'), in line with the structure proposed by the Internet security policy content model (here portrayed by the oval labelled 'Outline of content for Internet security policy', fully presented in Table 4.1 in Section 4.1). The Internet security policy is clearly positioned within the Corporate Information Security Policy (here portrayed by the oval thus labelled).

The key risk assessment process considers internal and external Internet risks, risks occurring at any of the company network’s external access points, and the level of sensitivity and value of corporate data at risk (Faroughi and Perkins, 1996). 'Risk' can be defined as 'a measurable result of the realisation of a vulnerability' (Ekenberk and Danielson, 1995). As already described, the risk assessment process uses the Internet risks model presented earlier (Figure 3-5), to provide a reference for identifying the possible Internet risks to be assessed.

Calculations of risk for each identified risk and Internet resource that is impacted, can be carried out using estimates of likelihood and impact, historical statistics of actual breaches, available security experts’ professional opinions (Baskerville, 1988) or other methods (Bernstein *et al*., 1996; GAO, 1998; Guttman and Bagwill, 1997). The Internet resources which may be impacted include: corporate data, Internet hardware and software (including Internet services). Corporate data must be valued by its data owners, and the valuation should include replacement or recreation costs (Bernstein *et al*., 1996). Customer data and marketing data are almost always highly valued. Likelihood of risk occurrence and impact for each identified Internet risk are very difficult to place quantitative estimates on, given the current lack of reliable metrics in this area. Hence, a qualitative risk assessment may be preferable, with

each risk being attributed values such as high, medium or low. Guttman and Bagwill (1997) offer an alternative method of qualitative risk assessment.

The risk assessment results are considered in conjunction with a consideration of other factors in Internet security policy (Figure 3-3), and the outline of the content for an Internet security policy (Table 4.1), to determine the Internet security policy.

As discussed in Section 3.4.4.7, and initially suggested by Bernstein *et al*. (1996), an Internet security policy should be developed with the characteristics of *flexibility, pertinence, applicability, implementability, timeliness, cost-effectiveness, enforceability,* and *integratibility* (Bernstein *et al*., 1996). The policy should also be developed with due regard for appropriate information security principles, such as those suggested for modern organisations by Lichtenstein (1995a; 1995b; 1996e). For example, an Internet security policy should feature *human involvement*, as technological controls may not keep up with new risks in a rapidly changing Internet environment.

4.3 Framework for Internet security policy for organisations

I have integrated the three major sets of guidelines for factors, content and development, and their accompanying models, to form a framework for Internet security policy for organisations, as illustrated in Figure 4-2.

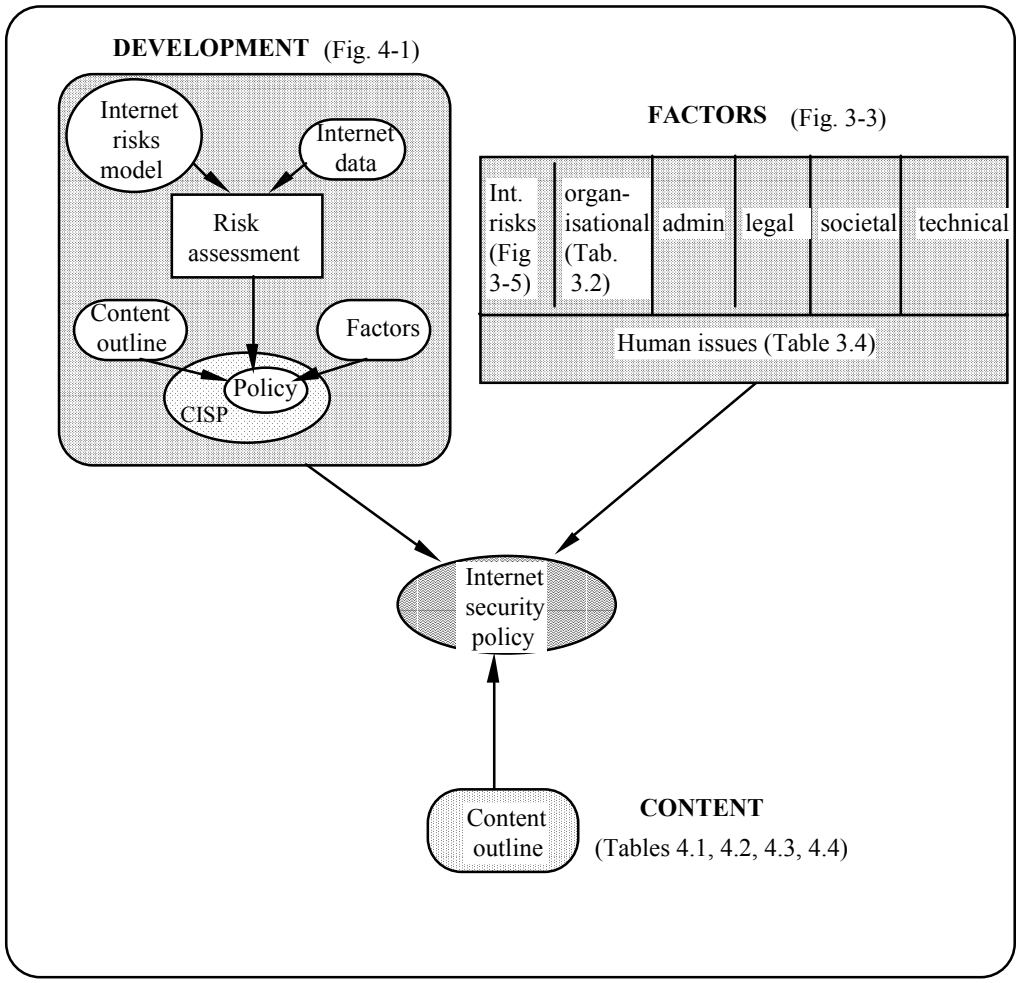

Figure 4-2 Framework for Internet security policy for organisations

I now explain Figure 4-2. The Internet security policy itself is represented by the oval shape in the centre of the diagram.

This policy is *developed* using the Development framework, which is depicted by the large, shaded-in, curved-corner rectangle located in the top left hand corner (*this rectangle contains a sketch of the model presented earlier in Section 4.2 of this Chapter as Figure 4-1*). *Although I described the Development model in Section 4.2, I remind the reader here of the earlier description.*

The Development model shows the Internet risks model (here portrayed by the circle labelled 'Internet risks model', and fully presented in Figure 3-5) in the top left hand corner. Company-specific Internet data (here portrayed as the curved-corner rectangle labelled 'Internet data') is shown in the top right hand corner. The Internet risks model is used in conjunction with the company-specific Internet data as input into a risk assessment process (here portrayed by the rectangle labelled 'Risk assessment'), in order to determine the significant Internet risks for the company. These risks are then considered, in conjunction

with other influential policy factors (here portrayed by the curved-corner rectangle labelled 'Factors', and fully presented in Figure 3-3), in order to construct the Internet security policy itself (here portrayed by the oval labelled 'Policy'), in line with the structure proposed by the policy content model (here portrayed by the curved-corner rectangle labelled 'Content outline', and fully presented as Tables 4.1, 4.2, 4.3 and 4.4 in Section 4.1 of this Chapter). The Internet security policy is clearly positioned within the corporate information security policy (here portrayed by the oval labelled 'CISP').

The Factors model of factors influencing the Internet security policy is depicted as the Factors model in the top right hand corner (*this is a sketch of the model presented earlier as Figure 3-3*). Three models of factor categories are also referenced in this section of the diagram (Internet risks—Figure 3-5, Organisational issues—Table 3.2, and Human issues—Table 3.4), as these three models assist in identifying specific factors in these factor categories. As is shown in the sketch of the Development framework in the top left hand corner of the diagram, the factors are critical input into policymaking.

The content outline for the policy is depicted in the bottom centre of the diagram as the rectangle labelled 'Content outline' (*this represents the models fully presented earlier as Table 4.1, Table 4.2, Table 4.3 and Table 4.4*). As is shown in the sketch of the Development framework in the top left hand corner of the diagram, the content outline is critical input into policymaking.

4.4 Conclusion

In this Chapter, I drew together all the identified factors to arrive at an outline for the content of an Internet security policy (Table 4.1). In discussing each component of the policy, I developed several models for sub-policies of the Internet security policy:

- Internet firewall policy: Table 4.2;
- Internet acceptable use policy (IAUP): Table 4.3; and
- email policy: Table 4.4.

I then proposed a framework for developing an Internet security policy, by drawing together the previous work, and incorporating the well-known security technique of risk assessment (Figure 4-1).

Finally, I presented an overall framework for Internet security policy for organisations (Figure 4-2), showing the three major components (factors, content and development) as well as other developed models.

This framework forms the first-cut model which was an outcome from the subjective/argumentative research method, and was based exclusively on a literature review. In the next two Parts of the thesis,

Preliminary Analysis and *In-Depth Analysis*, I will test this preliminary framework using empirical studies, to determine whether the framework holds good in practice.

Part II

Preliminary Analysis

Chapter 5
Mini-Case Studies

"*If a man does his best, what else is there?"*

(General George S. Patton)

In Chapters 3 and 4, I described the *theoretical analysis* sub-project, building a framework for Internet security policy for organisations (Figure 4-2) from scholarship, a process which involved utilising information collected from a large variety of sources. This Chapter describes the *preliminary analysis* sub-project, in which early indicative support is sought for the framework. In Chapter 2, I noted that two mini case studies which explored the topic area further would be appropriate for this sub-project. The present Chapter describes and analyses the two mini case studies, and presents the results which provide selective support for aspects of the proposed framework.

I undertook both case studies in October, 1996. The case study timings are relevant to this research project, because Internet diffusion is taking place so rapidly that there are changes daily in Internet conditions in almost every organisation.

Hence, I will be taking the time (several years ago now) at which these case studies were conducted into account, in determining the validity of the results obtained.

The first case study (Case A) explores many aspects of the proposed framework, in particular, Internet risks and their possible reduction via policy, *by sourcing data from final year computing/accounting students* at Monash University, a large Australian tertiary institution. The second case study (Case B) focuses on exploring the human issues for Internet security policy in business, *using a different group of final year computing/accounting students* (at a different campus), also at Monash. Both groups of students were about to enter the workforce in 1997. I selected the Monash University environment because it was readily accessible to me, as well as being eminently suitable due to the extensive Internet usage and Internet familiarity of the university students whom I used as the primary source of case data.

In both mini cases, then, I have explored the issues from the Internet user perspective. In Part III, the major case studies, I explore the issues from the corporate perspective.

The next three sections (Sections 5.1, 5.2 and 5.3) describe, analyse and present results from Case A, the first mini case study, while the following three sections (Sections 5.4, 5.5 and 5.6) describe, analyse and present results from Case B, the second mini case study. I conclude with a summary of the Chapter.

5.1 Case A: Internet security policy needs at Monash University

This section describes a case study of Internet security policy needs, conducted at Monash University in October, 1996. This case study concentrates on the special needs of the university's students for Internet security policy.

Selected portions of this case research were published in Lichtenstein and Swatman (1997b).

The study objectives were:

(1) to identify and assess Internet risks for students using the Internet at Monash University;

(2) to determine the value of a university Internet security policy as a control measure against such risks; and

(3) to identify other influences in a university Internet security policy.

As stated earlier, I hoped that by achieving these objectives, I would discover indicative support for aspects of my proposed framework (Figure 4-2).

I initially discuss the case study procedure (sampling procedure, data collection, case instrument, case conduct, and data analysis), then provide a case background sourced from existing corporate documents and informal interviews with relevant institute personnel. I then present the analysis of the case data obtained via the questionnaire, and draw conclusions relating to the proposed framework.

5.1.1 Case study procedure

5.1.1.1 Sampling procedure

The sampling procedure for selecting a unit to investigate as a case study is considered critical (Galliers, 1992). I selected Monash University because of its extensive Internet usage and associated security problems at the time (October, 1996). Furthermore, it met a personal need in being readily accessible, to provide a much-needed indicator—after lengthy scholarship activities—that my proposed framework was on the right track. I (in my role as the researcher) was then lecturing in a computer security subject to a group of final year computing/accounting university students who were highly computer and Internet literate. The largest group of Internet users at Monash is the student population and, hence, a group of final year students already aware of computer security issues constituted a representative, ready and willing source of credible data regarding Internet security policy issues for Monash University.

5.1.1.2 Data collection

I initially collected background data from informal discussions with the university's computer centre personnel, readily available printed documentation at the computer centre and in the Internet-connected university laboratories, and relevant university Web sites. I then collected data about the state of Internet security and the need for policy from the student group to whom I lectured in the computer security subject, *via a personally administered questionnaire to each student*—as discussed below. *Note that scheduled interviews, a common case study data collection technique, were not used in this case study, due to the impracticality of personally interviewing some fifty students in order to gain a sufficient breadth of data to explore and identify the various issues.*

5.1.1.3 Case instrument

A questionnaire (Appendix A), structured according to the Internet risks model (Figure 3-5) (which is considered a key component of the overall framework in Figure 4-2), was used to collect data from the students. There were twelve (12) sections in the questionnaire, one per Internet risk type in Figure 3-5, each section being designed to gather detailed information about the existence and significance of a given Internet risk type at Monash University at the time, and related issues for Internet security policy for effective risk management and improved Internet usage.

Neuman (1994) suggests mixing open-ended and closed questions in a questionnaire, and I incorporated a suitable mix of each type within my questionnaire. Closed questions were employed to elicit a rating using a Likert scale from 0 - 10 for the likelihood of occurrence of each Internet risk articulated in the questionnaire, as well as to elicit a Yes/No response to certain questions (see questionnaire in Appendix A). Open-ended questions were employed at times, for example, to elicit detailed descriptions of risk occurrences, from which I could analyse (to some extent) the impact of those risks which had actually occurrred.

Specifically, for each Internet risk type, students were asked:

(a) to indicate a frequency rating with which the risk probably occurred at Monash University, using a Likert scale (0 - 10) with the following legend:

0 - 2	Rarely
3 - 5	Occasionally (about once a month)
6	Often (about once a week)
7	About once a day
8	About once an hour
9	About once every five minutes
10	About once a minute, or even more frequently

(b) to describe any incidence of the risk at Monash of which they were aware;
(c) to indicate whether a written policy would help control the risk;
(d) to indicate possible risk management advice to be given to students in a written policy; and
(e) to indicate why a policy may not help to control the risk.

The questionnaire allowed data to be collected which would satisfy the three case study objectives, as follows:

(a) To identify and assess Internet risks for students using the Internet at Monash university.

Sub-questions (a) and (b) allowed an informal, indicative risk assessment of the given Internet risk, by using a Likert scale in subquestion (a) to quantitatively estimate the likelihood of a risk occurring, and the students' comments in subquestion (b) to qualitatively assess the impact of a risk (the two major components of *risk* are *likelihood* and *impact* (Baskerville, 1988)).

(2) *To determine the value of a university Internet security policy as a control measure against such risks.*

Sub-questions (c), (d) and (e) provided useful information for this purpose.

(3) *To identify other influences for consideration in a university Internet security policy.*

Sub-questions (b), (c), (d) and (e) provided useful information for this purpose.

It should be noted that the questions did not suggest or evaluate any other types of security measures for controlling Internet risks, as other measures were not the focus of this research.

The wide range covered by sub-questions (a) to (e), included for each Internet risk type, enabled extensive data collection for achieving the case study objectives.

5.1.1.4 Case conduct

The printed questionnaire was distributed to a class of 55 final year computing/accounting students in a normal class period, and completed over one and a half hours. *Only students who had used the Internet extensively over the previous two years (amounting to almost all the students present) were permitted to complete and return a questionnaire.*

The students were informed that the questionnaire was part of a research project in which I was involved, and that their participation was voluntary. Almost all students, being enrolled in a computer security subject, were keen to participate!

I verbally informed students, after distributing the questionnaire, of the three case study objectives mentioned earlier.

49 (out of the 55) students returned a completed, useable questionnaire. In some cases, students left entire questions unanswered, or only answered selected parts of questions, and I took this into account in deciding how to proceed with data analysis.

5.1.1.5 Data analysis

I collated responses within each Internet risk type category, then analysed them to determine:

- whether students felt an Internet security policy could be helpful in reducing that risk type;
- recurring reasons why students lacked faith in the power of a policy for risk
- management of that risk; and
- recurring advice (for management of that risk) which students suggested for inclusion in a written policy.

In view of the small size of the student sample and its comparatively unrepresentative nature (comparing it with the total number of student Internet users at a large university), I did not endeavour to provide a quantitative analysis, that is, statistical calculations based on the results, believing rather that a *qualitative* analysis was appropriate to provide an indication of student opinion of Internet risks in their Internet usage, and possible control of these via a written policy.

5.1.2 Organisational background and Internet infrastructure

The organisation under investigation is a large Australian university, Monash University. During 1996, Monash was experiencing increasing problems with its Internet usage, according to plentiful anecdotal evidence supplied by students and staff with whom I worked closely or interacted in various ways in my role as a faculty member. The largest group of Internet users at Monash is the student population, and therefore this case study concentrates on the special needs of the university's students for Internet security policy.

The university has some forty thousand students overall, although the majority of students did not at that time make use of the Internet connection facilities provided. The computer-literate students undertaking information technology courses were (and still are) the main student users. Student Internet usage had grown from several hundred users a few years earlier to several thousand student Internet users by

October, 1996, comprising undergraduates in their late teens to mid-twenties age range and postgraduate students whose ages primarily ranged from their twenties to forties. The students were of many different nationalities, with approximately one third being from Asia.

At that time, Monash had many hundreds of workstations in laboratories (located at several sites), connected to the Internet via various internal Web servers linked to the Australian Academic Research Network (AARNet), which is an internetwork of regional (state) networks connected within Australia and internationally to other Internet participants, by Telstra Internet Services (Telstra is the new name of Australia's former PTT, now a major common carrier competing with other, similar organisations. AARNet is now operated by Cable & Wireless Optus).

In the main, students gained Internet connection from these workstations, although many students also used dial-up facilities from home or elsewhere. Each university workstation had its own Internet connection. The university's intention in permitting and encouraging Internet connection has been to allow and encourage research, communication, collaboration, information sharing and management, and access to software, in order to fulfil the academic aims and objectives of the various courses.

5.1.3 Internet security at Monash: abuse and misuse

There had been a number of serious security incidents relating to Internet usage at Monash, as would be anticipated in a large tertiary organisation. For example, hackers had broken into the university's systems at different times, and hackers from within the university had attacked safety-critical and security-critical external organisations (for example, one ex-student had hacked into NASA (Branigin, 1991)). Abuse and misuse was handled informally at the time. Monash was aware of Internet risks via the plentiful and regular media publicity given to Internet misuses and breaches in other organisations worldwide.

The university lacked formal Internet security management. There was no formal Internet security strategy, Internet security programme, Internet security policy or Internet acceptable usage policy. *There was, however, a set of computer use regulations in place which treated Internet security or Internet acceptable use matters in a cursory manner.*

The university was subject to the acceptable use policy of AARNet (1995), and therefore also to the policies of Telstra Internet Services, although student users did not, at the time of the study, consult these policies. There were also several firewalls in place to protect isolated parts of the organisation, and plans existed for the development of additional firewalls. Security policies for those firewalls did not provide much protection (via filtering rules or special software such as antivirus software) for student Internet use. Various other technical Internet security measures were in place throughout the organisation—for example, antivirus software was available for students if required.

5.1.4 Case analysis

The analysis which follows is structured according to the Internet risk types in Figure 3-5.

The corresponding question from the questionnaire is indicated following the risk title for the section.

5.1.4.1 Accidental disclosure (question (vi) on questionnaire)

Students knew very little about this risk incidence, commonly assigning this a value of between 2 and 5, while being unable to cite specific incidences and were unable to advise as to how this type of risk could be controlled through policy. *A few students suggested issuing a warning, and stipulating sanctions, in a policy.*

5.1.4.2 Accidental/erroneous business transactions (question (iii) on questionnaire)

Students strongly related to the experience of sending email to an incorrect email address, rating this risk type at around 8. This would be expected in a learning environment where the age group is predominantly young (and often careless!). Most students did not recognise that a policy could help, asserting that accidental risks could not be addressed within policies. Other students, however, realised that a policy could help, for example, by advising students to double-check the email "send" address prior to despatching email.

5.1.4.3 Corrupted or erroneous software (Question (i) on questionnaire)

This risk type was rated as reasonably frequent, with typical responses in the range 2 to 6. Students mentioned downloading “buggy” software or viruses via shareware sites or FTP.

Many students believed that a policy would help control this risk type. Suggestions made for a policy included:

- advice on recognising risky sites and software prior to downloading;
- advice to scan downloaded software for viruses, prior to use of software;
- advice on virus-avoidance procedures;
- advice on how to use available antivirus software; and
- advice against downloading software from other than a recognised, reputable source or organisation.

Many other students believed that a policy would not help, as:

- students will take this risk anyway, in order to obtain the software; and
- accidental risks could not be controlled by policy (students mistakenly think that only deliberate risks can be controlled by policy).

5.1.4.4 Denial-of-service *(question (ix) from questionnaire)*

All students rated this in the range 0 - 2, and were unable to cite specific incidences other than general slowing of Internet traffic for unknown reasons. *A few students believed that a policy would help to control this risk type, making suggestions such as "stop Internet surfing!"*

5.1.4.5 Fraud *(question (xi) from questionnaire)*

All students rated this with a 0 rating, being unable to cite specific instances. This is as one would expect around October, 1996, at which time electronic commerce transactions were comparatively rare.

5.1.4.6 Hacking *(question (ii) on questionnaire)*

Students varied in their rating of this issue, most rating it between 1 and 5, and typically around 3, although some students rated it as high as 7. These figures suggested that hacking may have been happening as often as once a month, and that the impact may have been severe. Some students were able to cite specific incidences, although many did not know of specific incidences, despite being aware that hacking was, indeed, occurring. Students who did cite incidences referred to the hacking of their internal accounts by others (note that this may not have involved the Internet), and a few cited an isolated, headline-grabbing international incident involving NASA, from several years earlier (Branigin, 1991).

Many students believed that a policy would help control this risk type, and made suggestions including:

- indicate the severity with which hacking is regarded;
- specify severe sanctions for hacking;
- advise how to avoid hacking;
- advise how to protect one's authentication mechanism, for example, safeguarding one's password; and
- advise how to recover after hacking.

Many students also commented that a policy would not help, as:

- hacking would still occur (hacking was fun, hackers knew how to avoid being caught, hackers could crack any system, etc.);
- hackers may be non-students, and therefore policies would not apply; and
- people who liked hacking disregarded laws anyway, and policies were essentially laws.

5.1.4.7 Inaccurate advertising *(question (iv) on questionnaire)*

Students rated this with very varied values within the range 0 - 7. Few were able to discuss this risk or cite an incident. Many gave the rating 0, indicating a blissful lack of awareness of the possibility of inaccurate advertising material on Web sites or in postings.

A few students believed that a policy would help control this risk type, making suggestions such as "educate students to differentiate between personal opinion and fact on Web sites".

Some students asserted that a policy could not help, mistakenly believing that "internal policy cannot control an external risk".

5.1.4.8 Inappropriate email *(question (vii) from questionnaire)*

Most students rated this risk type at around 5, frequently citing the receipt of chain mail as well as email harassment from other students (including students at other institutes to which Monash was connected via the Internet). Some students disclosed the email addresses of others to chat groups, and these addresses were then bombarded with email!

Some students cited receipt of email from commercial companies which had obtained their email addresses in some way. It was felt by the majority that a policy could not control this risk type.

A few students believed that a policy would help to control this risk type, making suggestions including "advise students not to send junk email".

5.1.4.9 Low quality data *(question (iv) on questionnaire)*

This risk type was rated between 2 and 7, with a typical rating of 5. Students were given the following examples of this risk type: viewing inaccurate Web pages, viewing inaccurate data from another organisation's database, or receipt of inaccurate email. Many students described the receipt of email hoaxes informing of viruses, the receipt of low quality email via mailing lists, impersonation of email sender in email, receipt of email with corrupted message bodies, inaccurate Web page content (for example, "information about various music bands was inaccurate"), and low quality Web pages (with misleading or ambiguous content).

A few students believed that a policy would help control this risk type. Suggestions made for a policy included:

- authenticate Web page data with an authority; and
- advise that not all Web page information is accurate.

Most students, however, did not believe that a policy would help, commenting (due to lack of awareness) that policies cannot control accidental risks.

5.1.4.10 Non-business usage *(Question (v) on questionnaire)*

The majority of students gave this a frequency rating of 8, 9 or 10, indicating that there was indeed a significant level of frivolous Internet usage. One student commented that "85% of the university Internet usage will be for these activities". Student after student stated that many students were occupying the computers for non-university Internet purposes, preventing those having a more serious or academic purpose from using the computers.

Within this particular risk type, students were asked to rate the frequency of occurrence of the following risks:

(i) excessive personal email

The majority of students gave this a rating of 8 or 9. One student's explanation for this was that "Students use Internet email as a social tool". Many students apparently regularly sent personal email to overseas locations.

(ii) surfing

This rated between 6 and 10, and often scored either 8, 9 or 10. It was commented on by many students, with most comments being of the following kind: "Students with spare time, or who are bored, always/often surf the Internet".

(iii) downloading games and images

This was very highly rated, mostly scoring from 7 to 10. Many comments were made about students downloading pornographic/dubious images from the Internet. One comment stated that this occurred during tutorial time (when tutors were in the room), remarking "That should be stopped immediately". Significant numbers also commented on the playing of noisy, multi-user games in the laboratories—for example, one student stated "I personally hate this kind of attitude". Another referred to "rooms full of people playing games".

(iv) newsgroups and mailing lists

This was highly rated, mostly scoring from 6 to 10.

(v) Internet relay chatting (IRC)

This was highly rated, mostly scoring from 6 to 8.

Most students believed that a policy would help control this risk type. Many suggestions were made for such a policy, including:

- informing students of those Internet uses which were considered to be misuses;
- warning students that only legal Web sites may be visited;
- limiting time for student Internet usage, for example to two hours per week;
- only permitting Internet usage in some of the laboratories, rather than in all of them;
- forcing students to give up computers which are being used for non-academic reasons to others who intend to do valid, academic work;
- filtering transactions to and from student accounts;
- spot checking of the laboratories to detect misuses;
- banning of multiuser games; and
- specifying the consequences of frivolous misuse (suggestions ranged from denial or closure of student accounts to expulsion from the institute).

A significant proportion of students did not believe a policy would help with this risk type, many giving reasons such as:

- students would misuse these facilities irrespective of policy (typical comments: "it can't be stopped", "the Internet is just too attractive" and "it's uncontrollable");
- the purpose of the Internet is to share information;
- difficulty in differentiating valid from frivolous usage;
- a policy would not work unless it were monitored; and
- no-one reads policies.

5.1.4.11 Pirated media (question (x) on questionnaire)

Piracy was rated very highly (7 to 10) by almost all students, with several citing the downloading of software with limited trial periods which are deliberately exceeded by students.

Many students believed that a policy would help control this risk type. Suggestions made for a policy included:

- severe sanctions;
- warnings of legal liabilities; and
- raids by university authorities.

Many students commented that a policy would not help, as:

- software is far too expensive for students to purchase legally; and
- students will always try and obtain software the cheapest way.

5.1.4.12 Theft of information *(question (xii) on questionnaire)*

Students rated this between 2 and 6, with a typical rating of 3. Some students cited the unauthorised reading of email by other students, while others referred to knowing students who sometimes copied large chunks of information from various Web sites.

5.2 Case A: Results

The case analysis in the previous section clearly indicates the need at that time for managerial measures to address an obvious problem in student Internet usage at Monash.

The managerial measure suggested to the students—the Internet security policy—was recognised by the students as a viable measure judging by many of the positive suggestions for such a policy, along with strong indicators for policy support from other measures such as awareness activities (as will be discussed later in this section).

Many comments were indeed made about the usefulness of an Internet security policy in controlling the perceived Internet risks. Aside from those mentioned in the case analysis, the following comments were also made many times over:

- policy should be distributed when students first register;
- policy is essential for eliminating the liability of Monash should a breach occur;
- there should be policing of policy, and sanctions for misuse; and
- support is required for written policy.

However, cautionary comments also made many times over against Internet security policy for all the risk types, included:

6 using the Internet is fun, and therefore policy will be unsuccessful;

7 students do not check or follow policy ("too lazy", "won't read it", "will forget it", or "won't listen")—until confronted with a related problem;

8 some students will always deliberately break rules; and

9 there is no way to enforce a policy.

One can only conclude that there are many complexities involved in achieving effective Internet security policy for organisations.

Via this case study, I gathered data which indicate support for two of the three components of the overall framework for Internet security policy (Figure 4-2), as will be shown in the remainder of Section 5.2. (The sole component *not* directly addressed by the collected data is the *Development of Internet security*

policy model (Figure 4-1). It would be unreasonable to expect students to contribute ideas directly to this aspect of the policy.) The two components that were supported are: *Factors in Internet security policy* (Figure 3-3 and related models), and *Internet security policy content* (Table 3.4 and the component model for the IAUP content, Table 3.6). Sections 5.2.1 and 5.2.2 discuss support provided for these two major components of the overall framework.

5.2.1 Support for Factors model

This section examines support provided for the *Factors in Internet security policy* component (Figure 3-3) of the proposed overall framework (Figure 4-2), by the case analysis. One section follows for each of the seven proposed types of factors: Internet risks, organisational, administrative, legal, societal, technical and human issues.

5.2.1.1 Internet risks

The case analysis provided in the previous section signals the existence of significant Internet risks at Monash, of the types suggested in Figure 3-5 (the Internet risks model) which forms a vital component of the proposed framework, as will be shown in this section. As it proved quite difficult (and indeed, perhaps too much to expect from students aged about 20, who lacked experience in truly understanding risk impact) to gain an idea of the significance of the impact that each risk had, from the risk incident descriptions provided by the students, I decided to use the risk likelihood estimates provided by the students, as summarised in Table 5.1, as an indicator of each risk's presence and significance at Monash.

Internet risks at Monash University	Risk likelihood (0 - 10)
Accidental disclosure	2 - 5
Accidental erroneous business transactions	8
Corrupted or erroneous software	2 - 6
Denial-of-service	0 - 2
Fraud	0
Hacking	1 - 5
Inaccurate advertising	0 - 7
Inappropriate email	5
Low quality data	2 - 7
Non-business usage	8 - 10
Pirated media	7 - 10
Theft of information	2 - 6

Table 5.1 Internet risks at Monash University

The risks listed in the first column are those I have suggested in my Internet risks model (Figure 3-5) which forms part of the overall framework in Figure 4-2. From this table, it is clear that all Internet risks—except fraud—were considered to be of some significance (some more than others).

The fact that fraud was not noted is not an indicator that it should be eliminated from the proposed model. Firstly, this is only the first empirical study in this research project, with limited data sources, and therefore it would be foolish to generalise from the data obtained. Secondly, students themselves are unlikely victims of fraud as there are no student financial data stored and accessible via the Internet. Thirdly, if the students themselves were carrying out fraudulent activities at external locations through hacking, this may not have been picked up by the companies or individuals who were defrauded, nor reported in the media or through proper university channels (by which students could be informed).

The most significant Internet risks at Monash were indicated to be:

- *accidental erroneous business transactions*: The particular risk that students related to in this category was misdirected email. This is to be expected in a learning environment populated by young, eager, hasty and incautious students.
- *non-business usage*: Students referred to excessive, service-denying, personal email, personal surfing, downloading of games and images, use of newsgroups and mailing lists, and Internet relay chatting. It is easy to see the temptation provided for students by the Internet presence, which led to this misuse.

- *pirated media*: Students described frequent downloading of unauthorised and illegal software, as might be expected from a fairly "poor" section of the community, who need these resources for academic purposes, peer group pressure purposes, or purely fun.

It is clear that the Internet risks data provided by the case lends indicative support to the proposed model of Internet risks (Figure 3-5).

5.2.1.2 Organisational factors in Internet security policy

Table 3.2 suggested the following broad categories of organisational factors which influence Internet security policy: organisational objectives, Internet security infrastructure, management commitment, Internet security management programme, Internet security awareness, policy integration, and principles for Internet security and policy.

Organisational objectives: Students related tales of Internet usage for non-university purposes. There was no awareness by students of any Internet strategy stipulating usage following from Monash University objectives. Students were uncertain as to those permitted Internet usages which would be considered valid for support of their studies.

Internet security infrastructure: There was no Internet security plan, strategy, or student-known Internet security philosophy—although the adopted Internet security posture seemed to be "permissive"—everything was allowed except what was explicitly forbidden. The lack of an infrastructure was reflected in the existing security problems and uncertainty in Internet acceptable usage.

Management commitment: Students lacked personal contact with any managerial representatives to instruct them of "the right things to do". There was no policy indicating top-level university support for "reporting security incidents" or behaving in a responsible manner in Internet usage.

Internet security management programme: The lack of a programme of policies, procedures, training and awareness activities, access restrictions and monitoring, compliance procedures including sanctions, an Internet plan and advanced technologies was reflected in student uncertainty and widespread misuse of the Internet facility. Three examples serve to illustrate this claim:

- One student referred to "rooms full of people playing games", indicating inadequate monitoring.
- Many students constantly referred to the belief that policies could not control accidental misuse of the Internet, highlighting inadequate Internet awareness activities at Monash.
- Many students suggested limiting Internet usage time in order to allow valid laboratory work, indicating inadequate access restrictions.

Internet security awareness: Many students referred to policies being of no use, as "students don't read policies" "students are too lazy to read policies", "students forget policies" and "students deliberately flout policies". This highlights the need for plentiful awareness activities supporting the policy, which should, themselves, be documented within the policy.

Policy integration: Many students were unaware of other policies which already existed, such as computer use regulations at Monash, highlighting the importance of referencing other policies to be complied with, within an Internet security policy.

Principles for Internet security and Internet security policy: Students referred over and over to the principle of "enforceability" (suggested by Bernstein *et al*. (1996)) (note: students did not use this term, of course)—that is, any written policy must be enforceable in the existing environment. This example illustrates the need for a set of Internet security and policy principles.

5.2.1.3 Administrative factors in Internet security policy

Matters to do with administrative procedures were not able to be determined from the questionnaire data collected from students (rather than administrators), however it was evident that procedures for Internet security matters were not achieving the desired level of security. This supports the defining of administrative procedures as part of (a) policy.

5.2.1.4 Legal factors in Internet security policy

Students referred to obvious breakages of specific laws (for example, intellectual copyright laws), but had at best a hazy understanding of the existence of many other laws relating to Internet usage. The law most frequently referenced was the "anti-piracy law" which was never once referred to by its rightful title of "intellectual property"! The hazy awareness by students of law breakages supports the inclusion of legal factors as an influence on policy.

5.2.1.5 Societal factors in Internet security policy

Students referred to unethical global practices, such as supplying international chat groups with email addresses of fellow students, who were then bombarded with email. Students referred to receiving harassing email messages from other students, many of whom were from different cultures (Monash has had a large contingent of overseas students during this decade). The need for netiquette standards (as part of a policy) to avoid unintentional harassment is obvious.

5.2.1.6 Technical factors in Internet security policy

Students referred to risks which could be reduced by new technologies. For example, misdirection of email could be reduced by installing email clients which prompt students to check the send addresses prior to despatching. Firewall filters could be employed to eliminate resource-hungry, non-university accesses to many unscholarly newsgroups, IRC's and dubious sites. Requirements for such technologies should be part of a policy.

5.2.1.7 Human issues in Internet security policy

Human issues included in the human issues model (Table 3.4) are: freedom of Internet use, privacy, censorship, right to be kept informed, accountability, ownership and ethics. This case study did not attempt to draw out the human issues, although some were inadvertently touched upon (the focus of the *second* mini case is human issues). Hence, I will not attempt here to discuss each of the human issues from my proposed model. Instead, I illustrate the problem of human issues via four examples:

- Personal student "ethics" was questioned when students referred to other students utilising the limited Internet resources for non-university purposes, as well as piracy.
- Some students objected to the idea of a policy, making comments such as "using the Internet is fun"—an indication that new Internet restrictions may meet with objections (the "freedom of use" issue).
- Students also referred to the need to be "kept informed" of policy if it existed.
- Students referred to being bombarded with email from people who had obtained their email addresses without authority—a privacy issue.

5.2.1.8 Summary of case support for the Factors model (Figure 3-3)

At the beginning of Section 5.2, I highlighted the need for an Internet security policy at Monash university, and the complexity of obtaining an effective policy. The above discussion has given clear support (to varying degrees) for all the major factors proposed in Figure 3-3: Internet risks, organisational, administrative, legal, societal, technical and human issues. Support was indicated for addressing all the Internet risks in Figure 3-5 with the exception of fraud (which was to be expected); all the organisational issues included in Table 3.2 (administrative issues, legal issues, societal issues, technical issues, and several of the human issues listed in Table 3.4, within the Internet security policy.

5.2.2 Support for model of content of Internet security policy

The case data analysis in Section 5.1.4, as well as the discussions of indicative support for the *Factors in Internet security policy* model (Figure 3-3) presented in Section 5.2.1, suggest certain *direct* support for

the model of *Internet security policy content* (Table 4.1) as well as for the model of an IAUP (Table 4.3), as summarised in Tables 5.2 and 5.3.

Internet security policy content	Supported
Purpose and scope of policy	
Philosophy of policy	•
Internet security infrastructure	•
Internet security management programmme	•
Other applicable policies	•
Internet privacy policy	•
Internet censorship policy	
Internet responsibility and accountability policy	•
Internet information protection policy	
Internet information access policy	•
Internet firewall policy	•
Internet security technology policy	•
Password policy	
Internet acceptable usage policy	•
Internet publication policy	
Email policy	•
Internet virus policy	•
Internet audit policy	
Internet incident response policy	•
Internet legal policy	•
Internet security policy review policy	

Table 5.2: Internet security policy content support in Case A

Note: Those aspects directly supported are bulleted. This does not mean that the unbulleted components are not required, rather that only data relating to the bulleted components was gathered in this particular case.

I have not justified the indicative support for the bulleted sub-components yet again in this section, as there is adequate evidence already provided in Sections 5.1.4 and 5.2.1.

Internet acceptable use policy	Support
purpose and scope of policy	•
ethics policy	•
Internet services policy	•
confidentiality policy	
acceptable uses	•
unacceptable uses	•
Internet risks	•
legal policy	•
roles and responsibilities	•
privacy	•
accountability	•
monitoring and surveillance	•
sanctions	•
awareness	•
user consent	•

Table 5.3 Internet acceptable use policy content support in Case A

I remark here that I did not analyse support for the models of email policy (Table 4.4) and firewall policy (Table 4.2), as these two important issues were not investigated in sufficient detail via the case instrument. Indeed, it is highly unlikely that students would be able to provide detailed information regarding firewall policy. Hence, little usable data in either area were supplied by the students.

5.3 Case A: Summary

In the previous sections, I analysed case data collected from the Monash University case, and presented the results of the case study which clearly indicated support for many aspects of *two* (out of the three) key components of the overall framework—these are: *Factors in Internet security policy* and *Internet security policy content* (and within that, *Internet acceptable usage policy content)*. I was not able, in this particular study, to provide support for the third component (*Development of Internet security policy*), as data for this purpose were neither sought specifically, nor inadvertently obtained, via the case instrument.

These results are indicative of support for noted aspects of the framework, with some significant limitations. Firstly, the organisation studied here was from the educational industry sector, and therefore the results could not be generalised, on their own, to other industry sectors such as commercial industries. Secondly, the only perspective studied in this case was that of the students—*the Internet users*. The other

major perspective to be taken into account in policy is that of the *employer*. In the major case studies in Part III, I study the *employer* perspective of Internet security policy.

In the next three sections, I describe and analyse Case B, the second mini case, which lends further indicative support for part of the overall framework.

5.4 Case B: Human issues in Internet security policy at Monash University

This section describes a second mini case study of human issues in Internet security policy for organisations, conducted at Monash University in October, 1996. *Note that the students participating were a different group to those participating in Case A.*

I judged the area of "human issues" to be of great importance in this project, as highlighted by my proposed model of the Factors in Internet security policy (Figure 3-3), in which all factors must be viewed through the filter of related human issues, and hence I was very keen to obtain some rapid feedback to determine whether my proposed model of *human issues in Internet usage* (Table 3.4) had an empirical basis, as well as being keen to explore each issue in more depth.

I was also interested in obtaining some guidelines for current Internet acceptable usage policies, such as "How much freedom of Internet usage do employees expect?" and was aware that many companies were (and still are) struggling to determine acceptable levels of employee Internet usage. Acceptable usage guidelines should be determined after considering the viewpoints of *all* stakeholders. The two major players here are the company itself (represented by management) and the employees. I anticipated (correctly, as it turned out) that there would be two very different views expressed by these two players as to what would be "rightful" and "proper" in Internet acceptable usage. This case study, by exploring the expectations of final year accounting/computing students about to enter the workforce, in human issues for Internet acceptable usage and security within organisations, makes an attempt to determine the employee perspective of human issues in Internet acceptable usage. The four major case studies in Part III of this thesis explore the other perspective—that of the employer.

Formally, the case study objectives were:
(1) to identify human issues in Internet security policy for organisations ;
(2) to determine employee expectations for acceptable Internet usage and related human issues, in an organisational Internet security policy;
(3) to identify possible guidelines for Internet acceptable usage, given the identified human issues as well as employee expectations, from the employee perspective.

I hoped that, by achieving these objectives, I would discover indicative support for the human issues model component (Table 3.4) of the Factors in Internet security policy model (Figure 3-3).

I initially discuss the case study procedure (sampling procedure, data collection, case instrument, case conduct, and data analysis), then give a brief background to the case environment. Finally, I present an analysis of the case data obtained via a questionnaire administered to students, and draw conclusions relating to the proposed framework.

5.4.1 Case study procedure

5.4.1.1 Sampling procedure

I selected Monash University once again (*note: a completely different group of students from those studied in Case A was investigated—indeed, the students for Case B were located on a different campus*) for investigating human issues in Internet security policy, as Monash featured extensive student Internet usage and associated security problems at the time (October, 1996), and hence, students (especially computer security students in the final year of accounting/computing courses, who were readily accessible to me, and were also keen to participate in this fascinating and topical area) possessed reasonable knowledge of related issues.

These students were used to represent the thoughts and expectations of young employees in the workforce (which the vast majority of them would indeed be, several months later). It was not feasible to arrange a case study with another company as quickly, or to gain detailed and credible data in any such company from as many Internet-experienced and computer-security-aware employees of a similar demographic background (in this case, their age-group—almost all aged between 20 - 22 years). I refer the reader to Section 5.1.1.1 for further justification of the choice of the students within this computer security student group (to whom I lectured at the time).

5.4.1.2 Data collection

I had already obtained (for Case A) background data from informal discussions with the university's computer centre personnel, readily available printed documentation at the computer centre and in the Internet-connected university laboratories, and relevant university Web sites. I then collected data about human issues in Internet security policy from a student group to which I lectured in a computer security subject (as discussed in the previous section), *via a personally administered questionnaire to each student*—as is discussed below. *Note that scheduled interviews, a common case study data collection technique, were not used in this mini case study (as in Case A), due to the impracticality of personally interviewing some seventy students in order to obtain a sufficient range of individual experiences to explore and identify the various issues.*

5.4.1.3 Case instrument

A questionnaire (Appendix B) was used to collect data from the students. There were seven (7) sections in the questionnaire, as follows: Internet usage; Internet privacy; censorship; monitoring; compliance and sanctions; netiquette; and responsibilities, duties and accountability. I designed each section to relate to important human issues as they might be perceived by the students, rather than structuring it strictly according to the proposed human issues model.

I incorporated a mix of open-ended and closed questions within the questionnaire. Closed questions were employed in order to uncover patterns regarding issues where the student may not otherwise have been aware of typical business decisions. As one example, five possible sanctions were listed for the student to choose from, so that I could determine the most acceptable choice(s). If I had left such a question open-ended, I might not have gained a consensus, due to lack of student awareness of typical business choices for sanctions for Internet misuse or abuse. I also elicited Yes/No responses to certain questions, again for pattern-detection purposes (see questionnaire in Appendix B). Open-ended questions were employed at times, for example, to elicit suggestions about how to make a policy work, from which I could pick out popular and viable suggestions.

5.4.1.4 Case conduct

The printed questionnaire was distributed to a class of 79 final year computing/accounting students in a normal class period for their computer security subject, and completed over one and a half hours. *Only students who had used the Internet extensively over the previous two years (amounting to almost all of the students present) were permitted to complete and return a questionnaire, as for Case A.*

The students were informed that the questionnaire was part of a research project in which I was involved, and that their participation in it was voluntary. Again, almost all students, being enrolled in a computer security subject, and being highly interested in issues likely to affect them in their future employment, were keen to participate.

I verbally informed students, after distributing the questionnaire, of the three case study objectives mentioned earlier. *I also instructed them, as did the questionnaire (see Appendix B), that they were to imagine that they were employees in an Internet-connected business, when considering the issues addressed by the questionnaire.*

72 (out of the 79) students returned a completed, usable questionnaire. In some cases, students left entire questions unanswered, or only answered selected parts of questions, and I took this into account in deciding how to proceed with data analysis.

5.4.1.5 Data analysis

I collated responses for each category, then analysed them in order to detect patterns and special issues. In view of the small size of the student sample and its comparatively unrepresentative nature (comparing it with the total of all student Internet users at Monash), I did not endeavour to provide a quantitative analysis, that is, statistical calculations based on the results, believing rather that a *qualitative* analysis is appropriate here to provide an indication of student opinion of human issues in Internet security policy for organisations, which may affect their eventual Internet usage at work.

5.4.2 Organisational background and Internet infrastructure

An introduction to Monash University and student Internet usage there has already been provided in Sections 5.1.2 and 5.1.3.

5.4.3 Case analysis

The analysis which follows summarises responses and patterns for each question, using the questions themselves as headings.

5.4.3.1 Internet usage

(i) How do you feel about your right to freely use the Internet at work?

For example, do you think you should be able to use the Internet freely for non-business purposes as well as business purposes all day? Do you think you should be restricted to, say, two hours per day Internet usage in total? Or some other time limit?

Most students believed in business-only usage within work hours, but that they should be free to use the Internet for two hours a day for non-business purposes during lunchtime or after finishing work. Illustrative comments representing this view were:
"People are paid to work while at work—this implies no non-business usage....people should regulate their usage, including how much and when, eg during lunch break, or after hours. Excessive use would be that which affects their work output, or other people's, badly."
"The Internet should be available at all times for business purposes. But for non-business purposes, only at lunch-times, as long as the load on the system isn't high or (use) eats into work time."

Many students believed they should be able to freely use the Internet as long as they got their work tasks done. For example:

"I believe that since I am given the right to access the Internet, there should be no restriction to when I can use it, as long as I perform my job."

Quite a few believed in totally free use of the Internet as it would help them gain useful job skills, stumble upon useful information, etc. For example,
"Not only can the Internet be used for business purposes but also to improve on the employees' knowledge of other useful information which could contribute towards achievement of the company's goals."

(ii) How many hours a day of non-business usage would you accept as reasonable, if a limit were to be imposed?

Most students believed in two hours of non-business use per day, either during lunchtime or after hours. However, a few students thought that three, four, five, even ten (!) hours were reasonable.

(iii) Do you believe in your right to use personal email across the Internet during work hours?
(Yes / No)

Most students responded Yes, with comments such as:
"If my employer refused to provide this, I would buy my own access at work and expect to be allowed to use it."
However, provisional usage was suggested via comments such as:
"Not too often though."
A few students responded No, feeling that there should be no personal Internet use during employer-paid time—including personal email.

(iv) Would you do so if given the opportunity? (Yes / No)

Most students responded Yes, indicating that if a facility were made available at work, then they would use it. Again, provisional usage was advised, for example:
"But not all day".

(v) *Do you believe in your right to download games and non-business images across the Internet during work hours?* (Yes / No)

Most students responded No, indicating that, while personal email feels comfortable for most, this type of use is unnecessary. A typical comment was:
"These consume large amounts of resources".

However, a few students responded Yes, indicating that there are people around who think that everything the Internet offers is their right to use at work—a worrying prospect.

(vi) Would you do so if given the opportunity? (Yes / No)

Most students responded Yes (despite having replied No to the previous question!), highlighting yet again the reality that if a facility is made available at work, it will be used.

(vii)Do you believe in your right to have an employee home page for which you have complete freedom in its design? (Yes / No)

About three-quarters of the students responded Yes, with occasional provisos, for example:
"However this might contradict what should be legally placed on the net. Any political or religious issues should not be placed on the net (n)or any sensitive matters."
The remaining students believed that the company should be able to place some restrictions on their home page designs, referring to the need to eliminate pornography or other dubious information that employees might put on their home pages.

5.4.3.2 Internet privacy

What concerns do you have about Internet privacy?

- *Are you concerned that your personal data may be collected by other sites?* (Yes / No)

Most students responded Yes, remarking on unintentionally providing details to other Web sites via cookies, then being placed on various mailing lists. Some students responded No, for example:
"Let's face the facts! Who doesn't have the information already?"

(ii) Are you concerned that you don't know what the data collected would be used for? (Yes / No)

Most students responded Yes, commenting on the need to know what information was being collected about them, and the purpose of such data collection. One student noted:
"More so, that I do know some of the things they use it for!"

(iii) Would you send credit card details across the Internet to a vendor site? (Yes / No)

The students responded with a *unanimous* No, making comments showing awareness of the relevant risks, for example:

"It is not guaranteed that the data is safe as it is not being encrypted and may be hacked by someone on the net."
This reflects the timing of this case, October, 1996, when such data were rarely being encrypted. By 1999, the situation had changed, with encryption of payment details being commonplace. However there has been a spate of serious hacking over the last year affecting public confidence in transmitting credit card details online.

(iv) Do you believe in your right to access sites anonymously? (Yes / No)

Most students responded Yes, with some worrying comments, for example:
"I don't want people to know when I hack a site."
"As you can tell them what is right/wrong without their getting angry."
Others responded "No", for example:
"We'd be logged by our network administrator anyway!"

(v) Any other privacy concerns?

All students ran out of privacy ideas at this point.

5.4.3.3 Censorship

(i) Would you approve of your company filtering out Internet content via a firewall? (Yes / No)

About three-quarters of students responded No, often quite angrily, for example:
"I would sue them", while others gave reasons such as:
"No, because after working hours I can use the Internet for other purposes. If the company filters content, I can't have freedom at this time."
The remainder thought filtering of content was acceptable, for example:
"As the company is paying for the access they should have the right to identify information which they do not believe is acceptable, and refuse employee access to those sites."

Censorship is obviously a contentious issue.

5.4.3.4 Monitoring

(i) How do you feel about your company monitoring your Internet activities via a firewall logging your activities?

The vast majority of students responded negatively, believing that logging and monitoring represented a lack of trust between employer and employee, as well as an invasion of employee privacy.

Comments received included:
"I would hate it, there would be no privacy".
"They should back off before I sue them!"
plus a liberal sprinkling of abusive words.
The many angry responses received clearly indicated a lack of awareness of the importance of monitoring in achieving employee accountability in Internet usage.

The remainder, however, thought monitoring was acceptable. For example:
"I have nothing to hide."
"If an employee is only visiting legitimate sites they should have nothing to worry about."
"Employee can always have their own (unmonitored) Internet access personally at home."

5.4.3.5 Compliance and sanctions

(i) If your company had an Internet security policy, how could they make it work?

A heartening response was received here, with the most popular student suggestions being (in no particular order):

- gaining employee cooperation;
- explaining benefits to employees;
- setting and enforcing penalties (by far the most popular suggestion);
- monitoring usage via a person (not a log!);
- policy awareness sessions;
- displaying policy when starting up browser;
- employee-employer involvement in creation of policy;
- get employees to sign consent forms;
- give each employee their own copy of the policy.

(ii) *Which one of the following would be the most appropriate sanction if an employee in your company was found guilty of excessive personal surfing of the Internet during work hours?*

None (Yes)
A warning (Yes)
Suspend Internet connection for one week (Yes)
A fine (Yes)
Dismissal (Yes)

Other (please specify)

Students approved of warnings, suspensions, fines and dismissal, with by far the most popular suggestion being:
"Give one or two warnings first, if that doesn't work, suspend connection for a period, if that doesn't work, then consider dismissal." However, quite a few students advised to suspend connection immediately, then dismiss the employee if necessary.

5.4.3.6 Netiquette

(i) Would you like company guidelines for correct etiquette in Internet usage?
(Yes / No)

Most students responded Yes, for example:
"It is good to follow etiquette so that I won't do something that the company doesn't like."

In fact, most students who responded yes were eager to have guidelines due to fear of "saying something inappropriate" over the Internet and getting into trouble, showing the importance of providing Netiquette guidelines for young employees.

Quite a few responded No, for example:
"A waste of time and effort. Correct etiquette in Internet usage is common sense. It all boils down to the individual choosing the right or wrong thing to do."
Others claimed that it would make employees feel uncomfortable being so constrained, for example:
"Employees should be allowed the freedom and if any guidelines are to be imposed then this would make employees feel uncomfortable."
"I don't like any restriction when I access the Internet."

5.4.3.7 Responsibilities, duties and accountability

(i) Would you expect to have your Internet responsibilities made clear in a policy of some kind? (Yes / No)

All students responded Yes, mostly without adding comments. One student said:
"Absolutely mandatory!"

This is a clear indication of the need for policy.

(ii) Would you like to have an Internet security awareness session to clarify all Internet usage policies? (Yes / No)

All students responded Yes, making comments such as:
"So that I can ask questions".

This is a clear indication of the need for policy awareness.

5.5 Case B: Results

The case analysis in the previous section clearly indicates the problems involved in deciding Internet security policy in view of the sensitive human issues for company employees.

Via this case study, I gathered data which indicate support for the human issues model (Table 3.4), an important and highly sensitive component of the overall framework, as will be shown in the remainder of this section.

One section follows for each of the seven proposed types of human issues: freedom of Internet use, privacy, censorship, right to be kept informed, accountability, ownership and ethics.

5.5.1 Freedom of Internet use

It seems clear that most students were aware of their obligations to future employers to carry out work (rather than play) during business hours, and the majority recognised this obligation by suggesting non-business Internet use at lunchtime or after work, limited to about two hours per day overall.

The exception was use of personal email, which the majority felt should be available, within reason, all day. Another interesting result was that students admitted that if a company made an Internet service available, they would take advantage of it, *even if they considered it unethical*—for example, personal email, and the downloading of games and non-business images during work hours. Of the latter, one student stated, "I would do so given the opportunity, however I do not believe that people have a right to do so." I imagine this kind of attitude extends to personal surfing as well, although unfortunately I did not directly query this particular misuse. This problem indicates a need for policy awareness sessions, via which such ethical issues can be addressed. I feel that a slight push might be all that is required to convince some (not all) employees not to take this attitude.

Another interesting result was that some students pointed out that Internet surfing allows them to gain valuable work skills and knowledge. I was interested, therefore, to take this issue up with the employer representatives whom I interviewed in the detailed case studies (as I will discuss in later Chapters).

5.5.2 Privacy

Students were highly concerned about privacy matters, indicating a distinct distrust in Web site access privacy and Internet credit card payment privacy, and exhibiting cynicism over so-called anonymous accesses.

5.5.3 Censorship

This was another contentious issue, with many students outraged at the prospect of not being allowed access to selected company-determined, objectionable sites, suggesting that it may prove hard to convince employees on this issue.

5.5.4 Right to be kept informed

Students clearly indicated their perceived right to a policy as well as associated awareness activities.

5.5.5 Accountability

Students clearly saw the need for a policy to inform them of their responsibilities and duties, as well as acceptable and unacceptable Internet usages, and approved of sanctions to achieve policy compliance—thereby indicating a degree of belief in their accountability for their actions. *However, many did not approve of the monitoring steps required to achieve this accountability.* Perhaps the need for monitoring could be addressed in education sessions and awareness sessions.

5.5.6 Ownership

In the question about employee home pages, the majority of students believed the company owned the Web pages concerned, and should therefore protect itself by approving or vetoing the content. However, there were some students who would need convincing.

5.5.7 Ethics

Students illustrated ethical dilemmas in policy issues when they made remarks about using Internet facilities if they were made available, even if they did not believe in their right to those facilities.

5.6 Case B: Summary

In the previous sections, I analysed case data collected from the Monash University case, and presented the results of the case study which clearly indicated support for *all* aspects of *the human issues component model* (Table 3.4) of the Factors in Internet security policy model (Figure 3-3).

These results have some significant limitations. Firstly, it should be noted that the students were expected to respond as if they were already employed, thereby trying to gauge the employee perspective of these issues. Were they indeed in employment, they may find things somewhat different to their student expectations, and begin to see things in a different way. Hence, I have really only assessed *student expectations* for the human issues for employees in Internet security policy. Secondly, the only perspective studied in this case was that of the students—*the (would-be) employees*, that is. The other major perspective to be taken into account in Internet security policy is that of the *employer*. In the detailed case studies described in Part III, I study the *employer* perspective of human issues (as well as all the other issues) in Internet security policy.

5.7 Conclusion

In this Chapter I described, analysed and presented results from two mini case studies, providing indicative support for significant aspects of the following key components of the overall framework for Internet security policy (Figure 4-2):

- Factors in Internet security policy (Figure 3-3) (Case A)
- Internet risks which influence Internet security policy (Figure 3-5) (Case A)
- Organisational issues in Internet security policy (Table 3.2) (Case A)
- Human issues in Internet security policy (Table 3.4) (Case B)
- Internet security policy content (Table 4.1) (Case A)
- Internet acceptable use policy (IAUP) content (Table 4.3) (Case A)

In both mini cases, I explored the employee perspective of Internet security policy by viewing the students as "almost employees".

In Case A, I found that the students were able to see certain Internet risks as being very significant (for example, non-business usage and pirated media), and that they themselves were being negatively affected by some risks. For example, excessive non-business use by some students was leading to denial-of-service for others wishing to use the facilities for university-related purposes. On the other hand, students did not care about their own piracy of Internet software. With both these risks (as with the others discussed in Case A), a policy may help in risk management.

It was also apparent that the risk significance of risks occurring in an educational sector (such as the university) differs from those occurring in other kinds of environments. For example, personal surfing (rated separately within non-business usage) was rated at typically 8, 9 or 10, indicating a frequency of occurrence within the university of between once a minute and once an hour. Comments referred to students having much "spare time", indicating that if they didn't have so much "spare time", they may not be able to surf the Internet as much. I was then able to plan, in the three detailed cases to follow, to enquire about the correspondence between employee "spare time" and non-business use of the Internet. Similarly, fraud was rated a low risk, again commensurate with a noncommercial organisation.

I was able to conclude that it is very important for a risk assessment (as in my development model - Figure 4-1) to be carried out in each individual environment, as the significant risks are highly specific to that environment.

There were many suggestions made by students in *both Cases A and B* as to how a policy would be able to control individual risks. Hence, students did show a belief in the power of a policy for Internet risk management. I decided to follow these suggestions up with organisations in later case studies. Students mentioned, amongst other suggestions:

- gaining employee cooperation, for example by explaining the benefits of following policy;
- monitoring, including spot checking (sporadic human surveillance) of employee use;
- setting and enforcing sanctions;
- warnings of legal liabilities where relevant;
- company raids for pirated software;
- Internet awareness activities;
- placing technically-enforced limits of various kinds on employee Internet use;
- advising employees of the existence of low quality data on the Web, and educating employees to tell the difference, in particular, to differentiate between personal opinion and fact ; and
- signed employee consent forms.

I resolved to query companies in the detailed case studies about the viability of these ideas.

Students also made suggestions, which I resolved to follow up with other organisations in the three detailed cases, about why a policy might not work, specifically:

- employees may misuse facilities regardless of policy, either due to the inherent appeal of the Internet, or due to the unethical nature of some employees;
- employees may not read policies;
- detection of employee misuse may be difficult (for example, distinguishing frivolous use from valid usage);
- some employees will take risks, even if policy exists, as "the reward", if the employee is successful, may seem worth the risk (for example, pirated software).

Student comments in Case A, relating to organisational factors (see summary in Section 5.2.1.2), indicated the need for an Internet strategy aligning Internet use with organisational objectives, and the unsuitability of a permissive Internet security posture, in which everything is allowed except that which is explicitly forbidden. Their attitudes also reflected the negative impact of a lack of formal Internet infrastructure and Internet security management programme on the significant incidence of Internet misuse. It also appeared that lack of senior management commitment or support for Internet security could be contributing to the problems. Finally, students made comments highlighting the need for awareness activities. I followed all these organisational issues up in the detailed case studies, to see if they held true within different industry sectors.

Student comments in Case A, regarding administrative procedures, indicated that the existing procedures may not be feasible. I resolved to follow this up in the detailed case studies.

Student comments in Case A, regarding legal factors, indicated their lack of knowledge of relevant laws. I resolved to see if this was true in the detailed case studies, and to see if policy could be used to inform employees of their legal obligations as well as illegal Internet uses.

In both Cases A and B, there were comments made indicating the need for company netiquette standards for multicultural exchanges in a global society. I resolved to check for this need in the detailed case studies.

With respect to human issues, many were raised by Case A (see Section 5.2.1.7), although they were specifically addressed and analysed by Case B. The responses I obtained from students led me to believe that dealing with the human issues for company employees, in trying to set policy, would be a very complex task. It was also clear that people may not have a clear idea of what is ethical in Internet use, and what is not, and do not have a clear idea as to what is a right and what is a privilege, in Internet use. I resolved to spend significant time addressing these issues with the three companies I chose for the detailed case studies.

Both mini cases in this Chapter explored and described *the employee perspective* of Internet security policy. In Part III which follows, I explore, via four major case studies, *the employer perspective* of Internet security policy, using the results of the two mini cases to guide many of my investigations. As these four upcoming cases are more detailed than the two mini cases, I am also able to explore a greater portion of the overall framework (Figure 4-2).

Part III

In-Depth Analysis

Chapter 6
Case Study: Medical Science Research Institute

In Chapters 3 and 4, I built a framework for Internet security policy for organisations entirely from scholarship (Figure 4-2). In Chapter 5, I explored two mini case studies which contributed very early research results for the project, and provided indicative support for various aspects of the framework—as viewed from the employee perspective. In this part, I describe the third sub-project of this research project, *In-Depth Analysis*. This sub-project consists of the conduct of four detailed case studies exploring the topic area, searching for support and improvements for the proposed framework.

The first three case studies were undertaken relatively early in the research project, which eventually extended over a longer period than originally expected (four years: 1996 – 2000). Hence, I chose to conduct an additional, fourth case study toward the end of the project, in order to check whether the early case studies were still relevant.

All case studies are explored from the employer perspective, in order to provide "the other side of the story".

In this Chapter, I present the first detailed case study, conducted at Medical Science Research Institute, a large, Australian medical research organisation. The study was performed very early in the research project, in November, 1996.

As this was the first of the four detailed case studies, and I was still in a very exploratory stage of the research project, I focused on exploring only part of the framework in Figure 4-2: the model for Factors in Internet security policy (Figure 3-3), and its component models. I did not study much of the Content component nor the Development component of the framework.

Further, as the case was a relatively early exploration of the area, I did not collect as much data in it as I did in the two subsequent case studies.

The extent and value of this study are therefore far more limited than those of the following three studies.

I commence by introducing the Medical Science Research Institute, outlining case procedures, and drawing a background picture of the Internet infrastructure and usage at the institute. I then present the case study analysis and results, and draw conclusions.

Selected aspects of this case were reported in Lichtenstein and Swatman (1997a).

6.1 Introduction to Medical Science Research Institute and the case study procedures

A limited introduction is given to this organisation, for reasons of confidentiality. Medical Science Research Institute (henceforth referred to as MSRI), located in a major city in Australia, had several hundred employees at the time of study—mostly biomedical researchers. MSRI employs biomedical researchers from many nations, possesses state of the art equipment, and maintains strong connections with the international research community. It became apparent in the early nineties that the Internet would prove a valuable workplace tool, and hence, an Internet connection was established.

6.1.1 Sampling procedure

MSRI was planning to develop an Internet security policy at the time of the study (November, 1996), due to the continued growth of the organisation and its Internet connection to several hundred Internet users by mid-1996, and due to a growing awareness of the various Internet risks of both employee misuse and abuse, and external misuse and abuse. For this reason it was at least a candidate organisation to consider for a case study. Furthermore, although it was still in the early stages of Internet usage, MSRI represented a very different industry segment to the other three major case studies (which follow). MSRI was a research establishment peopled by skilled researchers, whereas the other three organisations studied were from the travel, retail and energy sectors. For these reasons, I selected MSRI as a suitable organisation for a case study.

6.1.2 Data collection and case instrument

I collected data for this case study via two, two-hour semi-structured interviews with MSRI's network manager, whose duties include responsibility for Internet management, employing:

- a collated document consisting of the various models composing the framework in Figure 4-2, as well as summarised responses from the mini case, Case B, student expectations when eventually employed, in Internet acceptable usage; and
- a set of guideline questions which repeatedly referred to the collated document (see below), to structure and guide the interviews.

There were no documents available concerning any type of Internet security policy, as MSRI did not have one.

The questions asked of the interviewee (MSRI's network manager), in order to structure the interview, were:

- to provide background information about his company, Internet usage, Internet architecture and Internet access controls;
- to perform a qualitative risk analysis of MSRI'S Internet risks, using the Internet risks model (Figure 3-5) as a guide, in order to determine the significance of each identified Internet risk, and to gauge support for the model; and
- to comment on the Factors for Internet security policy model (Figure 3-3) in the context of MSRI, and to gauge support for the model.

6.1.3 Case conduct

I recruited the company by telephone, and despatched an explanatory document describing the research project to the network manager for perusal, prior to his formally agreeing to the study. Interview times were arranged by email after initial agreement was obtained. The main contact signed a research consent form at the initial interview. The two interviews were approximately two hours in duration, taking place at the company's head office.

I distributed a copy of the collated document of proposed models to the network manager, and followed the set of questions listed earlier in order to obtain the data required. I took notes during the interviews in preference to recording them, as a personal preference (see my comments for earlier cases).

6.1.4 Data analysis

I later analysed the data collected by comparing and contrasting the collected data with the component models of the proposed framework, and identified similarities, differences and patterns. A draft copy of the resulting case study analysis was forwarded to the network manager for correction, and for the addition of missing information.

6.2 Internet infrastructure and usage

MSRI's IT activities were handled by its IT department, which was staffed by several technical personnel including the network manager whom I interviewed, and a departmental manager. Several hundred workstations were connected to the Internet via a LAN.

MSRI's Internet usage grew from single-user several years prior to the study to much larger numbers by mid-1996, sparking concerns regarding the lack of Internet security measures. At the time there were several hundred Internet users within the organisation, all employees, composed of senior biomedical scientists, postgraduate students, postdoctoral scientists, and support staff. MSRI possessed an Intranet for internal information sharing.

Internet users shared computers, each of which had its own Internet connection. The scientists mostly utilised the research mechanisms of the Internet for scientific research purposes and, to a lesser extent, used the Internet mechanisms available for communication and collaboration, information sharing and management, and access to applications. Electronic trading was not being carried out through the Internet, as the relevant suppliers did not have Web sites set up for trading (all purchases were fax-based). At the time of the study, there had not been any serious security incidents relating to Internet usage, although a number of small incidents were occurring, as will be described in Section 6.3.

6.3 Case analysis and results

In this section, I analyse the results collected by pattern-matching the data with aspects of the proposed framework (Figure 4-2) under investigation—in particular, the Factors in Internet security policy (Figure 3-3), and its component models: Internet risks, organisational issues, administrative issues, legal issues, societal issues, technical issues and human issues.

MSRI accepted the Factors model as a fair breakdown of the many holistic issues involved in managing Internet security.

The following sections discuss each type of factor, as it presented itself at MSRI.

6.3.1 Internet risks at MSRI

MSRI informally analysed their Internet risks, using the Internet risks model in Figure 3-5 as a guideline to assist in identifying existing risks, and assigning each identified risk type a rating of low, medium or high, based on the professional opinion of the network manager interviewed, including his opinion-based, qualitative estimates of *frequency of risk occurrence* and *impact*. The results are summarised in Table 6.1 in order of most significant to least significant risk, and the analysis of each risk type is discussed below.

Internet Risks	Risk Rating L, M, H
Non-business usage	H
Corrupted or erroneous software	H
Accidental erroneous business transactions	M
Hacking	M
Inaccurate advertising	M
Pirated media	M
Accidental disclosure	M
Inappropriate email	L
Low quality data	L
Fraud	L
Denial-of-service	L
Theft of information	L

Legend: L = Low; M = Medium; H = High.

Table 6.1 Internet risks at MSRI

6.3.1.1 Non-business usage

The extent of non-business usage of the Internet *during work hours* was unknown, although it was estimated that 80% of usage during non-work hours was for non-business purposes (personal surfing, downloading games and images, etc).

The organisation was understandably concerned that the level and type of non-business usage during work hours was unknown, because of the high figures for out-of-work-hours personal usage, and the belief that business-hours personal usage was excessive (for example, one employee was fired for excessive net surfing.)

Web sites visited from a given machine could be checked via a proxy server on which both the machine ID and the site were logged.

Since some machines were shared, however, it would be difficult to track exactly who visited a particular site.

MSRI rated the risk of non-business usage as *high*.

6.3.1.2 Corrupted or erroneous software

The computers were all virus-protected by anti-virus software. One virus had been brought in recently from a home computer, and this was regarded as the main source of viruses. The risk remained, however, of employees downloading virus-infested or buggy software from the Internet. As the impact of such a virus could be high, and as MSRI was aware of the growing virus problem, they rated this risk as *high*.

6.3.1.3 Accidental erroneous business transactions

With respect to misdirected email, MSRI had experienced plenty of such instances, with several causing embarrassment. With respect to electronic trading and the possibility of corrupted transactions: At some future time when supplier companies to MSRI will be setting up facilities for electronic trading via Web sites, the risk of corrupted transactions will increase in significance. As misdirected email was already a problem, MSRI rated this risk as *medium.*

6.3.1.4 Hacking

An activity report listing accessed Web sites was scanned manually each day by the network manager, who was able to spot well-known, troublesome newsgroup addresses. On one occasion, a hacker site had been accessed several times. The network manager queried the motives for the access with the employee concerned, and no further irresponsible activity took place. In a separate incident, MSRI was unsuccessfully attacked by a hacker. Nevertheless, due to the possible severity and loss of data incurred by any successful hacking attempt, either in or out, MSRI rated this risk as *medium*.

6.3.1.5 Inaccurate advertising

Email and other postings may have been misrepresenting official MSRI positions and views, as disclaimers were not mandatory. Planned employee home pages in the future would, however, require disclaimers. Research information posted by employees at MSRI via Internet mechanisms lacked credibility with global readers, who had a tradition of only trusting material found in reputable academic journals (although this could change). Hence, MSRI rated this risk as *medium*.

6.3.1.6 Pirated media

Internet piracy via downloading may have been occurring, but MSRI actively deterred this by removal of illegal software on detection, accompanied by a warning. Nevertheless, due to legal liability concerns, MSRI rated this risk as *medium*.

6.3.1.7 Accidental disclosure

MSRI's scientific research data and results were regarded as sensitive information.

MSRI did not stipulate that confidential information should not be disclosed outside the company. However, most information communicated via the Internet by MSRI researchers was public knowledge anyway, as it had already been published. Unpublished research information was regarded as 'secret', and retained that sensitivity level until after publication (which typically took about six months).

It would be undesirable for this 'secret' information to be disclosed over the Internet via email, Web sites, or other posting mechanisms, during the pre-publication period.

However, only a few research projects at any time were in this 'secret' state. Access privileges for relevant MSRI accounts were set and monitored, in accordance with the research information sensitivity levels and the employees' 'need to know'.

As there was some chance that scientists might indeed leak such 'secret' project information, this risk was rated as *medium*.

6.3.1.8 Inappropriate email

One MSRI employee who was a member of a mailing list, decided to correct an innacurate email sent out by another member of that mailing list. The person whose email had been corrected reacted angrily, deliberately flooding the MSRI employee with email. Although the ISP of the abusive person rebuked him for having carried out the mail-bombing attack, the MSRI employee suffered obvious harassment and denial-of-service, as a result of the attack In addition, unsolicited email was becoming a problem at MSRI. Overall, however, as employees were appearing to cope with the various problems in this category, MSRI rated this risk as *low*.

6.3.1.9 Low quality data

It was not likely that MSRI's scientists would give genuine credence to scientific research data presented via global Web pages, as the scientists, being highly conservative and traditional, only believed in the validity of work which had been published in reputable, medical, printed journals.

Employees did not have their own Web pages at the time. With the development of the internal Intranet, however, it was considered more likely that employees would create their own pages, although interest at that stage had been low. In the future, Web pages may be made accessible to the global audience, at which time there would indeed be a risk of low quality pages. For the time being, MSRI rated this risk as *low*.

6.3.1.10 Fraud

There was no financial data stored on MSRI's systems, nor had employees (as far as was aware) attempted or committed fraud. Hence, MSRI rated this risk as *low*.

6.3.1.11 Denial-of-service

The local university network had experienced problems which had brought MSRI's network connection down on several occasions. However, the scientists had work to get on with while the connections were down, and had not been seriously impeded at those times. Bandwidth was 10MB per second, and this was adequate to ensure no Internet traffic delays at that stage. Hence, MSRI rated this risk as *low*.

6.3.1.12 Theft of information

Internet software piracy has already been mentioned as a concern. However, MSRI's scientists produce research publication and may be infringing copyright by plagiarising Web sites accidentally or knowingly, at times. There had not been any reported incidents, however, so MSRI still rated this risk as *low*.

6.3.1.13 Summary of Internet risks and their management.

It is clear that MSRI suffered from Internet misuse and abuse. In particular, the 80% estimate for non-business Internet usage outside work hours was disturbing, as was the suspected heavy non-business use during business hours. These and the other risks identified were prompting MSRI to develop an Internet security policy as a starting point for coping with the problem. However, they foresaw problems with such a policy, as will be discussed in the next section.

6.3.2 Other factors in Internet security policy at MSRI

MSRI was aware that there were other factors to consider in devising an effective Internet security policy.

6.3.2.1 Organisational issues

Table 3.2 suggested the following broad categories of organisational factors which influence Internet security policy.

(i) Organisational objectives

MSRI had not specified that usage should be in accordance with organisational objectives.

(ii) Internet security infrastructure and Internet security management programme
(Note: two organisational categories are discussed together here)

MSRI lacked a formal Internet security infrastructure. It did not possess an Internet security strategy, Internet security management programme, Internet security policy nor IAUP. The IT departmental manager was totally responsible and accountable for Internet management. There was no delegation of authority, although a certain amount of independent activity by other IT staff ensured that the necessary actions to resolve Internet-related problems were undertaken (with the manager's approval).

(iii) Management commitment

Senior managers had not, as yet, taken an interest in this issue, although this was expected to change, given the high level of non-business usage.

(iv) Internet security awareness

MSRI's philosophy regarding policies in general was one of ‘employee beware’, in the belief that if existing policies were to be explained or highlighted in any way, employees would blame MSRI when accused of breaching policy, claiming that the relevant policy had either not been explained at all, or had been inadequately explained. This view can be restated as "If you tell users something, you must tell them everything", a goal which MSRI believes is unattainable. As already mentioned, MSRI's supporting philosophy had been “ignorance is no excuse". This was now being regarded as an untenable attitude.

(v) Policy integration

The local university through which Internet connection was obtained did not itself impose any IAUP on MSRI. However, the university was subject at the time to the IAUP of AARNet (1995), and therefore also to the policies of Telstra Internet Services. However, employees usually did not check these policies.

(vi) Principles

MSRI recognised that a policy should meet certain criteria for effectiveness, such as *enforceability*.

6.3.2.2 Administrative factors in Internet security policy at MSRI

MSRI recognised the need to formally define procedures for auditing, applying, monitoring and updating Internet security for compliance with the eventual policy.

6.3.2.3 Legal factors in Internet security policy at MSRI

MSRI employees were not informed of relevant laws and standards, and it was left up to the employees to familiarise themselves with these, MSRI being in accord with the old legal slogan, "ignorance is no excuse". MSRI was recognising that with a formal policy must come the responsibility of informing employees of the legal issues, such as intellectual copyright laws, in order to protect the employees, as well as themselves, from legal liability.

6.3.2.4 Societal factors in Internet security policy at MSRI

MSRI recognised the need for netiquette standards for interacting with international cultures, and external organisations.

6.3.2.5 Technical issues in Internet security policy at MSRI

Although no firewall existed at the time of the study, one was planned for the near future, in order to comply with auditing requirements. Various other technical Internet security measures were, however, provided (for example, antivirus software).

6.3.2.6 Human issues in Internet security policy at MSRI

I have not attempted to analyse the issues in the categories presented in Table 3.4, as I did not collect sufficient data for this purpose. Instead, I discuss three human issues presented by the data that I did collect: freedom of Internet use, right to be kept informed, and accountability.

(i) Freedom of Internet use

MSRI's culture was one of employee IT usage being controlled by the power of the IT department, and employees were therefore wary of misusing the Internet *during business hours*. This form of control was not considered ideal, however. Internet misuse was also managed by the employees' immediate managers keeping them occupied with work-related tasks—a more reliable and acceptable form of control at the time and in the longer term. Nonetheless, with the steady growth of the organisation (as well as increased numbers of connected Internet users), MSRI recognised that it needed an Internet security policy featuring an IAUP, to manage their Internet security problem.

MSRI expressed some concern regarding employee expectations of perceived "unlimited freedom" on the Internet—despite some current control via the combination of IT departmental power and sufficient work to keep them occupied. The employees were expected to resent and possibly resist any attempt to curtail their current, unconstrained usage.

Last but not least, the network manager with whom I spoke was himself uncertain about the degree of Internet usage freedom which should be granted to employees. The resolution of this issue would need considerable deliberation.

(ii) Right to be kept informed, and accountability

Any misuse was handled informally, with non-compliant employees being 'spoken to'. An important concern voiced was that employees might not consult an IAUP if one existed—except, perhaps, for a few experienced Internet users—although such a policy could prove useful as a weapon following misuse. Further, MSRI recognised a certain lack of fairness to its employees in its attitude of "employee beware". Hence, policy awareness sessions would need to be mounted.

6.3.3 Summary of factors influencing Internet security policy at MSRI

Clearly there were many factors which would influence MSRI in the development of an Internet security policy. Organisational, administrative, legal, societal and human issues had not yet been dealt with adequately, and these issues would first need to be addressed in order for an effective policy to subsequently be developed.

6.4 Conclusion

I commence this section by summarising the research models supported by the case study results, then draw conclusions for this research project.

6.4.1 Summary of models supported by case study

I obtained support via this case study, as described in detail in Section 6.3, for the following aspects of the overall framework for Internet security policy:

- factors in Internet security policy (Figure 3-3)
- societal issues in Internet security policy (Section 3.4.2)
- Internet risks for Internet security policy (Figure 3-5)
- organisational issues in Internet security policy (Table 3.2)
- administrative issues in Internet security policy (Section 3.4.5)
- legal issues in Internet security policy (Section 3.4.6)
- technical issues in Internet security policy (Section 3.4.7)
- human issues in Internet security policy (Table 3.4)

No aspects of my proposed models were contradicted by the study.

6.4.2 Case study conclusions

In this section, I discuss what this case study means in terms of the original research questions stated in Chapter 1.

1. What are the factors influencing effective Internet security policy for an organisation?

The investigation highlighted the influence of a number of key factors to be addressed by a policy. Two key Internet risks were identified—non-business usage of the Internet, and the downloading of viruses via the Internet. Other Internet risks of significance were also identified. MSRI agreed that all these risks needed addressing in a future policy. It was clear that organisational issues, such as the need to establish a formal Internet security infrastructure, would need to be addressed and referenced in the policy. Administative, legal, societal and technical factors which would influence the policy, were also identified. It was also clear that human issues would play a pivotal role in the final policy, due to the specific research culture of the organisation, in which employees expected unlimited research opportunities on the Internet.

The Factors model that I proposed in Figure 3-3 included all the types of factors that I identified at MSRI: Internet risks, organisational, administrative, legal, societal, technical and human issues.

Hence, this case study has helped answer this research question by identifying factors which influence the Internet security policy at MSRI, and by pattern-matching those factors with those proposed in my Factors model (Figure 3-3).

2. Is an holistic approach to an Internet security policy more effective than the piecemeal approach adopted to date?

The investigation of MSRI indicated that only by considering and drawing together the diverse factors identified, could an effective policy be developed. Hence this investigation has contributed to answering this research question in the affirmative.

3. Can a framework be specified for the development, issues and content in effective Internet security policy for organisations?

The diverse factors (issues) that I identified at MSRI as influencing an Internet security policy, correspond to the various types of factors specified in the Factors model (Figure 3-3) in the proposed overall framework (Figure 4-2). Hence, this study has provided indicative support for part of my proposed framework, and has contributed to answering this research question in the affirmative.

I have clearly shown the contribution of the study of MSRI to this research project. I acknowledge, as I stated in the beginning of this Chapter, that I only chose to investigate the factors component of the overall framework in this study, as it was the first of the detailed studies, and I was still exploring the topic area. In the next Chapter, I present the second of the four detailed case studies, a study of Flyway Australia, a large Australian travel organisation—in which I investigate *all* aspects of the proposed framework.

Chapter 7
Case Study: Flyway Australia

In earlier Chapters, I developed a framework for Internet security policy for organisations, then explored the topic further via two mini case studies which focussed on the employee perspective of the topic, and a detailed (albeit limited) case study which focussed on the employer perspective. In these three studies, I obtained useful results for the research project, as well as support for selected components of the proposed framework.

In this Chapter, I present the second detailed case study, conducted at Flyway Australia—a large, leading Australian transport and travel organisation—in October, 1997. This case also focuses on the employer perspective of the topic, but explores the complete framework proposed earlier (Figure 4-2), rather than focusing solely the Factors component (as was the case for the first case study of MSRI).

In Section 7.1, I introduce Flyway Australia and outline case procedures. In Section 7.2, I draw a background picture of Internet usage, architecture and access control in the company. In Section 7.3, I discuss the Internet security infrastructure which supports Internet usage and security, and comment on the current Internet security set-up. In Section 7.4, I present the case study analysis and results. I draw conclusions in Section 7.5.

Selected aspects of this case were reported in Lichtenstein and Swatman (1998).

7.1 Introduction to Flyway Australia and case study procedures

For reasons of anonymity, I present only a very limited introduction to Flyway Australia. Flyway Australia is a large Australian transport and travel company, with thousands of employees (at the time of study) spread across Australia. Flyway has permitted online reservations with online payment, for some time now.

7.1.1 Sampling procedure

I selected Flyway as it is a major example of the service provision sector in Australia, and as an organisation which, although still in the early stages of Internet usage was planning to expand to full electronic commerce capability, with Internet travel reservations (note: in 2000, online travel reservations are now operating).

7.1.2 Data collection, case instrument and case conduct

I collected data for this case study via three semi-structured interviews of approximately one and a half hours' duration each, employing:

- a collated document consisting of the various models composing the framework in Figure 4-2, as well as summarised responses from the mini case, Case B, showing student expectations (when eventually employed) in Internet acceptable usage; and
- a set of guideline questions which constantly referred to the collated document (see below), to structure and guide the interviews.

I collected two documents: Flyway's Internet acceptable use policy (IAUP) and a diagram of Flyway's Internet architecture.

I conducted the three interviews with two information security managers: the manager of the IT risk management section and the manager of the Information security group (in the first interview, a third person, the manager of Risk Identification and Controls, also participated). The information sought was ascertained and verified by discussion and clarification with the parties present.

The questions asked of the interview participants, in order to structure the interview, were:

- to provide background information about their company, Internet usage, Internet architecture and Internet access controls;
- to perform a qualitative risk analysis of their Internet risks, using the Internet risks model (Figure 3-5) as a guide, in order to determine the significance of each identified Internet risk, and to gauge support for the model;
- to comment on the Factors for Internet security policy model (Figure 3-3) in the context of Flyway, and to gauge support for the model;
- to provide information about their existing approach to developing Internet security policy;
- to comment on the Internet security policy development model (Figure 4-1); and
- to comment on the Internet security policy structure and content model (Table 4.1), the IAUP content model (Table 4.3) and the email policy content model (Table 4.4) as these models pertained to Flyway's situation.

I recruited the company by telephone, and despatched an explanatory document describing the research project to the main contact for perusal, prior to the contact formally agreeing to the study. Interview times were arranged by email after the initial agreement had been obtained. The main contact signed a research consent form at the initial interview. Each of the three interviews was approximately one and a half hours in duration, taking place at the company's head office. I distributed copies of the collated document of proposed models to those present, and followed the set of questions listed earlier to obtain the data required. I took notes during the interviews.

7.1.3 Data analysis

I later analysed the data collected by comparing and contrasting the collected data with the component models of the proposed framework, and identified similarities, differences and patterns. A draft copy of the resulting case study analysis was forwarded to Flyway for correction, and for the addition of missing information.

7.2 Internet usage, architecture and access control

7.2.1 Internet usage

The Internet had been deployed at Flyway since 1996, with several thousand employees using it for email. Many of these employees also used Web browsers (email ran via a client rather than though these browsers) from their PC workstations. Requests for browser installation were currently running at about 20 per week, and the company anticipated that 7000 Internet browsers would be installed by the year 2000.

Flyway had, up till then, regarded Internet usage as analogous to telephone usage, allowing its departments and individuals to determine how best to use it, in preference to setting guidelines. The Marketing department had, thus far, influenced how the Internet had been used. At the time of study Internet was used for information sharing and management, research, communication and collaboration, and purchasing negotiations—but not for any actual transactions (although by 2000, online travel reservations had been implemented.) Although internal usage for communication purposes was the main Internet usage at the time, the company already anticipated that full Internet commerce functionality would eventually be supported (as it now is).

7.2.2 Internet architecture

Figure 7-1 illustrates the Internet architecture at Flyway.

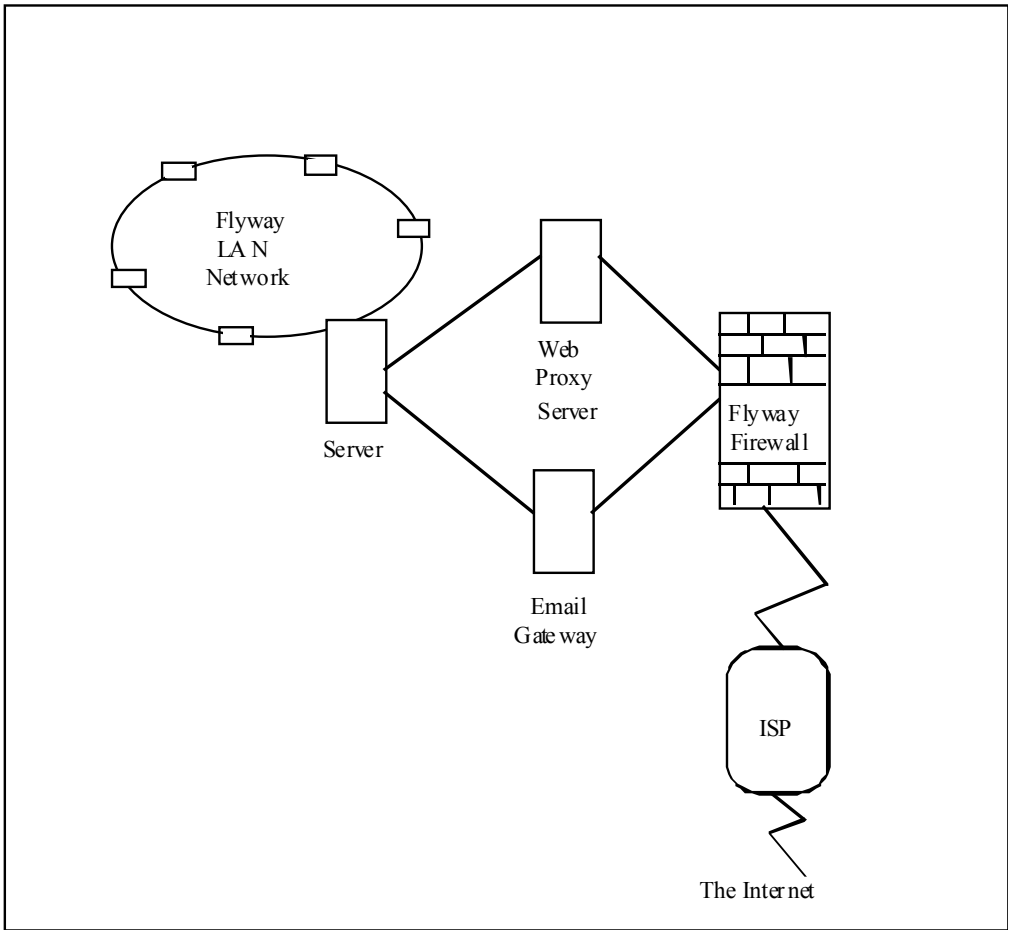

Figure 7-1 Internet architecture at Flyway

Employee workstations were mainly Pentiums and 486s connected internally at each geographic location via LANs. The LANs were connected to a proxy server, an email gateway and a firewall, which connected to an ISP. There were several mainframes (containing corporate systems) connected to the LANs, but the company considered it extremely unlikely that these mainframes could be accessed from outside the company (if the firewall did not prevent access, there were still many other technical hurdles to be overcome to gain access). However, there were also several Unix servers containing sensitive corporate applications and data, including an information warehouse under development, connected to a LAN—these could conceivably be accessed from outside the company via the Internet (in a worst case scenario).

7.2.3 Internet access control

7.2.3.1 Internet access policy

Internet access control was handled by an access policy implemented by a proxy server and a firewall. Together, these implemented Internet access control, logging, and storage of information required for monitoring usage. Employees with browser facilities connected to the proxy server, which consulted an access control list of user ids and passwords in order to grant Internet access by company employees via matching of user identifier plus password. (Employees were verbally encouraged to safeguard knowledge of the user id and password combination.) It was planned to change this access control policy to a far more liberal one of granting all employees with browser facilities Internet access. Email access would soon be permitted in a similar fashion, i.e. all employees possessing email facilities would be permitted Internet email access. Flyway believed that Internet access was first and foremost a resource issue—provided that there was sufficient bandwidth and infrastructure and processing capability, the requested Internet access would be permitted.

7.2.3.2 Proxy server control of Internet service access and Web site access

The proxy server permitted company-initiated ftp into the LAN, internal ftp to the outside world and access to chat groups and newsgroup services. However, the proxy server blocked access to a list of undesirable site urls supplied by ISAC and kept up-to-date by the company's firewall administrator. It was planned to filter access to newsgroups through another server which would effectively blacklist prespecified, undesirable newsgroups while allowing the others through.

7.2.3.3 Firewall filtering, logging and monitoring

The proxy server connected to a firewall which monitored and restricted incoming traffic, logged all accesses and emails, and denied telnet in and out. The manager of the Information security group monitored the firewall log on a sporadic basis (about once a week), on the lookout for suspicious attempts at hacking into or out of Flyway, and inappropriate email content and site accesses. At the time, there were inadequate resources and a lack of relevant policy for monitoring the firewall logs more frequently than this—printed reports were sometimes produced to facilitate the checks, but online monitoring was the norm. The IT risk management section reviewed the firewall configuration and proxy server rules from time to time.

If suspicious activities were noticed on the firewall log, the manager of the Information security group evaluated the seriousness of the situation and acted accordingly. Employees were aware that their site accesses and emails were being logged, and that the log was being monitored. They were so informed through the IAUP (which they signed on Internet connection), and were also reminded by a LAN log-in

screen which stated that: Internet traffic is being logged and monitored, the Internet should be used for business purposes only, and company information is confidential and should not be communicated freely.

7.3 Internet security infrastructure

7.3.1 Internet security as a "vertical slice" of information security

Flyway lacked a formal Internet security infrastructure, although it planned to set one up in the future—when Internet transactions were implemented.

Flyway regarded Internet security as a vertical slice within information security. The Internet's use was being driven by the Marketing division's perceptions and decisions, rather than by a formal Intenet strategy. The undocumented Internet security posture was "permissive"—everything was allowed except what was explicitly forbidden. Figure 7-2 illustrates the information security infrastructure at Flyway, with Internet security being handled by all the divisions, departments, sections and groups shown.

The IT risk management section was the main body in charge of all information security issues including Internet security, and was composed of an Information security group, a Risk identification and controls group and a Contingency planning group—about ten people altogether. The section talked to individual business departments about their information security needs—these departments assessed their needs (including Internet security needs) and informed the IT risk management section accordingly. The IT risk management section then supplied the perceived demand. The IT risk management section was contained within an Information systems services department which was part of an IT division (containing many departments).

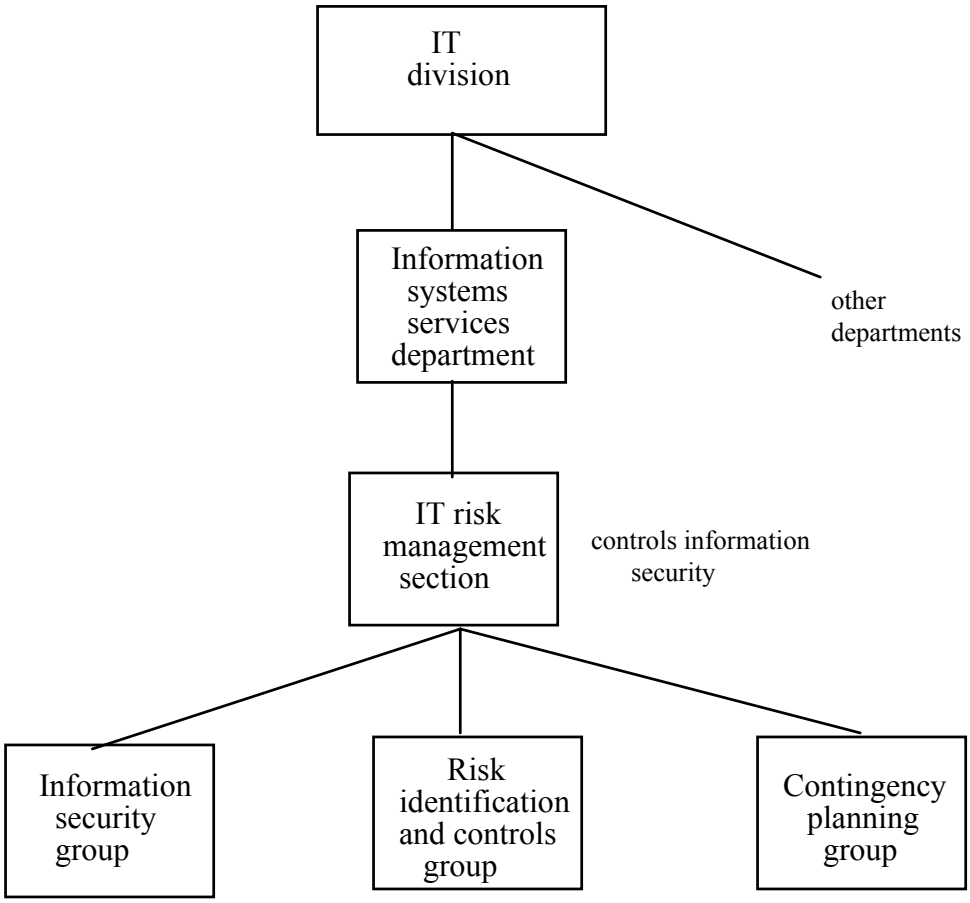

Figure 7-2 Information security infrastructure at Flyway

7.3.2 Roles and responsibilities in Internet security management

Internet security responsibilities were divided. *The manager of the Information security group was directly responsible for Internet security issues at a day to day level, while the manager of the IT risk management section bore ultimate responsibility.* As stated earlier, the Marketing division decided how best to use the Internet. Some Internet security issues were handled by other parts of the IT division, including setting email policy as well as setting the "look and feel" for company HTML Web publications. *The IT risk management section was reactive rather than proactive to Internet usage problems, a situation which it now believed needed to be addressed.* Other parties within the company were also involved in Internet issues. There was a Quality assurance and content group which monitored the quality and content of materials published on the Internet. The Marketing division had developed the company's Web site, but that site had recently received an unsatisfactory review from the IT risk management section, which now insisted on auditing future company Web sites. (As will be mentioned later, in 1998 Flyway had begun reviewing its Web site, and as at the year 2000, there is now a high quality site up.) A company Security Group liaised with the IT risk management section on issues of common interest, such as computer fraud.

7.3.3 Internet policies and related policies

Several policy documents informed employees of their information security responsibilities and restrictions—a company security policy, conditions of employment, an Internet acceptable use policy (IAUP), a company Code of Conduct and a set of HTML standards. There was also a firewall policy (in network protocol language) and an Internet access policy implemented as a list consulted by the proxy server (see Section 2.3.1).

The company security policy was in the Human resources department's manual. When an employee joined the company, their conditions of employment incorporated a policy relating to information security.

An IAUP form was issued by the IT risk management section to each employee on browser connection—the employee signed their consent to these conditions and returned the form (although this requirement was being disabled at the time). The IAUP was structured by Internet service, with six sections: email policy, World Wide Web policy, FTP policy, Telnet policy, Other services policy, and Inappropriate use policy. *There was no Internet security policy—only the IAUP.* A company Code of Conduct governed ethical standards.

A set of HTML standards existed to control Web page publication. These were developed by a Rules and Regulations group outside the IT division, although all publications were required to be passed to the corporate activities department for ratification prior to release.

All the abovementioned policies tended to be updated about every two years—although their contents became outdated far more rapidly than this period allowed. Flyway was concerned that the various policies that controlled Internet usage were developed independently by disparate groups and departments within Flyway, which could affect the ability to produce high quality, consistent, effective policies.

7.3.4 Plans for future Internet security infrastructure and policy

Flyway had an adhoc organisational Internet security infrastructure at the time but, as mentioned at the beginning of this section, saw the need for a formal Internet security infrastructure which it intended to develop as more resources became available, and when true electronic commerce was realised.

Flyway recognised the need for an Internet security policy as a key component of the anticipated new infrastructure.

7.4 Case analysis

In this section, I analyse the data collected, by pattern-matching the data with various aspects of the proposed framework (Figure 4-2). The specific aspects explored are:

- factors in Internet security policy (Figure 3-3)
- societal issues in Internet security policy (Section 3.4.2)
- Internet risks for Internet security policy (Figure 3-5)
- organisational issues in Internet security policy (Table 3.2)
- administrative issues in Internet security policy (Section 3.4.5)
- legal issues in Internet security policy (Section 3.4.6)
- technical issues in Internet security policy (Section 3.4.7)
- human issues in Internet security policy (Table 3.4)
- Internet security policy content (Table 4.1)
- IAUP content (Table 4.3)
- email policy content (Table 4.4)
- framework for development of Internet security policy (Figure 4-1)
- overall framework for Internet security policy (Figure 4-2)

I first analyse the various factors in Internet security policy at Flyway (Section 7.4.1), then analyse the support provided by this analysis for the factors model and its component models (Section 7.4.2). Next, I analyse Flyway's requirements for Internet security policy content, and the support provided for the corresponding content models (Section 7.4.3). I then analyse Flyway's requirements for the development of Internet security policy and the support provided for the corresponding framework for development (Section 7.4.4).

7.4.1 Analysis of factors in Internet security policy at Flyway

In this section, I investigate each type of factor in the model in Figure 3-3: *Internet risks, organisational issues, administrative issues, legal issues, societal issues, technical issues and human issues.*

7.4.1.1 Internet risks at Flyway

Flyway informally analysed their Internet risks, using the Internet risks model in Figure 3-5 as a guide to assist in identifying existing risks, and assigning each identified risk type a rating of low, medium or high, based on the professional opinion of the two information security managers interviewed, including their opinion-based, qualitative estimates of *frequency of risk occurrence* and *impact*. The results are summarised in Table 7.1 in order of most significant to least significant risk, and the analysis of each risk type is discussed below.

Internet Risks	Risk Rating L, M, H
Non-business usage	H
Hacking	H
Accidental erroneous business transactions	H
Corrupted or erroneous software	H
Low quality data	M
Inaccurate advertising	M
Inappropriate email	L
Pirated media	L
Accidental disclosure	L
Fraud	L
Denial-of-service	L
Theft of information	L

Legend: L = Low; M = Medium; H = High.

Table 7.1 Internet risks at Flyway

(i) Non-business usage

Flyway hoped that business unit managers acted as a control when assigning and monitoring employee workloads, thereby leaving little time for non-business Internet use.

However, despite this measure, and despite the fact that the IAUP prohibited non-business use and warned of sanctions for non-compliance, the company estimated that over 50% of its Internet usage was for personal purposes.

The average number of Web site hits per month per Flyway employee with browser connection was 800, so approximately 400 hits a month per employee (50% of 800) were probably personal surfing. One Flyway employee was logged at 25,000 Web site hits in one month.

Personal surfing and personal email (note: inappropriate email, which was rated 'low', includes junk email and harassing email, *not* personal email) were especially rife, leading to loss of productivity and other problems—such as the frustrating delay frequently experienced at the printers due to the printing of large volumes of downloaded personal Internet material.

Flyway was extremely concerned about Internet non-business usage, estimating the consequent productivity loss at some A$20,000 per week. Flyway rated the risk of 'non-business usage' as *high*.

(ii) Hacking

Although most of Flyway's corporate data were inaccessible via the firewall, some sensitive data could possibly be hacked into, including several financial applications as well as a data warehouse currently being developed. In the previous year, Flyway had observed four attempts on the firewall log at hacking into the company, although all of these had failed.

Flyway also noted that some employees had attempted to hack into other institutions, although no pattern had yet been detected—Flyway chose to assume that all one-off attempts were merely inquisitive. *Hacking was specifically prohibited in the IAUP.*

When planned online travel reservations eventuated (note: by 2000, Flyway processed online reservations), Flyway would view hacking as an even more significant concern. Overall, Flyway rated the risk of 'hacking' as *high*.

(iii) Accidental erroneous business transactions

There had been some cases at Flyway of confidential email being misdirected to groups of employees rather than being sent only to the intended recipient. *There was no warning in the IAUP regarding checking despatch addresses.* The impact of several past accidents had been considerable, and their likelihood remained quite high. Flyway accordingly rated the risk of 'accidental erroneous business transactions' as *high*.

(iv) Corrupted or erroneous software

At Flyway, there had been two instances of viruses associated with downloaded software in the preceding twelve months, resulting in minor damage. Flyway already scanned all inbound and outbound email (including attachments) for viruses, and planned to utilise the firewall to scan downloaded software. Desktop virus scanners were also available for employees. *The IAUP advised against transmitting viruses, and advised of existing virus-scanning procedures.* As Flyway was aware that the damage associated with viruses could be severe, it rated the risk of 'corrupted or erroneous software' as *high*.

(v) Low quality data

This refers to the risk of employees accessing invalid data via the Internet, in particular, invalid Web site content and invalid data in inbound email (for example, email scams, Web site scams, offensive Web site material and email impersonation).

This risk also includes the possibility of invalid data being disseminated from inside a company (for example, employees placing offensive material on company Web sites).

With respect to employees ascertaining the validity and acceptability of the data which they obtain via the Internet (in particular, external web site content and received email), the IAUP did not provide any advice cautioning employees against accepting at face value Internet data obtained, nor did it recommend verification of accessed material. There may well have been problems in this area, but it was difficult for Flyway to determine the extent to which such problems were actually occurring.

With respect to employees being the source of low quality data, Flyway employees did not possess home pages. Flyway did, however, include advice in its IAUP to prevent dissemination of low quality data via Web sites by employees, as follows:

The IAUP stipulated that employees must gain approval in writing for... Web pages relating to Flyway, prior to their publication on the Internet.

Note: the IAUP also warned employees against 'inappropriate email use', a term which Flyway used to cover not only the risks of junk email and email harassment in (vii) below, but also the risk of *invalid data* occurring in email—a risk which I have included in the 'low quality data' risk. Overall, Flyway rated the risk of 'low quality data' as *medium*.

(vi) Inaccurate advertising

This refers to the company or its employees consciously 'advertising' within email, Web sites, or other posting mechanisms, without due authority, *in such a way as to appear to represent an official view.* The content of this information may be inaccurate, in an organisational context.

The IAUP warned that the email must not be used to state official company position or otherwise commit the company. As mentioned in (v) above, the IAUP also advised official approval by Flyway of any Web sites or postings prior to publication.

At Flyway, there was a quality assurance and content group which monitored selected material to be officially published on the Internet—they had noted few problems with inaccurate advertising to date.

Flyway's Marketing division had developed the company's Web site, but as the IT risk management group was unhappy with the result, believing it to lack 'high professional standards', it planned to review future Web site developments.

The IAUP specifically prohibited the use of email for stating Flyway's official position, and email use was monitored sporadically for compliance. To date, there had been several minor occurrences of 'inaccurate advertising', but with one eye on the future expansion of Internet usage, Flyway rated this risk as *medium*.

(vii) Inappropriate email

This risk refers to companies sending or receiving unwanted or unsolicited email (*junk email*), harassing, discriminatory or defamatory email (*flame email*) or excessive unwanted email (*spamming*).

The IAUP advised that employee email must conform to high professional standards. The IAUP also warned of inappropriate email use, specifically prohibiting "sexual or racial harassment, and defamatory statements", advised of email monitoring, and stipulated that inappropriate email use may result in disciplinary action.

However, the IAUP did not warn of excessive or junk email, and Flyway had indeed experienced problems in this area. Email traffic ran at about 10,000 messages in and out per week (September, 1997), and the junk email within these has had, at the very least, interruptive impact.

Flyway had verbally (in training) informed their employees not to respond to incoming junk email, and to direct such email where necessary to the IT risk management section. For example, the email hoax virus announcements which were received from time to time were meant to be forwarded to IT risk management.

The following instances illustrate the problems occurring as a result of 'inappropriate email' risks. In one case, 800 emails were received by an employee from a mailing list over one week, thereby placing a severe load on the gateway. Flyway asked the employee to unsubscribe from the list. In another incident, objectionable advertising email (for an adult club) was posted on the local bulletin board. It was subsequently complained about, and removed by Flyway authorities. In yet another incident, a contract employee caused an Internet traffic delay by attaching a large, pornographic file to email and despatching it to colleagues—his Internet access was subsequently disabled. A final example was the frequent and often unwelcome circulation of jokes amongst employees—which had also been grumbled about. Nevertheless, Flyway rated the risk of 'email overload' as *low*, as its impact was considered relatively insignificant, compared with that of other Internet risks.

(viii) Pirated media

Software piracy via the Internet may have been occurring at Flyway, but the extent to which it was occurring was unknown. *The IAUP specifically deterred piracy in its IAUP, thereby assigning responsibility for compliance with licensing conditions to employees.* Flyway was also considering using its firewall to actively prevent downloading software illegally. Due to the unknown incidence of piracy, Flyway rated the risk of 'pirated media' as *low*.

(ix) Accidental disclosure

Flyway's IAUP specifically warned employees not to include confidential company information in their email, and recommended the immediate deletion of email once it had been read. At that stage, Flyway considered the risk unlikely, and the sensitivity of data likely to be communicated as low, and hence rated this risk as *low*.

(x) Fraud

At Flyway, when planned online travel reservations were realised, Internet fraud would be viewed as a serious concern. However at that stage, Flyway rated the risk of 'fraud' as *low*.

(xi) Denial-of-service

Flyway had not experienced many denial-of-service problems to date, although its attitude thus far had been to rely on the Internet only when there was a recovery procedure to follow should problems arise. However some incidents had occurred, such as the overloading of the gateway due to excessive email from a mailing list, as mentioned earlier. Flyway rated the risk of 'denial-of-service' as *low*.

(xii) Theft of information

Flyway reported only the piracy problem. It was unaware of employees plagiarising from Web sites or stealing data, and had not been a victim of such activities due to the inaccessibility of its corporate data. *The IAUP warned employees not to transmit material via the Internet in breach of copyright, and also to comply with licensing conditions when downloading software.*

(xiii) Summary of Internet risks and their management

It was clear that Flyway did have significant Internet risks. Flyway ranked: *non-business usage, hacking, accidental erroneous business transactions and corrupted or erroneous software* as their major Internet risks. At the time, although the company provided policies for many of these risks in the IAUP, this

policy was structured according to Internet services. *There were no individual risk policies.* Flyway agreed that it would be useful to have a specific policy within the IAUP for each of the risk types in the Internet risks model (Figure 3-5), informing employees of the specific risks for that risk type, and company policy for that risk type, including possible losses, remedies and sanctions.

Flyway could do far more to manage Internet risks via an *Internet security policy*, which would not only include the IAUP as a sub-policy, but would also specify requirements for other Internet security measures (for example, new technologies such as email content filter software, for the firewall, to check for harassing inbound and outbound email by "objectionable word" pattern-matching).

The risk analysis results presented above have provided support for the Internet risks model for Internet security policy (Figure 3-5).

7.4.1.2 Organisational issues in Internet security policy

Table 3.2 suggested the following broad categories of organisational factors which influence Internet security policy: organisational objectives, Internet security infrastructure, management commitment, Internet security management programme, Internet security awareness, policy integration, and principles for Internet security and policy. I discuss each of these below.

(i) Organisational objectives:

Flyway employees were given ample advice in the IAUP regarding the requirement for business usage only, with some detail supplied about what constituted valid business usage. For example, Web browsing was to be used "for research or other activity related to the job function of the user". In any new formal Internet infrastructure, the infrastructure development group would devise an Internet strategy based on business advantages of the Internet for Flyway. This strategy would stipulate a list of Internet usages which correlate with organisational objectives. These Internet usages would be listed as acceptable within the Internet security policy.

(ii) Internet security infrastructure:

In Section 7.3 of this Chapter, I discussed the absence of a formal Internet security infrastructure at Flyway, as well as plans for such an infrastructure when more resources became available, and when electronic transactions were implemented. The new infrastructure should be documented in the developed Internet security policy.

(iii) Management commitment:

Senior managers were not involved in Internet security awareness activities due to lack of time and lack of their own awareness of problems, although the IT risk management section was attempting to address this lack of involvement by talking to senior managers about the problems experienced. *The personnel whom I interviewed were uncertain as to whether this would reduce Internet usage problems.*

(iv) Internet security management programme:

The lack of a formal programme of policies, procedures, training and awareness activities, etc., was reflected in the Internet misuses occurring: over 50% non-business use and significant email overload, for example. The lack of a formal programme meant that some training sessions were voluntary. A formal programme would adopt a proactive stance, and produce a business case for additional resources. These resources would allow the programme to include mandatory employee Internet training, and would enable adequate human resources to be available for usage monitoring and other network administration tasks.

The components of the Internet security management programme should be documented in the Internet security policy.

(v) Internet security awareness:

Flyway had a number of Internet security awareness measures in place (although more could be added), including the IAUP, training, the risk management programme (see below) and log-in screen advice. I discuss each of these below.

As an awareness measure, the IAUP was quite extensive and informative, and included a user consent slip to 'ensure' employee awareness of its content. Although the IAUP stated that employees would be informed if the policy was amended, Flyway mentioned that employees were often unaware of the latest IAUP policies, as these had changed since the form was originally signed, and mentioned the need for a way of informing (and gaining consent) for changed policies. Flyway also accepted the need for employees to be aware of the purpose and scope of the policy (which could be stated within the policy itself), as part of awareness.

IT training included a one hour course in Internet use and a forty minute course in company information security, conducted by the IT risk management section (the Internet use course was mandatory for all Internet users). A new course on Internet security was being planned. All IT training was generally employee-requested rather than scheduled.

Flyway ran a special risk management programme in which employees were involved. This helped keep employees aware of Internet security issues.

As stated in Section 7.2.3, there was a LAN log-in screen which reminded employees that their Internet actions were being logged and monitored.

I noted that the IAUP did not inform employees of Internet security awareness activities. In any new Internet infrastructure including an Internet security policy, the policy should specify awareness requirements as part of the employee accountability sub-policy, while the IAUP should inform employees specifically of awareness activities.

(vi) Policy integration:

As mentioned in Section 3, there were several relevant company policy documents, as well as an ISP acceptable use policy, which were relevant for employee Internet acceptable use. None of these were referenced within the IAUP, and Flyway made minimal effort to integrate the various policies. This situation needed to be remedied in any new infrastructure, with all relevant policies being referenced within the new Internet security policy.

(vii) Principles for Internet security and Internet security policy:

Flyway recognised the need for enforceability and other principles for the new Internet security policy.

7.4.1.3 Administrative factors in Internet security policy

Some procedures were certainly applied at Flyway—for example, there was an external independent auditor who regularly audited their systems, including the Internet connection, reported weaknesses and advised "Best practice". There were informal procedures for applying, monitoring and updating the IAUP, but these were neither formalised nor documented (in the IAUP or elsewhere). All procedures were in the heads of IT risk management personnel. Procedures to be carried out by employees, for example, concerning virus checking, were given summarily in the IAUP. An Internet security policy is the place where Internet security procedures should be documented or referenced.

7.4.1.4 Legal factors in Internet security policy

Flyway was aware of the need to be kept informed of relevant legal issues in Internet security, and had held various activities, for example, seminar on legal issues in Internet usage. They also received relevant legal materials from the Contracts Officer in the IT Finance and Administration Department. The only specific legal references in the IAUP were:

- advice to comply with licensing conditions when downloading software; and
- advice not to transfer material in breach of copyright.

Flyway was aware of the need for far more legal references in an Internet security policy.

7.4.1.5 Societal factors in Internet security policy

Flyway referred to unethical practices, such as sending rude jokes into and out of the company. One employee posted an objectionable message on a Flyway bulletin board, drawing complaints. There was a need for ethical and netiquette standards (as part of a policy) to avoid such embarrassing incidents. With the advent of electronic transactions, Flyway expected online travel bookings to be made from overseas, with the differences between various global cultures producing an additional need for netiquette standards.

7.4.1.6 Technical factors in Internet security policy

Flyway had Internet risks which could be reduced by new technologies. For example, an email client with a standard disclaimer could be employed. Requirements for such technologies should be part of the Internet security policy.

7.4.1.7 Human issues in Internet security policy

Human issues included in the human issues model (Table 3.4) were: *freedom of Internet use, privacy, censorship, right to be kept informed, accountability, ownership and ethics*.

(i) Freedom of Internet use

There was an obvious problem with employees using the Internet for personal reasons over 50% of the time (see Section 7.4.1.1). Flyway referred to a lack of employee supervision as a major factor contributing to this misuse. There were many problems in deciding the appropriate degree of freedom for employees.

I asked the Flyway staff to comment on the students' expectations in employment, from mini case B, and their responses were almost derisive:

- Students expected about two hours' non-business usage per day: Not possible, as this would saturate the server while other employees were trying to work.
- Students mostly expected to use the Internet for personal reasons at lunchtime or after work, only: Not possible, as it would be far too hard to monitor at Flyway. There were insufficient supervisory resources to check whether people were officially on lunch break or not, for example.

- Some students expected free use of the Internet at work: This would be foolhardy, as illustrated by one Flyway employee who was logged making 25,000 Web site hits in one month.
- Most students expected personal email permissions at work: Flyway's undocumented, informal policy was that personal email use was analogous to telephone use—i.e. personal email within reasonable limits was acceptable. However, attaching a 5MB file, which led to delays at the email gateway, was not considered reasonable.

Overall, Flyway stood by its view, despite learning of the usage expectations of students verging on entering the workplace, from the results of mini case B: The policy *must* stipulate:

Use of the Internet is a privilege, not a right. There is to be NO personal usage of the Internet.

The employee's line manager would then have to take ultimate responsibility for policy enforcement, as follows: If the employee got their work done, and the line manager perceived limited personal Internet use in or out of hours, with NO abuse, then a blind eye would be turned to such limited personal use. If Internet delays became intolerable or all-too-frequent, however, this lenient attitude would have to change at Flyway.

(ii) Privacy

Flyway's comments on students' high levels of privacy expectations in employment, from mini case B, were:

- Flyway believed that only work-related data should be collected from employee Internet accesses at external Web sites, although Flyway had no control over this.
- Flyway did allow credit card payments for software across the Internet, using a company credit card, but only with prior purchase approval from the IT Risk Management section.
- Flyway were not willing to provide anonymous Internet access to external Web sites, as they needed to hold employees accountable for their actions, and therefore needed to log their accesses.

(iii) Censorship

Flyway's comments on students' censorship expectations in employment, from mini case B, were:

- Most students decried censorship—i.e. company filtering of dubious sites and newsgroups. However, Flyway would not support employee accesses to "just anywhere", as external sites could log the Flyway firewall DNS, and then use the gathered information for adverse publicity purposes, claiming, for example, "In May, 1998, xxx employees from Flyway accessed the .... Web site". Hence, to protect themselves, Flyway had to filter out dubious sites.

(iv) Right to be kept informed

Flyway's comments on students' expectations in employment, from mini case B, were:
Flyway fully concurred with the students' desire for policy and related awareness activities. In the new infrastructure, a comprehensive Internet security policy, incorporating a comprehensive IAUP, and including a full range of awareness activities, would be developed—subject to resource availability.

(v) Accountability

This issue is at the heart of most peoples' cynicism with respect to Internet security policies and acceptable use policies: ***How does one make them work?***

Flyway's comments on students' expectations for accountability for their Internet actions, in employment, from mini case B, were:

- *Students were willing to be held accountable via policy and awareness activities, but not via monitoring*. ***Flyway held firm that monitoring was an essential activity for accountability.*** Monitoring was required for two purposes. The first was 'corporate governance', that is, to fulfil corporate obligations to stakeholders, who would believe it prudent to have monitoring to minimise the risks associated with unmonitored Internet usage. The second was to protect the employees themselves: Innocent employees could prove their innocence by pointing to the audit trail—in this case, the firewall logs.

Methods suggested by students for making the policy work, which Flyway *agreed* with, were:

- Gaining employee co-operation, explaining policy benefits to employees, setting and enforcing penalties, monitoring via human observation, Internet awareness sessions, and displaying of policy on browser start-up (presently, a legal disclaimer notice is displayed on browser start-up, referring the user to the IAUP).

Methods suggested by students for making the policy work, which Flyway *disagreed* with, were:

- Employee involvement in policy creation: Firstly, Flyway did not believe that employees would have the skills, knowledge and responsibilities required to be of real use—a sad reflection of managerial perceptions of employees in modern company life. Secondly, Flyway believed that only small groups of three to five people were workable to develop the policy, and that relevant unions, of which there were several, would haggle over which unions had representatives in the working group.
- Get employees to sign a consent form: Flyway was dropping its current procedure for obtaining employee signatures on the IAUP as there was such a rapid request rate from employees for access that there was no time for this formality.
- Give each employee his/her own copy of the policy: Flyway intended to put the policy on a Web page instead.

Flyway did not believe that specific sanctions should be specified for various misuses or abuses, as:

- there were inadequate resources to write them all down in the policy, let alone to monitor for those abuses and apply the applicable policy.
- such sanctions would reflect an attitude of employee distrust. Instead, Flyway had a cover-all sanction: "disciplinary action" at the bottom of the IAUP, and the specific action was left to the judgment of the manager of the IT Risk Management section.
- Flyway did not approve of a combination suggestion such as that made by many students: "one or two warnings, followed by suspension of connection, followed by dismissal", because placing such a statement in a policy would be politically unacceptable from, for example, a union's perspective.

(vi) Ownership

Flyway's comments on students' expectations in employment, from mini case B, were: Students did not really expect freedom of home page design, and Flyway, looking to its future, concurred that pages should follow Flyway publication guidelines. Flyway further added that employee email belonged to the company, not to its employees.

(vii) Ethics

Flyway's comments on students' expectations in employment, from mini case B, were:
Students appeared to regard Internet use as "all rights, no responsibility", with their pro-free-use, anti-censorship, anti-monitoring, pro-privacy attitudes. Flyway were keen to promote a "some rights and some responsibilities" attitude instead, by promoting an atmosphere of trust and care, while protecting the company and its employees from Internet traffic delays, legal liability, and other unpleasant consequences of employee Internet misuse and abuse.

7.4.2 Analysis of support for the Factors model and component models

Flyway approved the model of influential factors in Internet security policy (Figure 3-3), in particular the concept that all factors should be considered with due regard for the human issues involved.

This case study provides empirical support for the Factors model (Figure 3-3) and its various components (*Internet risks, organisational issues, administrative factors, legal factors, societal factors, technical factors and human issues*) as follows.

This case study supported the inclusion of *Internet risks* in the Factors model in the discussion in Section 7.4.1.1, in that many Internet risks were not being adequately addressed by the current IAUP. The study also supported the model of Internet risks shown in Figure 3-5, as discussed in Section 7.4.1.1, in that

Flyway acknowledged that all the risks shown in the model were present, to varying degrees of significance, within their company.

The case study supported the inclusion of *organisational issues* in the Factors model in the discussion in Section 4.1.2, in which I investigated each of the issues in the proposed organisational issues model (Table 3.2): I found that:

- employees were not adequately informed of acceptable Internet uses (*organisational objectives* issue);
- there was a need for documenting future Internet infrastructure in the policy (*Internet security infrastructure* issue);
- there was uncertainty regarding the need to show management support in the policy itself (*management commitment* issue);
- there was a need for an Internet security management programme to support the policy, and this programme should be documented within the policy (*Internet security management programme* issue);
- there was a need for policy integration, with related policies being referenced within the Internet security policy (*policy integration* issue);
- the policy needed to include details of Internet security awareness activities (*Internet security awareness* issue); and
- the policy needed to meet prespecified principles (for example, enforceability) (*principles* issue).

The case study supported the inclusion of *administrative issues* in the Factors model in the discussion in Section 7.4.1.3, in that many Internet security procedures were not documented anywhere, and should either be documented or referenced in an Internet security policy.

The case study supported the inclusion of *legal factors* in the Factors model in the discussion in Section 7.4.1.4, in that employees were not adequately informed of relevant legal precautions in their Internet use. The employees should be informed via an Internet security policy.

The case study supported the inclusion of *societal issues* in the Factors model in the discussion in Section 7.4.1.5, in recognising a need for company netiquette standards and ethical guidance in Internet use as part of an Internet security policy.

The case study supported the inclusion of *technical issues* in the Factors model in the discussion in Section 7.4.1.6, in that the requirements for new technologies which could assist in reducing risks should be specified in the Internet security policy.

The case study supported the inclusion of *human issues* in the Factors model in the discussion in Section 7.4.1.7, in that each of the issues in Table 3.4 (freedom of Internet use, privacy, censorship, right to be

kept informed, accountability, ownership and ethics) were shown to be critical, and, in many cases controversial, issues to resolve in order to assure the effectiveness of the developed Internet security policy. The dilemmas to be faced were illustrated by presenting Flyway personnel at the interviews with the results of mini case B, in which final year university students put forward their views on human issues. Flyway's responses clearly highlighted potential clashes between the employee perspective (as represented via the mini case results) and the employer's perspective (as represented by Flyway), in setting policy involving human issues. The study also loaned support for the model of human issues (Table 3.4) through highlighting the impact of each issue in the table, on policy.

7.4.3 Analysis of support for Content models

Having discussed the Factors model in Section 7.4.2, I now discuss the support provided by this case study for three of the content models. The background discussions in Section 7.2 and 7.3, the case analysis in Section 7.4.1, as well as the content of Flyway's existing IAUP (which contained an email sub-policy, as mentioned earlier), suggest *direct* support for the model of *Internet security policy content* (Table 4.1), the model of *IAUP content* (Table 4.3) and the model of *email policy content* (Table 4.4). This support is summarised in Tables 7.2, 7.3 and 7.4, which include references to the sections in this Chapter indicating support.

I have not justified the indicative support for the supported sub-components in this section, as there is adequate evidence provided throughout Sections 7.2, 7.3, and 7.4.1. Instead, I have referred the reader to the relevant sections for each supported sub-component, within the tables.

Finally, I queried Flyway on their view of the proposed content for these policies, and received general approval. Flyway made a final comment that the Internet firewall policy should be restricted, i.e. not made available to the employees, as this may compromise security, in that employees may reveal such details to other hostile parties, who may then use the access rules to gain unauthorised access.

Internet security policy content	Sections providing support
Purpose and scope of policy	7.4.1.2
Philosophy of policy	7.2.3
Internet security infrastructure	7.2.1, 7.2.3, 7.3
Internet security management programme	7.4.1.2
Other applicable policies	7.3
Internet privacy policy	7.4.1.7
Internet censorship policy	7.2.3, 7.4.1.7
Internet responsibility and accountability policy	7.2.3
Internet information protection policy	7.2.3
Internet information access policy	7.2.3
Internet firewall policy	7.2.2
Internet security technology policy	7.4.1.6
Password policy	7.2.3
Internet acceptable usage policy	7.3
Internet publication policy	7.4.1.1
Email policy	7.3
Internet virus policy	7.4.1.1
Internet audit policy	7.4.1.3
Internet incident policy	7.4.1.1
Internet legal policy	7.4.1.4
Internet security policy review policy	7.3

Table 7.2 Internet security policy content support at Flyway

The first column of Table 7.2 lists the policy components suggested in the Internet security policy model (Table 4.1), while the second column lists the sections in this Chapter indicating support for the components.

Internet acceptable use policy content	Sections providing support
purpose and scope of policy	7.4.1.2
ethics policy	7.4.1.5
Internet services policy	7.3
confidentiality policy	7.2.3
acceptable uses	7.4.1.2, 7.4.1.7
unacceptable uses	7.3
Internet risks	7.4.1.1
legal policy	7.4.1.1
roles and responsibilities	7.3
privacy	7.4.1.7
accountability	7.2.3
monitoring and surveillance	7.2.3, 7.4.1.7
sanctions	7.4.1.7
awareness	7.4.1.2, 7.4.1.7
user consent	7.4.1.7

Table 7.3 Internet acceptable use policy content support at Flyway

The first column of Table 7.3 lists the policy components in the IAUP model (Table 4.3), while the second column lists the sections in this Chapter which indicate support for the components.

Email policy content	Policy support	Sections providing support
email ownership	•	7.4.1.7
acceptable email usage	•	7.4.1.1
email privacy	•	7.4.1.7
email encryption	•	
email monitoring	•	7.2.3, 7.4.1.7
email netiquette	•	7.4.1.7
emotional email	•	7.4.1.1
avoidance of references to third parties		
duties to third parties (eg auditors)	•	
external interception of email		
email deletion after usage	•	
distribution of email copies	•	
copyright implications of copy distribution	•	
legal issues	•	7.4.1.4
email virus protection	•	7.4.1.1
enforcement and dissemination of policy	•	7.4.1.2

Table 7.4 Email policy content support at Flyway

In the first column, I list the components of the email policy model (Table 4.4). In the second column, I mark with a bullet those components supported by Flyway's email policy (which resided within Flyway's IAUP) and/or other parts of the IAUP. In the third column, I list the sections which provide case study support for each component.

Note that I have added a new sub-policy for email virus protection to my model for email policy content, after finding such a sub-policy within Flyway's email sub-policy (in the IAUP).

I point out here that I did not attempt to analyse support at Flyway for the model of firewall policy (Table 4.2) as Flyway's firewall policy (at that time) only existed in network router protocol language form.

7.4.4 Analysis of support for framework for development of Internet security policy

Flyway believed that the approach for developing an Internet security policy, as portrayed in Figure 4-1, was excellent. *In particular, they liked the holistic nature of the approach*, with many diverse aspects being taken into account via the Factors model (Figure 3-3). The fact that some Internet risks were rated as more significant than others highlights the need for the risk assessment process shown in the framework.

Flyway also advised that their preferred technique for information security risk assessment was to use the judgment and experience of resident information security experts to identify the significant risks, rather than a formal, quantitative risk assessment method or technique. This was because their staff lacked the social science skills required to perform such techniques. However, they recognised that they needed to acquire these skills and utilise formal quantitative techniques in order to present a convincing business case to management. This was their best chance for obtaining the required resources for information security (including Internet security).

7.5 Conclusion

I commence this section by summarising the research models supported by the case study results, then draw conclusions for this research project, and make a few final remarks.

7.5.1 Summary of models supported by case study

I obtained support via this case study, as described in detail in Section 7.4, for the following aspects of the overall framework for Internet security policy:

- factors in Internet security policy (Figure 3-3)
- societal issues in Internet security policy (Section 3.4.2)
- Internet risks for Internet security policy (Figure 3-5)
- organisational issues in Internet security policy (Table 3.2)
- administrative issues in Internet security policy (Section 3.4.5)
- legal issues in Internet security policy (Section 3.4.6)
- technical issues in Internet security policy (Section 3.4.7)
- human issues in Internet security policy (Table 3.4)
- Internet security policy content (Table 4.1)
- IAUP content (Table 4.3)
- email policy content (Table 4.4)
- framework for development of Internet security policy (Figure 4-1)
- overall framework for Internet security policy (Figure 4-2)

7.5.2 Case study conclusions

In this section, I first indicate the presence of an Internet security problem at Flyway, then discuss what this case study mean in terms of the original research questions, as stated in Chapter 1.

This case study clearly shows the existence of an Internet security problem at Flyway, with inadequate control measures in place. I found that Internet risks were occurring at Flyway with varying degrees of significance, and that these risks were not being effectively controlled by existing policies (in particular, the IAUP), nontechnical measures (such as training) and technical measures (such as a firewall).

I now discuss the ways in which this case study has addressed the three research questions:

1. What are the factors influencing effective Internet security policy for an organisation?

This investigation identified a number of factors to be addressed by an effective Internet security policy, as summarised below.

As described in Section 7.4.1.1, the case study revealed four highly-rated Internet risks at Flyway—all inadequately managed by the existing IAUP and various other measures. The risks were—*non-business usage, hacking, accidental erroneous business transactions and corrupted or erroneous software*. I also identified a number of other Internet risks as being of significance. Flyway agreed that all the risks in my Internet risks model (Figure 3-5) needed addressing in a future policy, thereby not only supporting the Internet risks model (Figure 3-5) and the Factors model (Figure 3-3), but also contributing to answering the research question listed above.

As described in Section 7.4.1.2, the case study revealed that organisational issues, such as the need to establish a formal Internet security infrastructure and an Internet security management programme, would need to be addressed by a future policy. All the organisational issues listed in the proposed model (Table 3.2) were identified as influences on the policy, thereby supporting this model as well as the Factors model (Figure 3-3), and also contributing to answering the research question listed above.
As described in Sections 7.4.1.3, 7.4.1.4, 7.4.1.5 and 7.4.1.6, this case also illuminated administative, legal, societal and technical factors which would influence the policy. It was also clear that human issues would play a critical role in the final policy, justifying its special place in the factors model.

The Factors model that I proposed in Figure 3-3 included all the types of factors that I identified at Flyway: Internet risks, organisational, administrative, legal, societal, technical and human issues. Hence, this case study has helped answer this research question by firstly identifying factors which influence the

Internet security policy at Flyway, and then by pattern-matching of those factors with the ones proposed in my Factors model (Figure 3-3).

2. Is a holistic approach to an Internet security policy more effective than the piecemeal approach adopted to date?

The investigation of Flyway suggested that only by considering and drawing together the diverse factors identified, could an effective policy be developed. Hence this investigation has contributed to answering this research question in the affirmative.

3. Can a framework be specified for the development, issues and content in effective Internet security policy for organisations?

Evidence of support for the proposed framework (Figure 4-2) has been amply provided by this case study. Firstly, as already mentioned, the diverse factors (issues) that I identified at Flyway as influencing an Internet security policy, correspond to the various types of factors specified in the Factors model component (Figure 3-3) of the framework. This case study also suggests that, with Internet risks being rated as of varying levels of significance, a risk assessment is an appropriate process for developing the policy, as is shown in the framework. There is also ample evidence provided in Section 7.4.3 of support for the three proposed Content model components of the framework (Table 4.1, Table 4.3 and Table 4.4).

Note that I discovered a new sub-policy for email virus protection for the model of email policy (Table 4.4) as a result of this study.

Hence, this study has provided support for the proposed framework, and has contributed to answering this research question in the affirmative.

7.5.3 Final remarks

It may be of interest to the reader to hear of Flyway's immediate gains from the conduct of this study, as well as its follow-up plans. As a result of this case study, Flyway was reviewing its Internet security measures, both managerial and technical, in order to more effectively address the problems identified. In particular, Flyway was keen to reduce the risks of non-business Internet usage, hacking, accidental erroneous business transactions and corrupted or erroneous software, all of which were rated as high risks in the risk assessment.

Flyway announced in June, 1998 that its Web site was being reviewed, motivated in part by this case study alerting it to the importance of a high quality Web site, and their self-expressed dissatisfaction with their own site. They subsequently redesigned, developed and implemented a new and improved site.

More importantly, though,
Flyway recognised the need for an organisational Internet security infrastructure to manage all the measures required, and within this, the need for a comprehensive Internet security policy which would include, as a sub-policy, a new version of their current IAUP.

However, Flyway suffered, like many companies worldwide, from a shortage of human resources to develop this new infrastructure and policies.

As Flyway did not anticipate gaining additional human resources for such development purposes in the near future, it planned, as an interim measure, to improve its Internet usage and security via stronger use of firewall technology, improved Internet training and awareness, and a revised, more restrictive, IAUP.

Although there is more which can be concluded from this case on its own:
in the interests of keeping this thesis to a manageable size, I am reserving further conclusions for a later stage of the thesis.

In the next Chapter, I describe the third of the detailed case studies, a study of Aus-Retail Ltd, a large Australian retailing company, in order to explore the topic area further.

Chapter 8
Case Study: Aus-Retail Ltd

Earlier in this thesis, I built a framework for Internet security policy for organisations (Figure 4-2), which I have thus far explored via two mini case studies and two detailed case studies. These studies provided valuable support for the proposed framework. In this Chapter I present the third case study, conducted at Aus-Retail Ltd, Australia's largest retail company, in February, 1998. This case, like the previous two, focuses on the employer perspective of the issues involved.

I commence by introducing Aus-Retail Ltd and outlining case procedures. I then provide background to the Internet infrastructure and usage at Aus-Retail Ltd. Finally, I present the case study analysis and results, and draw conclusions.

8.1 Introduction to Aus-Retail and the case study procedures

For reasons of anonymity, I present only a very limited introduction to Aus-Retail Ltd (neceforth referred to as AUR). AUR is a large retail organization in Australia, with thousands of employees (at the time of study) spread across Australia. AUR has major offices and operations around Australia, and overseas.

Aus-Retail Computing Services, a division of AUR, was, at the time, in charge of several departments—including Information Technology Security (ITS), Audit and various other departments. ITS was responsible for AUR information security administration and management.

By 2000, AUR exhibited a web site with limited e-commerce capability, however at the time of the study, the AUR web site was not yet conducting e-commerce.

8.1.1 Sampling procedure

I selected AUR because it was typical of large organisations which had embraced the Internet to a significant extent—including actual electronic commerce transactions; and because it represented a particular industry segment—the retail sales industry.

I was also aware that AUR had launched a major electronic commerce initiative in late 1997, and hence would be ready to address Internet-related problems.

8.1.2 Data collection and case instrument

I collected data for this case study via two semi-structured interviews of approximately one and a half hours' duration each, with the manager of AUR's Information Technology Security (ITS) division. I employed:

(vii) a collated document consisting of the various models composing the framework in Figure 4-2, as well as summarised responses from the mini case, Case B, showing student expectations (when eventually employed) regarding human issues in Internet acceptable usage; and

(viii) a set of guideline questions (see below) which constantly referred to the collated document to structure and guide the interviews.

I collected one document—AUR's Information Security Management Standards (ISM standards), which was extensive and lengthy.

The questions I asked of the ITS manager in order to structure the interview were:

(b) to provide background information about his company, Internet usage, Internet architecture and Internet access controls;

(c) to perform a qualitative risk analysis of AUR's Internet risks using the Internet risks model (Figure 3-5) as a guide, in order to determine the significance of each identified Internet risk, and to gauge support for the model;

(d) to comment on the Factors for Internet security policy model (Figure 3-3) in the context of AUR, and to gauge support for the model;

(e) to provide information about AUR's current approach to developing Internet security policy;

(f) to comment on the Internet security policy development model (Figure 4-1); and

(g) to comment on the Internet security policy structure and content model (Table 4.1) and the IAUP content model (Table 4.3), as these models related to AUR's situation.

8.1.3 Case conduct

I recruited the company by telephone, and despatched an explanatory document describing the research project to the main contact for perusal, before receiving formal agreement to the study. Interview times were arranged by email after the initial agreement had been obtained. The main contact signed a research consent form at the initial interview.

The two interviews were approximately one and a half hours in duration, taking place at AUR's ITS offices. I distributed a copy of the collated document of proposed models to the ITS manager at the first interview, and followed the set of questions listed in Section 8.1.2 to obtain the data required. I took notes during the interviews.

8.1.4 Data analysis

I later analysed the data collected by comparing and contrasting the collected data with the component models of the proposed framework, and identified similarities, differences and patterns. A draft copy of the resulting case study analysis was forwarded to the ITS manager for correction, and for the addition of any missing information.

8.2 Internet infrastructure and usage

8.2.1 Internet security as a "vertical slice" of information security

AUR lacked a formal organisastional Internet security infrastructure, although it planned to set one up in the future—when full-scale Internet transactions were implemented.

AUR, like Flyway, regarded Internet security as a vertical slice within information security. There was no specific Internet plan or strategy. Internet use was driven by the Marketing division's perceptions and decisions. The undocumented Internet security posture was "permissive"—everything was allowed except what was explicitly forbidden.

8.2.2 Internet usage

The Internet had been been deployed at AUR since 1996, with several thousand office employees using it for email. About 1000 of those employees accessed Web browsers residing on their PCs. Approval of requests for browser installation was based on proof of business need, and the relevant business unit was charged running costs. Many of those employees also retained FTP access privileges. There was no telnet, news or chat service provision.

At the time, AUR used the Internet for information sharing and management, research (searching for, and evaluating, Web sites of competitive vendors and potential suppliers), communication and collaboration, downloading software patches, email purchasing negotiations (with retail and computer suppliers) and a limited number of transactions. *As already mentioned, AUR was planning full e-commerce functionality as a major initiative. (Note, in May, 2000, there was still only limited purchasing operational, as part of planning.)*

8.2.3 Internet architecture

Figure 8-1 illustrates the Internet architecture at AUR.

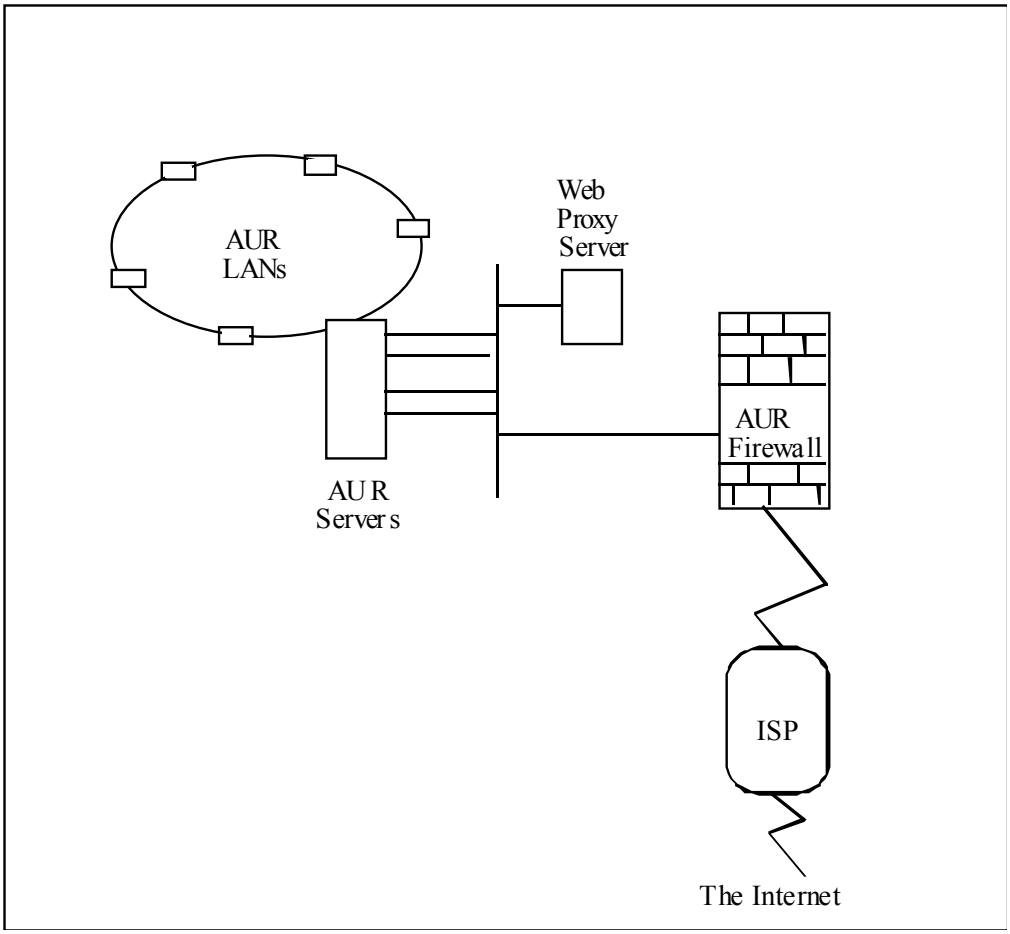

Figure 8-1 Internet architecture at Aus-Retail Limited

Employee workstations were mainly Pentiums and 486's connected internally at each geographic location via LANs. The LANs were connected to a proxy server and a firewall, in a main city. The firewall connected to an ISP via a direct line. Most of the network was centred in the one location, with links between three or four different buildings, and each building possessed a sizeable LAN. There were long distance links to other Australian locations; some of these were dial-up and some ISDN. There was a permanent overseas link to one country and a dial-up link to yet another.

There were several mainframes (containing corporate systems) connected to the LANs, although the company considered it technologically unlikely that these mainframes could be accessed from outside the company (if the firewall did not prevent access, there were still many other technical hurdles to overcome to gain access). In addition, data and processes were distributed, in order to minimise risks of data and software compromise.

8.2.4 Internet access control

8.2.4.1 Internet access policy at AUR

AUR believed that Internet access was first and foremost a business-need issue—provided there was a genuine business need, the requested Internet access privileges would be permitted. Internet access control was handled by an access policy implemented by a proxy server and firewall, located in a city. Together these implemented Internet access control, logging, and storage of information required for monitoring usage. Employees with browser facilities connected to the proxy server which consulted an access control list of user login ids and passwords in order to grant or deny Internet access.

8.2.4.2 Proxy server control of Internet service access and Web site access at AUR

The proxy server provided Web-http and ftp access control using a list of authorised user login ids and passwords to grant the requested accesses.

8.2.4.3 Firewall filtering, logging and monitoring at AUR

The proxy server connected to a firewall which monitored and restricted incoming traffic, logged all accesses and emails, and denied telnet in and out. The ITS manager monitored the firewall log via a daily exception report of suspicious attempts at hacking into or out of AUR, inappropriate email content and inappropriate site accesses. Occasional human surveillance of PC screens via "walking around" was also practised. The ITS department reviewed the firewall configuration and proxy server rules from time to time.

If suspicious activities were observed on the firewall exception reports, the ITS manager evaluated the situation and acted accordingly. Employees were aware that their site accesses and emails were being logged, and that the firewall log was being monitored. They were so informed through the ISM Standards and word of mouth.

8.2.5 Information security policies

Several policy documents informed employees of their information security responsibilities and restrictions, although none of these was Internet specific.

Existing policies consisted of:

- a document setting out AUR's Information Security Management standards (ISM standards) (restricted readership of AUR staff only), containing AUR's information security policies, standards

and procedures, developed by a AUR working group in 1995, and approved by several policy committees. The latest release at the time was June, 1997;

- individual business unit policies which had to conform with ISM standards;
- AUR Code of Conduct;
- an Internet access request form including a user consent-to-conditions signature section;
- a firewall policy (in network protocol language)—inaccessible by ordinary employees; and
- an Internet access policy implemented as a list consulted by the proxy server (again, inaccessible by ordinary employees).

The ISM standards were guidelines only rather than being prescriptive, and formed the basis for each AUR business to develop its own procedures. The ISM standards were in part based (with permission) on the standard for Information Security Management (AS/NZS 4444-1996) issued by Standards Australia.

The ISM standards document contained thirteen (13) information security policies, summarised below:

- information is a company asset;
- controlled access to electronic data;
- controlled access to company networks;
- login ids and passwords constitute the user authentication mechanism;
- individuals accountable for systems use;
- individual responsibilities in systems use to be clearly stated;
- prohibited use of unauthorised software;
- AUR-owned copyright to all AUR-developed software;
- contingency plans must be defined;
- security for systems borrowed by AUR subject to the same security as AUR systems;
- authorised access to external systems via AUR facilities;
- AUR information not to be distributed externally unless authorised by the information owner; and
- exemptions to policies were only permitted with approval of Director of ITS.

The ISM standards contained twenty-one sections, forming an extensive document of over fifty pages. *Internet-related standards and policies were very much disguised within each section*, with the most relevant section being "Computer and network management".

The ISM standards did not mention the word Internet or the phrase World Wide Web. There would be no way an employee could easily utilise this lengthy document to specifically determine Internet acceptable usage, Internet unacceptable usage, compliance requirements or other Internet-specific policies.

The ISM standard had been updated sporadically, six times at that stage since its initial development in the mid nineties. However, there had been one lapse of two years between two successive releases. These irregular policy reviews had resulted in out-of-date policies.

8.2.6 Plans for Internet security infrastructure and policy

As already indicated, AUR had an ad hoc Internet infrastructure but saw the need for a formal Internet infrastructure which it intended to develop as resources became available, and as the electronic commerce initiative gained momentum.

AUR recognised the need for an Internet security policy as a key component of the anticipated new infrastructure.

8.3 Case analysis

In this section I analyse the results collected by pattern-matching the data with various aspects of the proposed framework (Figure 4-2), specifically:

- factors in Internet security policy (Figure 3-3);
- societal issues in Internet security policy (Section 3.4.2);
- Internet risks for Internet security policy (Figure 3-5);
- organisational issues in Internet security policy (Table 3.2);
- administrative issues in Internet security policy (Section 3.4.5);
- legal issues in Internet security policy (Section 3.4.6);
- technical issues in Internet security policy (Section 3.4.7);
- human issues in Internet security policy (Table 3.4)
- Internet security policy content (Table 4.1)
- IAUP content (Table 4.3)
- email policy content (Table 4.4)
- framework for development of Internet security policy (Figure 4-1)
- overall framework for Internet security policy (Figure 4-2)

I initially analyse the various factors in Internet security policy at AUR (Section 8.3.1), then analyse support provided by this analysis for the factors model and component models (Section 8.3.2). Next, I analyse AUR's requirements for Internet security policy content, and support provided for corresponding content models (Section 8.3.3). I then analyse AUR's requirements for development of Internet security policy and support provided for the corresponding framework for development (Section 8.3.4).

8.3.1 Analysis of support for Factors model and component models

---

AUR agreed with the model of influential factors in Internet security policy (Figure 3-3), as well as with the concept that all factors should be considered with due regard for the human issues involved.

I now analyse each type of factor from Figure 3-3: *Internet risks, organisational issues, administrative issues, legal issues, societal issues, technical issues and human issues.*

8.3.1.1 Internet risks at AUR

AUR informally analysed their Internet risks, using the Internet risks model in Figure 3-5 as a guide to assist in identifying existing risks, and assigning each identified risk type a rating of low, medium or high, based on the professional opinion of the two information security managers interviewed, including their opinion-based, qualitative estimates of *frequency of risk occurrence* and *impact*. Results are summarised in Table 8.1 in order of most significant to least significant risk, and the analysis of each risk type is discussed below.

Internet Risks	**Risk Rating L, M, H**
Non-business usage	H
Corrupted or erroneous software	M
Accidental disclosure	M
Hacking	L
Low quality data	L
Inaccurate advertising	L
Inappropriate email	L
Pirated media	L
Accidental erroneous business transactions	L
Fraud	L
Denial-of-service	L
Theft of information	L

Legend: L = Low; M = Medium; H = High.

Table 8.1 Internet risks at AUR

(i) Non-business usage

In the ISM Standards, a section on employee responsibilities referred to policy (vi) (see Section 8.2.5), stating that computer assets be used by employees "solely in the interests of the company and for authorised business purposes only". The standards also stipulated monitoring of all kinds of system accesses (which naturally included the Internet) to ensure conformity with existing policies.

Even so, up until then, AUR had regarded non-business Internet use as harmless—even a perk of the job.

However, AUR reported that between 8am and 8pm, non-business usage was high, causing Internet traffic slowdowns. They estimated that about 50% of Internet usage was personal, with surfing and personal email the main culprits.

One employee had his Internet connection permanently disabled as a sanction for surfing the net all day. AUR were unable to distinguish business-hours usage from after-hours usage. However they calculated that, estimating half an hour per day per person with browser connection of non-business Internet usage, ***the company was experiencing approximately $60,000 in lost productivity per week.***

AUR had hoped that employee supervisors would act as controls when assigning and monitoring employee workloads, leaving little time for non-business Internet use. AUR also monitored by logging accesses on their firewall and alerting supervisors if individual employee misuse was observed on the firewall log. Supervisors then spoke to the employees concerned. Apparently, these measures were not enough to manage the problem.

With the high level of non-business Internet usage, combined with the ineffectiveness of current controls to address this, AUR rated this risk as *high*.

(ii) Corrupted or erroneous software

AUR's ISM standards referred to "protection from malicious software" within the Computer and Network Management Section, by requiring "precautions for prevention and detection of malicious software", as well as requiring that "procedures for antivirus software be active on microcomputers". Downloading of software was prohibited without authorisation, and employees were warned in the standards document to virus-scan software on an isolated system prior to use. There was no advice regarding viruses possibly sent as email attachments.

About two Internet-related viruses attacked each week, mainly macro or executable viruses. Desktop virus scanners were automatically activated whenever software was executed. Nevertheless, as AUR was

aware that damage from viruses could be severe, it rated the risk of 'corrupted or erroneous software' as *medium*.

(iii) Accidental disclosure

AUR's ISM standards referred to one of their thirteen policies within the Computer and Network Management Section, prohibiting unauthorised disclosure of confidential company information (see policy list in Section 8.2.5). There were many references throughout the extensive document to confidential data, defining it and prohibiting its disclosure, but they were not all in one place for convenient location. Email usage was logged and monitored via a daily exception report for compliance with this policy, but it was very difficult to identify confidential data in email via this approach.

Although the frequency with which accidental disclosure of confidential information via the Internet was occurring was low, AUR recognised that the potential impact could well be severe, and hence rated this risk as *medium.*

(iv) Hacking

AUR's ISM standards referred to one of their thirteen policies within the System Access Controls Section, prohibiting unauthorised access to external systems (see policy list in Section 8.2.5). This was effectively their "anti-hacking" policy. Several unsuccessful attempts by employees to access external systems via the Internet had been observed, although these were viewed as inquisitive rather than malicious.

Reducing attacks from the outside was handled by various measures: The firewall provided a technical mechanism to filter out unauthorised acceses, and logged hacking attempts. Data and processes were distributed, to reduce the impact of a successful hacking attempt. The ISM standards included login id and password protection standards and procedures to reduce the opportunity for external attackers to guess or borrow ids and passwords and thereby gain access. The standards also contained incident management procedures for responding to any observed security incidents (including hacking). For example, employees were instructed to report unusual security incidents.

AUR had observed several hacking attempts on the firewall log to date, but all of these had failed.

When planned, full-scale e-commerce actualised, AUR may view hacking as a significant concern. However at the time of the study, AUR still rated the risk of 'hacking' as *low*.

(v) Low quality data

AUR's ISM standards did not specifically deal with the dissemination of low quality data over public networks from within the company, nor the verification by employees of any external data accessed. However, all officially-advertised information emanating from AUR was thoroughly checked for accuracy prior to release. AUR required disclaimers at the end of email unless the email was an authorised official position, and email usage was logged and monitored via the firewall log as well as by daily exception reports, for compliance with email-disclaimer and other email-related policies.

AUR rated the risk of employee-generated 'low quality data' as *low*.

(vi) Inaccurate advertising

The ISM standards contained a cover-all email standard. All officially advertised information emanating from AUR was thoroughly checked for accuracy prior to release. As stated above, all email required disclaimers (placed at the end of email by employees) unless it was an authorised AUR official position.

Email usage was logged and monitored via the firewall log and exception reports for compliance. There had been several minor incidences of 'inaccurate advertising', but AUR still rated this risk as *low.*

(vii) Inappropriate email

The Code of Conduct and a coverall email standard in the ISM Standards warned employees against sending inappropriate email. Although the frequency of incoming junk email had been high, its impact had been low, not yet causing much of an employee nuisance, and not yet causing Internet traffic delay. Further, AUR employees had not unduly complained about incoming junk email. AUR hence rated the risk of 'inappropriate email' as *low*.

(viii) Pirated media

Software piracy via the Internet was considered a "firing" offence at AUR, that is, employees would lose their jobs for this offence. The ISM Standard specifically deterred software piracy, thereby assigning responsibility for compliance with licensing conditions to employees. AUR also had a standard desktop environment, and could spot new software installations via human surveillance. This control had worked reasonably well, with about six detected pirated Internet software incidents in the previous three months (November, 1997 - January, 1998). AUR believed the surveillance of desktops and a strong awareness by employees of the "firing" consequence of piracy, were managing the risk satisfactorily, and therefore rated the risk of 'pirated media' as *low*.

(ix) Accidental erroneous business transactions

The ISM standards referred to "the need to establish AUR controls for the safeguarding of the confidentiality and integrity of data passing over public networks" within the Computer and Network Management Section of the standards, and referred elsewhere to encryption to assist with this protection.

In regard to misdirection of email, the standards included a very simple email standard, which did not include advising employees to check email destination address prior to despatch.

There had been several cases at AUR of misdirected personal email, but AUR had not observed any serious ramifications, and hence rated the risk of 'accidental erroneous business transactions' as *low*.

(x) Fraud

When full-scale electronic transactions were eventually realised, AUR believed Internet fraud would be viewed as a high risk. However *at the time of study*, AUR rated the risk of (Internet) 'fraud' as *low*, as no financial databases were accessible yet via the Internet.

(xi) Denial-of-service

AUR's ISM standards referred to planning for capacity within the Computer and Network Management Section, but didn't specifically mention the Internet facility. AUR had experienced Internet traffic slowdown, believed to be due to excessive non-business usage, but had not yet suffered total denial-of-service. AUR's attitude to date had been not to rely on the Internet unless there was a recovery procedure to follow should problems arise (at the time, no such procedures had been defined). Due to the absence of Internet reliance, AUR rated the risk of 'denial-of service' as *low*.

(xii) Theft of information

The ISM standards included several statements prohibiting employees from possessing "stolen" (illegal or as-yet-unlicensed) software. The company Code of Conduct also cautioned against stealing as an unethical activity.

The email standard warned employees that their email could be intercepted by external parties.

AUR reported only the Internet software piracy problem from those mentioned above. AUR was unaware of any employees plagiarising from Web sites or stealing external data, nor had corporate data been

stolen from AUR (note that the data and processes were distributed for added protection), or email intercepted (that AUR was aware of). This risk was rated as *low*.

(xiii) Summary of Internet risks and their management

It was clear that AUR had significant Internet risks. AUR ranked non-business usage as its major Internet risk, with corrupted or erroneous software and accidental disclosure as the two next-highest risks of concern.

AUR clearly recognised that a large document not structured according to Internet-related issues was too large, cumbersome and unsuitably formatted for use as an IAUP.

AUR saw the need for an IAUP which addressed each of the Internet risk type in the Internet risks model (Figure 3-5), hence providing support for the model. They also saw the need for the Internet security policy to include the IAUP.

8.3.1.2 Organisational issues in Internet security policy at AUR

Table 3.2 suggested the following broad categories of organisational factors influencing Internet security policy: *organisational objectives, Internet security infrastructure, management commitment, Internet security management programme, Internet security awareness, policy integration, and principles for Internet security and policy*. I discuss each of these below.

(i) Organisational objectives:

AUR employees were given ample advice in the ISM standards regarding the requirements for business usage and "need to know" based Internet access, with little detail supplied about what constituted valid business usage. AUR agreed that valid business usage of the Internet should reflect an Internet strategy based on organisational objectives.

(ii) Internet security infrastructure:

In Section 8.2 of this Chapter, I described the lack of a formal organisational Internet security infrastructure at AUR, and AUR's future plans for such an infrastructure when additional resources were provided and when full-scale electronic transactions were implemented. This new infrastructure would be documented in the Internet security policy.

(iii) Management commitment:

Senior managers were not involved in Internet security awareness activities due to lack of time and lack of awareness of existing problems. *The manager I interviewed believed senior manager involvement, when a formal infrastructure was in place, would be beneficial, but of little use until then.*

(iv) Internet security management programme:

AUR believed its policies constituted a semi-formal programme already, but conceded that a formal well-thought-out programme with an Internet security policy and associated awareness activities would be preferable.

(v) Internet security awareness:

There were no formal Internet security awareness activities in place.

(vi) Policy integration:

As mentioned in Section 8.2, there were several company policy documents relevant to employee Internet acceptable use. These were referenced within the IAUP. AUR integrated its various policies, and this approach would be continued in the planned formal Internet infrastructure, with all relevant policies being integrated, and referenced within the new Internet security policy.

(vii) Principles for Internet security and Internet security policy:

AUR understood the need for *enforceability,* and other principles for the new Internet security policy. They already adhered to certain principles, such as Internet usage being granted on presentation of a business case as well as a "need to know" justification.

8.3.1.3 Administrative factors in Internet security policy at AUR

Many administrative security procedures were specifed—albeit at a fairly high level—within the ISM Standards. Internet security procedure requirements would need to be specified in any new Internet security policy: for example, procedures for internal and external audits. However at the time, all Internet-specific procedures were in the heads of ITS personnel rather than on paper. Procedures to be carried out by employees, for example virus-scanning, were summarised in the ISM standards.

8.3.1.4 Legal factors in Internet security policy at AUR

AUR had a legal section which checked their policies for legality. Some laws were referred to within the ISM standards, but the references were distributed within the document. AUR believed that a section on applicable laws for employee and company Internet usage would be useful to include in an Internet security policy.

8.3.1.5 Societal factors in Internet security policy at AUR

AUR acknowledged that their employees were behaving unethically in misusing their Internet privileges through excessive personal use. The company Code of Conduct was obviously insufficent to deter employees. AUR recognised the need for ethical and netiquette standards (as part of an Internet security policy). With possible overseas orders for AUR products taking place when full e-commerce was realised, AUR also saw the need to include advice for dealing with different cultures within the policy.

8.3.1.6 Technical factors in Internet security policy at AUR

AUR had Internet risks which could be reduced by new or improved technologies. For example, AUR mentioned the need for an improved logging mechanism, funding permitting. They believed that requirements for Internet security technologies should form part of the Internet security policy.

8.3.1.7 Human issues in Internet security policy at AUR

Human issues included in the human issues model (Table 3.4) are: *freedom of Internet use, privacy, censorship, right to be kept informed, accountability, ownership and ethics.*

(i) Freedom of Internet use

There was an obvious problem with employees using the Internet for personal reasons about 50% of the time. AUR's attitude—that Internet use was a perk of the job—did not augur well for controlling the problem, and AUR was being forced to rethink its philosophy. However, there would be problems in deciding the appropriate degree of freedom of Internet use for employees.

AUR's comments on students' expectations in employment, from mini case B, were:

- Students expected about two hours' non-business usage per day, and mostly expected to use the Internet for personal reasons at lunchtime or after work only: AUR thought this was workable, providing that supervisors took some monitoring responsibility.
- Some students expected free use of the Internet at work: AUR believed Internet use was a *cultural* issue. Their culture was reasonably casual and permissive, but not as permissive as some companies

that are goal-oriented (and allow totally free use of the Internet at any hour, provided work is carried out satisfactorily). AUR expected employees to get their work done and also be able to use the Internet for personal use, within the two to three hour limit outside work hours, as mentioned above.

- Most students expected personal email permissions at work, although not other privileges such as the ability to download games and images, or the ability to freely design employee home pages: AUR's policy was that personal email use within reasonable limits was acceptable, while downloading games and images was not. They discouraged such behaviour within their Code of Conduct.

Overall, AUR was fairly much in agreement with the usage expectations of students verging on entering the workplace, according to the results of mini case B: Nevertheless, they still believed in the safety of a policy which stipulated:

Use of the Internet is a privilege, not a right. There is to be NO personal usage of the Internet.

The employee's supervisor then had to take ultimate responsibility for policy enforcement, as follows: If the employee got their work done, and the line manager perceived limited personal Internet use in or out of hours, with NO abuse, then a blind eye was turned on such limited personal use (as for Flyway). As Internet delays were becoming all-too-frequent, this "lenient attitude" was not working—hence, the need for a policy with supporting technological implementation.

(ii) Privacy

AUR's comments on students' high levels of privacy expectations in employment, from mini case B, were:

- AUR would like a policy which warned staff to watch out for privacy assurance symbols on Web sites they visited, in order to assure themselves of a level of privacy.
- AUR encouraged credit card payments for software across the Internet with its own electronic transactions both now and in the planned future full-scale electronic transactions, and therefore declined to comment on this issue, regarding it as a "conflict of interest".
- AUR was interested in providing anonymous Internet access to external Web sites, as it believed in employee anonymity when visiting Web sites.

(iii) Censorship

AUR's comments on students' censorship expectations in employment, from mini case B, were:

- Most students denounced censorship—i.e. company filtering of dubious sites and newsgroups. AUR did not believe in filtering out dubious sites—that is, in censorship of what was viewed by employees. It also thought many useful sites would be inadvertently blocked if filtering took place. AUR pointed out that if companies admit to filtering, they may be in trouble legally.

AUR commented that employee access to dubious sites was a "people problem" which required "people management", not technological management, and that supervisors should be checking for reasonable employee Web site accesses by old-fashioned "walking around" methods.

(iv) Right to be kept informed

AUR's comments on students' expectations in employment, from mini case B, were:
AUR (like Flyway) fully concurred with students' desire for policy and related awareness activities. In the new infrastructure, a comprehensive Internet security policy, incorporating a comprehensive IAUP with a full range of awareness activities, would be aimed for—subject to resource availability. A netiquette guide was a good idea, but it should not be too prescriptive.

(v) Accountability

This issue is at the heart of any cynicism concerning Internet security policies and IAUPs. ***How does one make them work?***

AUR's comments on students' expectations for accountability for their Internet actions, in employment, from mini case B, were:

- *Students were willing to be held accountable, via policy and awareness activities, but not via monitoring*. AUR, like Flyway, held firm that monitoring is an essential activity for accountability. AUR did say that access to the firewall log should be restricted and well controlled, to prevent unauthorised access.

Methods suggested by students for making the policy work, which AUR *agrees* with are:

- Gaining employee co-operation, explaining policy benefits to employees, setting and enforcing penalties, monitoring via a person, Internet awareness sessions, employee consent forms, giving each employee a copy of the policy, and displaying of policy on browser start-up.

Methods suggested by students for making the policy work, which AUR *disagrees* with are:

- Employee involvement in policy creation: AUR does not believe that this is a feasible idea in a large company with over 150,000 employees, and also does not think it would make any difference having employees involved, as a good result could be achieved either way.

AUR approves of use of the following sanctions: warnings, short-term suspension of Internet connection, and eventual dismissal—but not of fines, which would not be culturally acceptable. AUR approves of a combination suggestion such as that made by many students: "one or two warnings, followed by

suspension of connection, followed by dismissal", but are wary of dismissal in general, with "unfair dismissal" being regarded as highly unethical.

They also suggest billing employees for recovery time from employee-caused incidents, hinting that, indeed, this may have already happened at AUR.

(vi) Ownership

AUR's comments on students' expectations in employment, from mini case B, were: Regarding unconstrained employee home page design, AUR did not accept employee "freedom of speech" for a commercial company (which it is). This tied in with the students' expectations.

(vii) Ethics

AUR's comments on students' expectations in employment, from mini case B, were:
Students appeared to regard Internet use as "all rights, no responsibility", with their pro-free-use, anti-censorship, anti-monitoring, pro-privacy attitudes. AUR, like Flyway, were keen to promote a "some rights and some responsibilities" attitude, instead, by promoting an atmosphere of trust and care, while protecting the company and its employees from Internet traffic delays, legal liability, and other unpleasant consequences of employee Internet misuse and abuse.

8.3.1.8 Summary of case support for the Factors model

The above discussion provided clear support (in varying degrees) for all major factors proposed in Figure 3-3: risks, organisational, administrative, legal, societal, technical and human issues. Support was indicated for addressing all Internet risks in Figure 3-5, all organisational issues included in Table 3.2, administrative issues, legal issues, societal issues, technical issues, and all human issues in Table 3.4, within the Internet security policy.

8.3.2 Analysis of support for content models

The background descriptions in Section 8.2, as well as the case analysis in Section 8.3.1, and the ISM standards document, suggest certain *direct* support for the model of *Internet security policy content* (Table 4.1) and the model of an IAUP (Table 4.3). I further queried AUR as to their view of the actual models for these two policies, and received general agreement with my models.

Direct support provided by this case study for policy content for these two models, i.e. support provided by the empirical data, is indicated by bullets in the columns labelled “Supported” in Tables 8.2 and 8.3. Evidence for the direct support has been provided in Sections 8.2 and 8.3.1

Internet security policy content	Supported
Purpose and scope of policy	•
Philosophy of policy	•
Internet security infrastructure	•
Internet security management programme	•
Other applicable policies	•
Internet privacy policy	•
Internet censorship policy	•
Internet accountability policy	•
Internet information protection policy	•
Internet information access policy	•
Internet firewall policy	•
Internet security technology policy	•
Password policy	•
Internet acceptable usage policy	•
Internet publication policy	•
Email policy	•
Internet virus policy	•
Internet audit policy	•
Internet incident policy	•
Internet legal policy	•
Internet security policy review policy	•

Table 8.2 Internet security policy content support at AUR

Internet acceptable use policy content	Supported
purpose and scope of policy	•
ethics policy	•
Internet services policy	•
confidentiality policy	•
acceptable uses	•
unacceptable uses	•
Internet risks	•
legal policy	•
roles and responsibilities	•
privacy	•
accountability	•
monitoring and surveillance	•
sanctions	•
awareness	•
user consent	•

Table 8.3 Internet acceptable use policy content support at AUR

I remark here that I did not attempt to analyse support for the model of firewall policy (Table 4.2). AUR's current firewall policy only existed, like Flyway's, in network router protocol language form.

8.3.3 Support for framework for development of Internet security policy

AUR believed that my approach for developing an Internet security policy, as portrayed in Figure 4-1, is sound. They approved of the holistic nature of the approach, with many diverse aspects being taken into account via the guidance provided by the Factors model (Figure 3-3).

They remarked that the corporate information security policy (in this case, their ISM Standards document) should be a high-level policy, and that specific, lower-level policies should then be developed in accordance with this existing policy. The Internet security policy would be one of these lower level policies. Their approach at the time of study was to perceive a new Internet risk and then carry out a risk assessment for that particular risk, conceiving policies and technological controls to control it as a result of the assessment. For example, a recent assessment of newly perceived JAVA and ACTIVE-X related risks had led to a policy proposal to block ACTIVE-X and JAVA sites from entering AUR.

AUR conceded that this approach may well work once an Internet security policy is in place, but for the initial policy development, an all-out approach starting with the Internet risks model, as suggested in the framework in Figure 4-1, may work.

8.4 Conclusion

I commence this section by summarising the research models supported by the case study results, then draw conclusions for this research project, and make some final comments.

8.4.1 Summary of models supported by case study

I obtained support from this case study, as described in detail in the previous section, for the following aspects of the overall framework for Internet security policy:

- factors in Internet security policy (Figure 3-3)
- societal issues in Internet security policy (Section 3.4.2)
- Internet risks for Internet security policy (Figure 3-5)
- organisational issues in Internet security policy (Table 3.2)
- administrative issues in Internet security policy (Section 3.4.5)
- legal issues in Internet security policy (Section 3.4.6)
- technical issues in Internet security policy (Section 3.4.7)
- human issues in Internet security policy (Table 3.3)
- Internet security policy content (Table 4.1)
- IAUP content (Table 4.3)
- framework for development of Internet security policy (Figure 4-1)
- overall framework for Internet security policy (Figure 4-2)

8.4.2 Case study conclusions

In this section, I highlight the existence of an Internet security problem at AUR, then discuss the implications of this study for the project, in terms of the project research questions.

Clearly, AUR had an Internet security problem, with a number of Internet risks rated as either high or medium—in particular, non-business usage. The risks were not being effectively controlled by existing policies, procedures or other existing measures.

Below, I examine how this study has addressed the three research questions:

1. What are the factors influencing effective Internet security policy for an organisation?

This investigation identified a number of factors to be addressed by an effective Internet security policy, as summarised below.

As described in Section 8.4.1.1, the case study exposed three significant Internet risks—*non-business usage, corrupted or erroneous software, and accidental disclosure.* Other Internet risks were acknowledged as existing, albeit at low levels. AUR agreed that *all* risks depicted in the Internet risks model (Figure 3-5) required addressing in a future policy, thereby supporting the Internet risks model (Figure 3-5) and the Factors model (Figure 3-3), and helping answer the research question listed above.

As described in Section 8.4.1.2, the case study highlighted the need for organisational issues to be addressed in a future Internet security policy. All organisational issues listed in the proposed model (Table 3.2) were identified as possible influences on policy at AUR, thereby supporting the organisational model as well as the Factors model (Figure 3-3), and contributing to answering the research question listed above.

As described in Sections 8.4.1.3, 8.4.1.4, 8.4.1.5 and 8.4.1.6, there were administative, legal, societal and technical factors at AUR which would influence the policy. It was also clear that human issues were a significant consideration in all factors.

The Factors model (Figure 3-3) lists all the types of factors identified at AUR: Internet risks, organisational, administrative, legal, societal, technical and human issues. Hence, this case study has helped answer the research question by identifying the factors which would influence Internet security policy at AUR, then matching those factors against the Factors model.

2. Is an holistic approach to an Internet security policy more effective than the piecemeal approach adopted to date?

AUR raised many diverse, interacting and conflicting policy issues in this study, suggesting that an holistic approach is required for an effective Internet security policy.

3. Can a framework be specified for the development, issues and content in effective Internet security policy for organisations?

The proposed framework (Figure 4-2) was supported by this case study, as follows: Firstly, the Factors model component (Figure 3-3) of the framework was supported, as discussed in answering Research Question 1 above. Secondly, a risk assessment process would identify certain risks as more significant and worthy of paying attention to improved control, than other risks, and is therefore an appropriate process for developing the policy, as shown in the framework. Thirdly, substantial evidence was provided

in Section 8.4.3 of support for the three proposed Content model components of the framework (Table 4.1, Table 4.3 and Table 4.4).

Hence, this study has provided support for the proposed framework, and has contributed to answering this research question in the affirmative.

8.4.3 Final remarks

As a result of this case study, AUR was reviewing its Internet security measures, managerial, procedural and technical, in order to more effectively address the problems identified. In particular, AUR was keen to reduce the risk of non-business Internet usage, which was running at the time at 50%.

AUR recognised the need for an organisastional Internet security infrastructure to manage all the measures required, and within this, the need for a comprehensive Internet security policy which would include, as a sub-policy, an IAUP.

AUR planned, with time and additional resources, to develop the new infrastructure and policies.

As I elected to do for the previous case study, in the interests of keeping this thesis to a manageable size, I reserve further conclusions for a later stage of the thesis. In the next Chapter, I describe the fourth and final case study of USEnergy Petroleum, a large American oil company. I remind the reader that, chronologically, a focus group followed the AUR case study, for theory validation purposes. Due to the ten month hiatus which occurred between the focus group in June, 1998, and the resumption of the research project in April, 1999, however, I actually conducted the USEnergy case study described in the next Chapter, *after* the focus group, in May 1999, in order to test the continuing relevance of the results of the three detailed cases conducted earlier (ie, the three cases which I have described in the previous three Chapters).

Chapter 9

Case Study: USEnergy Petroleum Company

"*It is very beautiful over there."*

(last words, Thomas Alva Edison, inventor)

In previous Chapters, I developed and described a framework for Internet security policy for organisations, then explored the research topic via two mini case studies and three detailed case studies, in the process obtaining useful results for the research project, as well as support for selected components of the framework.

Because I was concerned about the period of ten months which elapsed between the last collection of research data (a focus group—reported in Chapter 11—was conducted in June, 1998) and the resumption of the research project in April, 1999, I conducted an additional detailed case study in May, 1999, described in this Chapter, to test whether the research results obtained earlier were still relevant. Due to the limited interviewing time available (a single visit with a two hour interview while travelling overseas), I was unable to investigate UP as extensively as the earlier detailed case studies (notably, I did not get the opportunity to query UP about their opinion of the student views regarding human issues, obtained in mini case B). I did, however, obtain the necessary confirmation of the continuing validity of my earlier research findings.

In this Chapter, I present this case study, conducted at USEnergy Petroleum Company—a large, leading American petroleum organisation—in May, 1999. This case, as for the three detailed case studies in Chapters 6, 7 and 8, focuses on the employer perspective of the topic. I commence by introducing USEnergy Petroleum Company (henceforth referred to as UP) and outlining case procedures. I then provide background to the Internet infrastructure and usage at UP. Finally, I present the case study analysis and results, and draw conclusions for the research project.

9.1 Introduction to USEnergy Petroleum and the case study procedures

For reasons of anonymity, I present only a very limited introduction to UP. UP is one of America's largest petroleum companies. It conducts oil and natural gas exploration, and produces and markets petroleum products and chemicals from these resources. UP competes with major global petroleum companies, national oil companies and independent exploration and production companies—as well as being involved in many projects in countries around the world.

9.1.1 Sampling procedure

I selected UP to study, as it was an example of a large American company in the Energy (Petroleum-Diversified) industry sector, and I had established contacts who were employed there. Furthermore, I thought it would be interesting to study a non-Australian company, to test whether my framework might be useful outside Australia.

9.1.2 Data collection, case instrument and case conduct

I visited UP in May, 1999, and spent two hours collecting data via one semi-structured interview, employing:

(ix) a collated document consisting of the various models composing the framework in Figure 4-2; and

(x) a set of guideline questions which constantly referred to the collated document to structure and guide the interviews.

I collected three documents from UP: Intranet Guidelines, E-mail policy and Internet Usage Guidelines.

I conducted the interview with the Manager of Network Services and the Manager of Information Security Services.

The questions I asked of the interview participants, in order to structure the interview, were designed:

(h) to provide background information about their company, Internet usage, Internet architecture and Internet access controls;

(i) to perform a qualitative risk analysis of their Internet risks, using the Internet risks model (Figure 3-5) as a guide, in order to determine the significance of each identified Internet risk, and to gauge support for the model;

(j) to comment on the Factors for Internet security policy model (Figure 3-3) in the context of UP, and to gauge support for the model;

(k) to provide information about their existing approach to developing Internet security policy;

(l) to comment on the Internet security policy development model (Figure 4-1); and to comment on the Internet security policy content model (Table 4.1), the IAUP content model (Table 4.3) and the email policy content model (Table 4.4) as these models related to UP's situation.

I recruited the company by telephone from Australia, and faxed an explanatory document describing the research project to the main contact for perusal, prior to the contact formally agreeing to the study. I arranged the interview time by phone, after initial agreement had been obtained.

The interview took place at the company's corporate headquarters. The main contact signed a research consent form at the initial interview. I distributed copies of the collated document of proposed models to those present, and followed the set of questions listed earlier to obtain the data required. I took notes during the interview.

9.1.3 Data analysis

I later analysed the data collected by comparing and contrasting the collected data with the component models of the proposed framework, identifying similarities, differences and patterns. A draft copy of the resulting case study analysis was forwarded to UP for correction, and for addition of missing information.

9.2 Internet infrastructure and usage

9.2.1 Internet security as a "vertical slice" of information security

UP lacked a formal Internet security infrastructure, although it recognized the need for one, with increased use of the Internet being planned.

Information Security Services administered and managed information security at UP. UP viewed Internet security as a vertical slice through information security (as did Flyway and AUR). Internet planning and strategy were driven by UP's Marketing arm. A variety of policies supported Internet security management (see Section 9.2.5), although none of these corresponded to an Internet security policy.

It is noteworthy that UP involved itself in Internet security issues in the broader community. For example, UP was a member of a group which described an approach for a company to achieve a balance between the level of Internet security, and performance.

9.2.2 Internet usage

The Internet was initially deployed at UP in the early nineties, with all employees being provided with access to it for email purposes. Several thousand employees were using Web browsers (email was run via a client, rather than through these browsers) at their PC workstations, which were Pentium class or better.

Approval of requests for all non-email Internet usage was based on manager approval and business justification, with the relevant business unit being charged running costs.

At the time, an Intranet was deployed for document sharing, group communication, research project databases and information sharing. For example, an Intranet database project gave users fast access to the status of their oil-exploration projects. Another Intranet application employed devices for measurement

and control (such as pump stations along pipelines or throughout the refineries) to publish real-time changes to operational managers and an executive information system at head office, to support real-time accounting and tactical decisions.

The Internet was used for EDI transaction processing, business email, informing the public via the Web, and the issuing and updating of personal credit cards via the company's Web site. A certain amount of non-business email was both expected and tolerated, with employees being instructed to limit personal email to necessities.

9.2.3 Internet architecture

Figure 9-1 illustrates the Internet architecture at UP.

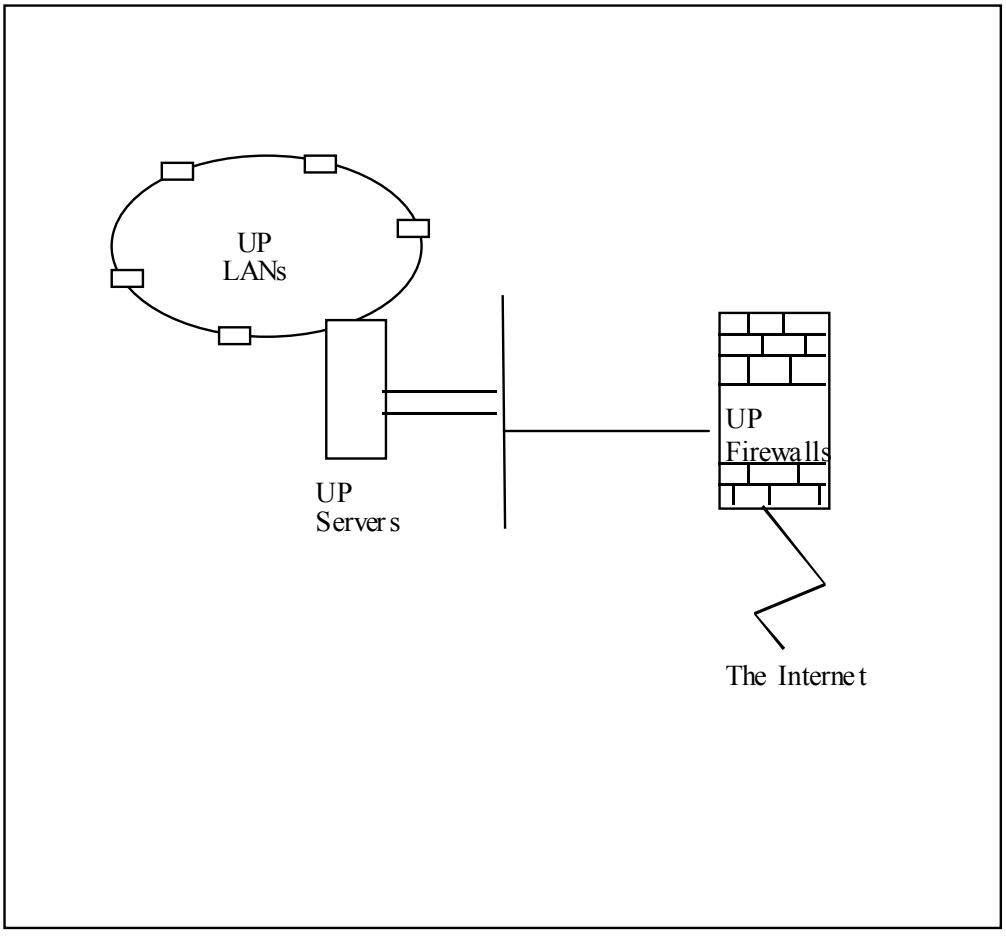

Figure 9-1 Internet architecture at each UP site

UP had several Internet gateways, some inside the US and some outside. Employee workstations were mainly Pentiums, connected internally at each geographic location via LANs. The LANs in each location

were connected to several servers and firewalls in each location, forming a WAN. Firewalls connected to the Internet via direct lines. There were long distance links between major UP locations.

There were several mainframes (running corporate systems) connected to the LANs, however the company considered it technologically highly unlikely that these mainframes could be accessed from outside the company (as if the firewalls did not prevent access, there were still many other technical hurdles to be overcome to gain access).

9.2.4 Internet access control

9.2.4.1 Internet access policy at UP

UP believed that employee Internet access should be granted according to the importance of the business need. Internet access control was handled by an access policy implemented by server and firewalls.

Employees with browser facilities connected to the server, which consulted an access control list of user login ids and passwords in order to grant Internet access. Ftp was permitted by authorized users, although telnet was prohibited universally. Users were charged per month for Internet access, with a corresponding chargeback to the user's business unit for each user connection.

9.2.4.2 Firewall filtering, logging and monitoring at UP

UP's head office server connected to a firewall, which logged, monitored and filtered incoming traffic, and logged all web accesses and emails to the outside. There were insufficient human resources to monitor the log effectively, rendering the monitoring policy ineffective. Surveillance by managers walking around and observing workstation screens served as a level of control.

Employees were aware that their web accesses and emails were being logged, and that the firewall log was being monitored, but recognized that action was not being taken on breach of policy, reducing the effectiveness of the monitoring still further. Employees were informed via the Internet Use guidelines of the rules for Internet use, as well as via occasional email reminders.

9.2.5 Information security policies

Several policy documents informed employees of their information security responsibilities and restrictions.

These policies were:

UP Code of Conduct, IT Security Policy, UP Web design guidelines, Intranet guidelines, E-mail policy, Internet usage guidelines, and Internet access policy.

The various policies were updated sporadically, for example the existing email policy had been developed in January, 1996, some three years prior to the study. UP mentioned that their information security policy (IT Security Policy) urgently needed a review, as it did not cater adequately for Internet technology use.

9.2.6 Internet training and awareness

Classes were regularly held in Internet basics and Web page development. However there were no Internet security awareness sessions to explain issues and policies to employees.

9.2.7 Future Internet security infrastructure and policy

UP lacked an Internet security infastructure, although they recognised the need for one, agreeing that this should be centred on an Internet security policy.

There were no plans for such an infrastructure or policy yet, due to a lack of attention to the area and issues to date.

9.3 Case analysis

In this section, I analyse the data collected, by pattern-matching the data with various aspects of the proposed framework (Figure 4-2). The specific aspects explored are:

- factors in Internet security policy (Figure 3-3)
- societal issues in Internet security policy (Section 3.4.2)
- Internet risks for Internet security (Figure 3-5)
- organisational issues in Internet security policy (Table 3.2)
- administrative issues in Internet security policy (Section 3.4.5)
- legal issues in Internet security policy (Section 3.4.6)
- technical issues in Internet security policy (Section 3.4.7)
- human issues in Internet security (Table 3.4)
- Internet security policy content (Table 4.1)
- IAUP content (Table 4.3)
- email policy content (Table 4.4)
- framework for development of Internet security policy (Figure 4-1)
- overall framework for Internet security policy (Figure 4-2)

I first analyse the various factors in Internet security policy at UP (Section 9.3.1), then analyse the support provided by this analysis for the factors model and its component models (Section 9.3.2). Next, I analyse UP's requirements for Internet security policy content, and determine the support provided for the corresponding content models (Section 9.3.3). I then analyse UP's requirements for the development of Internet security policy and the support provided for the corresponding framework for development (Section 9.3.4).

9.3.1 Analysis of factors in Internet security policy

In this section, I investigate each type of factor in the model in Figure 3-3: *Internet risks, organisational issues, administrative issues, legal issues, societal issues, technical issues and human issues.*

9.3.1.1 Internet risks at UP

UP informally analysed their Internet risks, using the Internet risks model in Figure 3-5 as a guide to assist in identifying existing risks, and assigning each identified risk type a rating of low, medium or high, based on the professional opinion of the two information security managers interviewed, including their opinion-based, qualitative estimates of *frequency of risk occurrence* and *impact*. The results are summarised in Table 9.1 in order of most significant to least significant risk, and the analysis of each risk type is discussed below.

Internet Risks	Risk Rating L, M, H
Non-business usage	H
Hacking	H
Corrupted or erroneous software	H
Inaccurate advertising	M
Low quality data	L
Accidental erroneous business transactions	L
Inappropriate email	L
Pirated media	L
Accidental disclosure	L
Fraud	L
Denial-of-service	L
Theft of information	L

Legend: L = Low; M = Medium; H = High.

Table 9.1 Internet risks at UP

(i) Non-business usage

UP had hoped that the policies in place would control non-business usage. For example, the E-Mail policy stated:

Incidental use for purposes other than business should be limited to necessities

In addition to this policy, there was also logging and monitoring of web accesses, and policy informing employees of these. However, there had been insufficient resources for implementing monitoring (that is, for checking the firewall logs), and hence this control was ineffective.

UP estimated that some 80% of its Internet usage was for personal purposes.

Personal surfing and personal email were widespread, leading to loss of productivity and the slowing down of Internet use for valid business purposes. Furthermore, UP paid a fixed subscription amount to an ISP for a given amount of Internet usage per month; any extra use cost UP more, and advice to employees accordingly was to 'use the Internet connection somewhat conservatively'.
UP was understandably concerned about the high rate of non-business usage, rating the risk as *high*.

UP was perplexed about this problem, taking the view that Internet personal use was an employee benefit (in accordance with the focus group's viewpoint). Therefore, UP was reluctant to remove employee Internet privileges. Furthermore, there was unlikely to be an increase in resources for monitoring purposes, in the near future. UP pondered such options as limiting the size of an email message including attached files, as well as charging business units extra for excessive employee Internet time—as possible new measures to control the problem.

(ii) Hacking

In 1994, UP's systems were attacked via the net (the attack failed), and *firewalls* were promptly deployed to prevent intrusion. Employees needing access from outside used a one-time authentication password. The Internet usage guidelines warned employees about the existence of "rogue users" and "crackers" outside the company, who might try and hack into the company systems.

No hacking attempts into other companies by UP employees had been noted, although UP admitted that they did not check their firewall logs often, and may therefore have missed such attempts. Nonetheless,

hacking (by employees) was specifically prohibited in the IT Security policy, and cautioned against in the Internet usage guidelines.

UP rated the risk of 'hacking' (into the company) as *high*, due to the corporate sensitivity of the organisation's data.

(iii) Accidental erroneous business transactions

There had been several cases at UP of sensitive email being misdirected.

The Internet usage guidelines cautioned employees regarding the common mistake of accidentally sending an email reply to all recipients of an initial email, rather than directing it solely to the individual for whom the reply was intended. However, there was no cautionary message regarding checking despatch addresses prior to sending, in any policy.

Although the likelihood of such incidents remained high, there had not as yet been any major repercussions from misdirected email. UP accordingly rated the risk of 'accidental erroneous business transactions' as *low*.

(iv) Corrupted or erroneous software

The Melissa virus entered and infected UP in April, 1999. This caused UP some concern, and UP's employees were warned about viruses in general in the Internet Usage guidelines as well as in the IT Security policy. Desktop virus scanners were also available for employees, although these were not updated frequently enough to protect against all incoming viruses. UP expressed concern at the amount of damage a virus could cause, and hence rated the risk of 'corrupted or erroneous software' as *high*.

(v) Low quality data

UP mentioned that their employees relied on confirmed data sources for information, and hence were not susceptible to low quality data residing on the web. As far as any UP web site's quality was concerned, the Intranet guidelines stipulated that:

Employee sites must adhere to the UP Web Design Guidelines.

Nevertheless, UP took care to divest itself of responsibility for the data listed on some sites. For example, UP had a statement on one of its division's sites, advising that UP did not assume liability or responsibility for the accuracy, completeness, or usefulness of the information disclosed at or accessed through the site.

Note: UP's E-mail policy cautioned employees in several sub-policies against inappropriate email use, covering not only the risks of junk email and email harassment in (vii) below, but also the risk of *invalid data* occurring in email—a risk which I have included in the 'low quality data' risk. Overall, UP rated the risk of 'low quality data' as *low*.

(vi) Inaccurate advertising

This refers to the company or its employees consciously 'advertising' within email, Web sites, or other posting mechanisms, without due authority, *in such a way as to appear to represent an official view.* The content of this information may be inaccurate, in an organisational context.

The UP E-mail policy stated that messages which disclosed sensitive or confidential information must be authorized. Disclaimers were not a requirement at UP, although the Internet usage guidelines recommended the use of a disclaimer unless specifically representing an official transaction. The guidelines also prohibited contractual agreements by email, unless the entire email was dedicated to that purpose.

The Intranet guidelines stated that business unit managers were required to approve employee web site content prior to release, providing a level of content verification.

Monitoring of email content, although an official policy, was not implemented, due to the lack of human resources to carry this out. UP believed that some emails were in fact being sent out containing inaccurate corporate information or views, but that the emails in question were not being detected.

Hence, UP rated this risk as *medium*.

(vii) Inappropriate email

This risk refers to companies sending or receiving unwanted or unsolicited email (*junk email*), harassing, discriminatory or defamatory email (*flame email*) or excessive unwanted email (*spamming*).

This was recognized as a problem. For example, recently one employee had been dismissed for downloading pornographic pictures, and a contractor had been fired for spamming.

The E-mail policy prohibited defamatory, obscene, offensive and harassing messages. The Internet usage guidelines cautioned against being abrupt, rude or misleading.

However, the E-mail policy did not warn of excessive or junk email, and UP had indeed experienced problems in this area.

Nevertheless, compared with the severity of some of the other risks, UP rated the risk of 'inappropriate email' as *low*.

(viii) Pirated media

It was unlikely that piracy was occurring at UP, as the company was well resourced for software. If employees required software to carry out their job tasks, it was usually purchased for them, or freeware was downloaded. It was considered politically unwise for UP to check individual workstations for possible pirated software residing there. Software piracy via the Internet may have been occurring at UP, but its extent was unknown.

UP specifically deterred software piracy in its IT Security Policy and E-mail policies, thereby assigning responsibility for compliance with licensing conditions to employees.

Due to the unknown incidence of piracy, UP rated the risk of 'pirated media' as *low*.

(ix) Accidental disclosure

The E-mail policy has many sub-policies which protect against this risk, for example it states:

Messages received should be forwarded ONLY to parties with a definite "need to know" and ONLY when there is no question of confidentiality

and

also prohibited are messages that disclose sensitive or confidential information without authorization.

The Internet usage guidelines cautioned that email could be forwarded or distributed by an email recipient to other parties, without the original author's knowledge.

UP has employed Pretty Good Privacy (PGP) encryption software for several years. Although email was, by default, not encrypted, employees were instructed in the Internet usage guidelines to encrypt confidential emails prior to transmission.

UP also recommended the immediate deletion of email once it no longer required action. Email administrators were asked (in the E-mail policy) to delete email after a fixed period, according to email retention rules prescribed in the policy.

At the time of study UP considered the risk unlikely, and the sensitivity of data likely to be communicated as low. Hence they rated this risk as *low*.

(x) Fraud

Internet fraud had not occurred to date. Electronic transactions were not being conducted via the Internet, so there was not a great deal of concern about this issue. However, UP did issue credit cards via the Internet, and hence had some responsibility for protecting the personal financial data of credit cardholders.

With a lack of fraud incidence to date, UP rated the risk as *low*.

(xi) Denial-of-service

The firewalls were regarded as good protection from attacks which could lead to denial-of-service. UP rated the risk of 'denial-of-service' as *low*.

(xii) Theft of information

The E-mail policy warned employees not to copy and/or transmit documents, software or other information protected by copyright.

With no detected incidence of this risk to date, UP rated the risk as *low*.

(xiii) Summary of Internet risks and their management

Clearly there were significant Internet risks occurring at UP. UP ranked: *non-business usage, hacking, and corrupted or erroneous software* as their major Internet risks. The diverse set of policies existing at UP did not treat each risk separately, and it was difficult to locate recommended policy for a given risk.

Possibly due to the scattered treatment of risks in the various policies, there was much uncertainty at UP as to how well each risk was being managed at the time.

UP agreed that it would be useful to have a specific sub-policy within an Internet security policy, for each of the risk types in the Internet risks model (Figure 3-5), informing employees of the specific risks for that risk type, and company policy regarding that risk type, including possible losses, remedies and sanctions.

The risk analysis results presented above have provided support for the Internet risks model for Internet security policy (Figure 3-5).

9.3.1.2 Organisational issues in Internet security policy

Table 3.2 suggested the following broad categories of organisational factors which influence Internet security policy: organisational objectives, Internet security infrastructure, management commitment, Internet security management programme, Internet security awareness, policy integration, and principles for Internet security and policy. I discuss each of these below.

(i) Organisational objectives:

UP employees were given some advice in various policies regarding the requirement for business usage only, however there was a lack of explanation of valid usage as well as an absence of Internet awareness sessions, to support that requirement.

UP agreed that in an Internet security policy, it would be advisable to give employees guidance to valid Internet business usage, that is, usage which supported organisational objectives.

(ii) Internet security infrastructure:

I mentioned earlier the absence of a formal Internet security infrastructure at UP, and although UP had not yet planned such an infrastucture, they agreed with the concept, and that an Internet security policy should form the cornerstone of such an infrastructure.

(iii) Management commitment:

UP believed this would make a difference to the success of an Internet security policy, although they were uncertain as to how such a commitment could be secured. There was sporadic commitment from higher up the organisation at the time.

(iv) Internet security management programme:

The lack of a formal, cohesive programme of policies, procedures, training and awareness activities, was reflected in the 80% non-business use as well as the infiltration by the Melissa virus in 1999. Internet training sessions were both voluntary and ad hoc, and security awareness sessions were not held. A formal programme would adopt a proactive stance, and produce a business case for additional resources for training, awareness, effective monitoring and other security duties.

UP agreed with the concept of such a programme, and that its components should be documented in the Internet security policy.

(v) Internet security awareness:

UP conducted Internet training courses but not Internet security awareness sessions. They recognized that mandatory training and awareness sessions for all Internet-connected employees would improve the success of implementation of Internet policies, and that policy for the awareness activities should be specified in the Internet security policy.

(vi) Policy integration:

There was a notable lack of integration of the various policies and sets of guidelines dealing with Internet use and security. This may have been contributing to the existing levels of Internet risks, as it would have been confusing trying to identify a consistent policy for a particular issue, from the existing set of policy and guideline documents.

UP agreed that all Internet-relevant policies should be integrated and consistent.

(vii) Principles for Internet security and Internet security policy:

UP recognised the need for enforceability and other principles for a new Internet security policy.

9.3.1.3 Administrative factors in Internet security policy

Some Internet security procedures were certainly applied at UP—for example, purchasing and installing relevant anti-virus programs, and use of independent auditors for auditing UP systems, including the Internet. While various procedures were documented in different places, there were no references to these in any of the policy documents.

UP agreed that an Internet security policy should document or reference Internet security procedures.

9.3.1.4 Legal factors in Internet security policy

UP lacked adequate reference to legal issues in their various Internet-relevant policies and guidelines.

UP was aware of the need for coverage of relevant legal issues in an Internet security policy.

9.3.1.5 Societal factors in Internet security policy

UP referred to various unethical Internet practices, such as sending rude jokes and file images into and out of the company. One employee had been fired for downloading a pornographic image.

Although there were several policy warnings against such practices, these were not managing the problem, possibly due to lack of enforcement of policies via effective monitoring and sanctions.

9.3.1.6 Technical factors in Internet security policy

UP agreed that their Internet risks could be reduced by new security technologies. For example, an email client with a standard disclaimer could be employed.

UP agreed that policies for such technologies should be part of the Internet security policy.

9.3.1.7 Human issues in Internet security policy

Human issues listed in the human issues model (Table 3.4) were: *freedom of Internet use, privacy, censorship, right to be kept informed, accountability, ownership and ethics*.

As mentioned at the beginning of this Chapter, I did not have the opportunity, due to time constraints, in this particular study, to investigate UP's views of student opinions regarding human issues, as reported earlier in this thesis in mini case B. Instead, I queried UP for their opinions as to whether and how human issues would influence Internet security policy.

(i) Freedom of Internet use

There was a significant problem with UP employees using the Internet for personal reasons some 80% of the time (see Section 9.3.1.1). UP referred to a lack of resources for policing Internet use as a major factor in this Internet misuse. There were uncertainties in deciding the appropriate degree of freedom of Internet use for employees, further complicating the issue.

UP did not believe that official policy should state "no personal Internet use whatsoever". Rather, they believed a limited amount of personal Internet use should be tolerated, as an employee benefit of working at USEnergy.

They further believed that employees' business unit managers should be responsible ultimately for policy enforcement, through chargeback costs to them of their employees' Internet use.

UP agreed that "freedom of Internet use" would be a significant issue for an Internet security policy.

(ii) Privacy

At the time, UP lacked a privacy statement on its Web site, demonstrating a lack of adequate awareness of this issue. As credit cards were issued via the Internet, UP acknowledged the need to inform potential credit cardholders of their data privacy rights, and agreed that these rights should be documented in an Internet security policy.

Regarding employee privacy issues, UP logged employee Internet accesses, believing that employees should be held accountable for their Internet actions at work (although at the time such accountability was not being enforced due to lack of human resources to check the logs).

Regarding employee Web accesses, UP believed that only business-related data should be collected from such visits by Web site owners. UP agreed that employees should be advised to check for Privacy statements and conditions when accessing external web sites.

UP agreed that "privacy" issues would certainly influence Internet security policy.

(iii) Censorship

UP did not believe in the right to actively censor either employee access to Web sites or employee emails via firewall filtering (a form of censoring), but did believe in logging and monitoring emails and Web accesses (also a form of censoring), although, as has been stated, the implementation of this monitoring was ineffective, due to insufficient human resources to check the logs.

UP agreed that "censorship" issues would influence Internet security policy.

(iv) Right to be kept informed

UP recognized that some of its problems may stem from a lack of employee awareness of the company policies and the issues involved. UP agreed that an ideal Internet security infrastructure would feature a range of Internet security awareness activities, and acknowledged that inadequate awareness had contributed to the unsatisfactory levels of several Internet risks (for example, the 1999 Melissa virus may have been avoided, with employee awareness of the dangers of downloading unknown email attachments and running them).

UP agreed that employees had the right to be kept informed via policies and awareness activities, of Internet security issues.

(v) Accountability

UP believed that employee accountability for Internet use was crucial.

Various measures to ensure employee accountability for Internet use were employed. The major measure implemented by UP was the logging and monitoring of web accesses, and the policy of monitoring employee email. Other policies contributed towards accountability, for example the requirement for complete employee signatures at the end of each email, stipulated in the Email policy.

However, UP believed it was very difficult to hold employees accountable for their Internet use, despite logging their accesses, given the inadequate monitoring resources. Nevertheless, UP intended to continue with monitoring, step up awareness of that monitoring, and seek additional resources for policy enforcement. At the time, employee signed consent was not sought for Internet conditions-of-use agreement, although this was being considered as a new measure. UP planned to devise additional measures by which accountability could be achieved, then advise of this via policy.

(vi) Ownership

UP had the ownership-of-web-site content issue well covered in its diverse policies, and agreed that the issue should be treated in an Internet security policy.

(vii) Ethics

UP were keen to promote an "Internet rights and responsibilities" attitude in their employees, by promoting an atmosphere of trust and care, although at the time there appeared to be more rights than responsibilities in some areas (notably, 80% of Internet usage was non-business).

9.3.2 Analysis of support for the Factors model

UP approved the model of influential factors in Internet security policy (Figure 3-3).

This case study provided additional empirical support for the Factors model (Figure 3-3) and its various components (*Internet risks, organisational issues, administrative factors, legal factors, societal factors, technical factors and human issues*) as follows.

This case study supported the inclusion of *Internet risks* in the Factors model in the discussion in Section 9.3.1.1, in that a number of Internet risks were not being adequately managed by the current set of policies. The study also supported the model of Internet risks shown in Figure 3-5, as discussed in Section 9.3.1.1, in that UP acknowledged that all the risks shown in the model were present, to varying degrees of significance, within their company.

The case study supported the inclusion of *organisational issues* in the Factors model, in the discussion in Section 9.3.1.2, in which I investigated each of the issues in the proposed organisational issues model (Table 3.2). I found that:

- employees were not adequately informed of acceptable Internet business uses (*organisational objectives* issue);
- there was a need for documenting future Internet infrastructure in the policy (*Internet security infrastructure* issue);
- there was agreement that management commitment would improve the chances of policy success (*management commitment* issue); and
- there was a need for an Internet security management programme to support the policy, and this programme should be documented within the policy (*Internet security management programme* issue);
- there was a need for policy integration, with related policies being referenced within the Internet security policy (*policy integration* issue);

- the policy needed to include policy on Internet security awareness activities (*Internet security awareness* issue); and
- the policy needed to meet predetermined principles (for example, enforceability) (*principles* issue).

The case study supported the inclusion of *administrative issues* in the Factors model in the discussion in Section 9.3.1.3, in that various Internet security procedures were either not documented anywhere, or not easily accessible.

The case study supported the inclusion of *legal factors* in the Factors model in the discussion in Section 9.3.1.4, in that UP recognized the importance of those in such a policy.

The case study supported the inclusion of *societal issues* in the Factors model in the discussion in Section 9.3.1.5, in that UP recognised the need for ethical guidance in Internet use, as part of an Internet security policy.

The case study supported the inclusion of *technical issues* in the Factors model in the discussion in Section 9.3.1.6, in that the requirements for new technologies which could assist in reducing risks should be specified in the Internet security policy.

The case study supported the inclusion of *human issues* in the Factors model in the discussion in Section 9.3.1.7, in that each of the issues in Table 3.4 (freedom of Internet use, privacy, censorship, right to be kept informed, accountability, ownership and ethics) were shown to be significant, and, in many cases controversial, issues to resolve in order to assure the effectiveness of the developed Internet security policy. The study also loaned support for the model of human issues (Table 3.4) through highlighting the impact of each issue in the table, on policy.

9.3.3 Analysis of support for Content models

In this section, I discuss the support provided by this case study for three of the content models. The background discussions in Section 9.2, the case analysis in Section 9.3.1, as well as the content of UP's existing set of policies and guidelines, suggest *direct* support for the model of *Internet security policy content* (Table 4.1), the model of *IAUP content* (Table 4.3) and the model of *email policy content* (Table 4.4). This support is summarised in Tables 9.2, 9.3 and 9.4, which include references to the sections in this Chapter indicating support.

Finally, I queried UP on their view of the proposed content models for these policies, and received overall approval.

Internet security policy content	Sections providing support
Purpose and scope of policy	9.3.1.2
Philosophy of policy	9.2.4
Internet security infrastructure	9.3.1.2
Internet security management programme	9.3.1.2
Other applicable policies	9.3
Internet privacy policy	9.3.1.7
Internet censorship policy	9.3.1.7
Internet accountability policy	9.3.1.7
Internet information protection policy	9.3.1.1, 9.2.4
Internet information access policy	9.3.1.1, 9.2.4
Internet firewall policy	9.3.1.1, 9.2.4.2
Internet security technology policy	9.3.1.6
Password policy	9.3.1.1, 9.2.4
Internet acceptable usage policy	9.3
Internet publication policy	9.3.1.1
Email policy	9.3
Internet virus policy	9.3.1.1
Internet audit policy	9.3.1.3
Internet incident policy	9.3.1.1
Internet legal policy	9.3.1.4
Internet security policy review policy	9.3

Table 9.2 Internet security policy content support at UP

The first column of Table 9.2 lists the policy components suggested in the Internet security policy model (Table 4.1), while the second column lists the sections in this Chapter indicating support for the components.

Internet acceptable use policy content	Sections providing support
purpose and scope of policy	9.3.1.2
ethics policy	9.3.1.5, 9.3.1.7
Internet services policy	9.2
confidentiality policy	9.3.1.1
acceptable uses	9.3
unacceptable uses	9.3
Internet risks	9.3.1.1
legal policy	9.3.1.4
roles and responsibilities	9.3
privacy	9.3.1.7
accountability	9.3.1.7
monitoring and surveillance	9.2, 9.3.1.7
sanctions	9.3.1.7
awareness	9.3.1.2, 9.3.1.7
user consent	9.3.1.7

Table 9.3 Internet acceptable use policy content support at UP

The first column of Table 9.3 lists the policy components in the IAUP model (Table 4.3), while the second column lists the sections in this Chapter which indicate support for the components.

Email policy content	Policy support	Sections providing support
email ownership	•	9.3.1.7
acceptable email usage	•	9.3.1.1
email privacy	•	9.3.1.1, 9.3.1.7
email encryption	•	9.3.1.1
email monitoring	•	9.2.4.2, 9.3.1.7
email netiquette	•	9.3.1.7
emotional email	•	9.3.1.1
avoidance of references to third parties		
duties to third parties (eg auditors)		
external interception of email		
email deletion after usage	•	9.3.1.1
distribution of email copies	•	9.3.1.1
copyright implications of copy distribution	•	9.3.1.1
legal issues	•	9.3.1.4
email virus protection	•	9.3.1.1
enforcement and dissemination of email policy	•	9.3.1.2
signature policy	•	9.3.1.7

Table 9.4 Email policy content support at UP

In the first column, I list the components of the email policy model (Table 4.4). In the second column, I denote by a bullet those components supported by UP's email policy and/or other Internet-related policies. In the third column, I list the sections which provide case study support for each component.

Note that I have added a new sub-policy—signature policy—to my model for email policy content, after discovering such a sub-policy in the UP Email policy (see Section 9.3.1.7).

Note that I did not attempt to determine support at UP for my proposed model for firewall policy (Table 4.2), due to interview time constraints.

9.3.4 Support for framework for development of Internet security policy

UP approved of the approach for developing an Internet security policy, as portrayed in Figure 4-1. *In particular, they liked the risk assessment process shown in the framework, and the holistic nature of the framework.*

9.4 Conclusion

I commence this section by summarising the research models supported by the case study results. I then draw conclusions for this research project, and make final comments.

9.4.1 Summary of models supported by case study

I obtained support via this case study, as described in Section 9.3, for the following aspects of the overall framework for Internet security policy:

10 factors in Internet security policy (Figure 3-3)
11 societal issues in Internet security policy (Section 3.4.2)
12 Internet risks for Internet security policy (Figure 3-5)
13 organisational issues in Internet security (Table 3.2)
14 administrative issues in Internet security policy (Section 3.4.5)
15 legal issues in Internet security policy (Section 3.4.6)
16 technical issues in Internet security policy (Section 3.4.7)
17 human issues in Internet security (Table 3.4)
18 Internet security policy content (Table 4.1)
19 IAUP content (Table 4.3)
20 email policy content (Table 4.4)
21 framework for development of Internet security (Figure 4-1)
22 overall framework for Internet security policy (Figure 4-2)

9.4.2 Case study conclusions

In this section, I first remind the reader of the intent of this final piece of research in this project. I then indicate the presence of an Internet security problem at UP, and analyse what this case study mean in terms of the original research questions stated in Chapter 1.

9.4.2.1 Intent of case study

I remind the reader here that this fourth detailed case study was conducted mainly in order to test the relevance in 1999 of earlier research results obtained in 1996, 1997 and 1998. Hence, my discussions below relate the UP study conclusions back to the earlier detailed case studies, in order to make appropriate comparisons to ascertain continuing relevance.

9.4.2.2 Internet security problem at UP

This case study indicated the existence of an Internet security problem at UP, as was concluded for MSRI, Flyway and AUR in the earlier years. Internet risks were not being effectively controlled by diverse and uncoordinated policies, nontechnical measures which implement the policies (for example, sporadic checking of firewall logs) and technical measures which implemented the policies (for example, out-of-date anti-virus software).

Below, I discuss the implications of this case study for the three research questions:

1. What are the factors influencing effective Internet security policy for an organisation?

This investigation identified a number of factors to be addressed by an Internet security policy, as summarised below.

As described in Section 9.3.1.1, the case study revealed three highly rated Internet risks at UP—*non-business usage, hacking, and corrupted or erroneous software*, as well as a number of other significant Internet risks. UP agreed that all the risks shown in the Internet risks model (Figure 3-5) needed addressing in a future Internet security policy, thus providing support for the Internet risks model (Figure 3-5) and the Factors model (Figure 3-3), as well as contributing to answering the research question above.

As discussed in Section 9.3.1.2, the case study revealed that organisational issues, such as the need to establish a formal Internet security infrastructure and an Internet security management programme, should be addressed in a future Internet security policy. All organisational issues listed in the proposed model for organisational issues (Table 3.2) were identified as policy influences, thereby supporting the organisational issues model (Table 3.2) as well as the Factors model (Figure 3-3), and also contributing to answering the research question above.

As discussed in Sections 9.3.1.3, 9.3.1.4, 9.3.1.5 and 9.3.1.6, this case also highlighted administrative, legal, societal and technical factors influencing the policy. Importantly, it was clear that human issues would play a pivotal role in the final policy, illustrated by the permissive attitude of the company towards Internet personal use rights for employees.

Hence, as for the MSRI, Flyway and AUR case studies conducted earlier in the project, this case study has helped answer this research question by firstly identifying factors which influence the Internet security policy at UP, then pattern-matching those factors with the ones proposed in the Factors model (Figure 3-3).

2. Is an holistic approach to an Internet security policy more effective than the piecemeal approach adopted to date?

As in the earlier studies of MSRI, Flyway and AUR, the investigation at UP suggested that only by considering and drawing together the diverse factors identified could an effective policy be developed. This investigation has yielded the same answer as the studies of MSRI, Flyway and AUR to the above research question: yes.

3. Can a framework be specified for the development, issues and content in effective Internet security policy for organisations?

Evidence of support for the proposed framework (Figure 4-2) was provided by this case study. Firstly as already mentioned, the diverse factors (issues) identified for UP as influencing Internet security policy correspond to the various types of factors specified in the Factors model component (Figure 3-3) of the framework. This case study also suggested that a risk assessment was an appropriate process for developing the policy, as is shown in the framework. Finally, ample evidence was provided in Section 9.3.3 of support for the three proposed Content model components of the framework (Table 4.1, Table 4.3 and Table 4.4), and an extra sub-policy was added to the email model (signature sub-policy).

Hence, this study has provided support for the proposed framework, as did the earlier detailed case studies, and has contributed to answering this research question in the affirmative.

9.4.3 Final remarks

As a result of this case study, UP was reviewing its Internet security measures, both managerial and technical, in order to more effectively address the problems identified.

Importantly,

UP recognised the need for an Internet security infrastructure to manage all the measures required, and within this, the need for a comprehensive Internet security policy which would include, as a sub-policy, a comprehensive IAUP, rather than the limited Internet usage guidelines extant at the time.

It must be pointed out that UP suffered, as did the earlier organisations studied, from a shortage of human resources to develop such an infrastructure and policies, and plans for an infrastructure and new policy were uncertain at the time of study, accordingly.

This case study clearly shows the continued relevance in 1999 of the research results obtained in the earlier pieces of research, which were conducted in 1996 – 1998.

Although there is more which could be concluded from this case on its own, I reserve further conclusions for a later stage in the thesis. In the next Chapter, I perform a cross-case analysis of the four major cases.

Chapter 10
Cross-Case Analysis

In Chapters 6, 7, 8 and 9, I explored four detailed case studies conducted at Medical Science Research Institute (MSRI), Flyway Australia (Flyway), Aus-Retail Ltd (AUR) and USEnergy Petroleum (UP), providing support for the proposed framework (Figure 4-2) and its components.

In this Chapter, I present a cross-case analysis of the four major case studies, focusing on the factors which influence Internet security policy—as it was in this area that I uncovered interesting and controversial issues affecting the research.

Note that each of the four major case studies explored the employer perspective, while the earlier two mini cases explored the employee perspective (as represented by the students at Monash), and were preliminary research only. Wherever an issue arises in the cross-case analysis in which the employer view, and the employee view (as represented by Monash students) differ, I reference the Monash mini cases, in order to illustrate the different opinions.

Within this Chapter, I analyse cross-case support for the Factors model and its component models (Section 10.1), the Internet security policy content models (Section 10.2), the Internet security policy development framework (Section 10.3) and the overall framework for Internet security policy (Section 10.4). Finally, I draw conclusions for the research (Section 10.5).

At the outset, I highlight the fact that all companies acknowledged the existence of an Internet security problem in their companies, and the need for an effective Internet security policy.

10.1 Analysis of factors in Internet security policy

In the earlier case descriptions (Chapters 6, 7, 8 and 9), I discussed how each case provided support for the Factors model (Figure 3-3) and its components. In this section, I analyse support for the Factors model by comparing results across the cases.

In the interests of keeping this thesis to a manageable size, I only compare and discuss selected, illustrative aspects for each type of factor in the Factors model (Figure 3-3). I have selected aspects which illustrate consensus between case studies, as well as aspects which illustrate differences, as my choices for discussion.

10.1.1 Internet risks

In the cases, I identified and assessed Internet risks. In Table 10.1, I summarise Internet risks at Flyway, AUR, MSRI, UP, and also Monash (as it may prove illuminating to study differences between the risk ratings perceived by Monash students viewed as prospective employees, and the risk ratings perceived by employers at the other companies). Recall that at Monash, a Likert scale was used to assist students in estimating risk significance. I have linked student estimates to Low, Medium and High risk values, in order to compare the Monash risk assessments with those of the other four organisations. Note that entries in the table are presented in order of highest to lowest risk, across the companies.

In the interests of limiting the thesis size, I have only selected two risks for detailed discussion, after which I discuss some of the issues arising from the risk results across the companies. I have selected *non-business usage* and *hacking* for detailed discussion, as non-business usage was rated a high risk by all the companies, whereas the risk ratings for hacking varied, and therefore an analysis may prove enlightening.

Internet risks	**Risk at Flyway**	**Risk at AUR**	**Risk at MSRI**	**Risk at UP**	**Risk at Monash**
Non-business usage	H	H	H	H	H (8-10)
Corrupted or erroneous software	H	M	H	H	M (2-6)
Accidental erroneous business transactions	H	L	M	L	H (8)
Hacking	H	L	M	H	M (1-5)
Inaccurate advertising	M	L	M	M	M (0-7)
Accidental disclosure	L	M	M	L	M (2-5)
Pirated media	L	L	M	L	H (7-10)
Low quality data	M	L	L	L	M (2-7)
Inappropriate email	L	L	L	L	M (5)
Theft of information	L	L	L	L	M (2-6)
Fraud	L	L	L	L	L (0)
Denial-of-service	L	L	L	L	L (0-2)

Legend: L = Low; M = Medium; H = High.

Table 10.1 Internet risks at five companies

10.1.1.1 Non-business usage

Clearly, excessive non-business usage was the most serious Internet risk for all the companies studied, an indication of what may be happening in other companies worldwide. This suggests a lack of effective management of non-business Internet usage.

I now discuss four Internet security policy issues that may be relevant to the high levels of non-business usage at all the companies.

(i) Each company lacked an Internet policy specifying clear and appropriate limits on non-business Internet usage.

Each company was uncertain as to the amount of use, and appropriate scheduling of non-business Internet usage which would be considered "reasonable", during a relatively early stage of Internet diffusion (1996 – 1999). In fact each company appeared, when interviewed, to have been sitting back and observing the excessive non-business usage with interest rather than dismay, although when the reality of the level of risk and lost productivity was exposed through the case interviews, they became concerned.

The companies regarded the Internet as an amazing new technology, and were fascinated by the diverse (non-business) usages which their employees had encountered or initiated on the Internet. It was almost as if the companies believed they had a duty to allow their employees to take advantage, for a time, of this powerful new organisational tool. Indeed, students in the Monash case study reported their readiness to take advantage of Internet services if available, for non-work purposes.

Flyway and AUR mentioned that with the introduction of a new business technology came an initial "settling down" period during which employees tenaciously tried out various facilities, eventually becoming blase about the new technology. (One company cited the fax machine as an example.) Flyway and AUR were therefore hopeful of non-business Internet use settling down in due course. However it is noteworthy that with each successive case study, the amount of non-business usage observed increased (to 80% personal use at UP in May, 1999), a possible indicator that the problem had been worsening for companies, and needed urgent attention.

All but one of the companies had chosen the safest path of totally prohibiting non-business usage, in both officially documented and "word-of-mouth" policies (Flyway: IAUP; AUR: ISM standards; MSRI: undocumented, "word-of-mouth" policy; UP: permitted “necessary” personal use)—while in reality turning a blind eye to non-business use unless it was particularly noticeable, or a complaint arose.

Each company was hoping that supervisors would manage the problem by "walking around" and acting upon any observed excessive non-business use, and by assigning employees adequate workloads to fill

their time. However, this approach had not been successful, with Flyway, AUR and UP estimating significant losses due to lost productivity. Hence, the problem needed addressing.

It appears that the various issues relating to non-business usage, such as “freedom of Internet use”, have not yet been resolved for companies.

(ii)Each company lacked clear, risk-specific (policy) sanctions for non-business usage.

Up till now, policy sanctions had been vague and open to interpretation (for example, the phrase "disciplinary action may be taken" (or similar) was commonplace). The research suggests that because of the combination of:

- the uncertainty regarding the degree of non-business usage that was reasonable;
- the "safe" but unworkable total prohibition on non-business use in the four company policies;
- the new-technology-observer attitude of the companies; and
- the apparent view by employees that some amount of non-business Internet use was a right rather than a privilege (supported by mini case B, in which many final year university students put forward this point of view):

companies had not yet set effective sanctions for non-business usage.

(iii) Each company lacked successful measures (technical and non-technical) for checking, detecting and acting upon non-business usage.

Each company employed some form of monitoring of non-business usage, typically via supervisory surveillance and firewall log reports (a combination of non-technical and technical methods). However, existing monitoring was not proving successful in managing non-business usage. The research data suggested that this was due to:

- limited human resources available for "walking around" checking employee activities, and for checking firewall log reports;
- an inability of the firewall log and/or related reports to reveal non-business usage;
- human surveillance being considered unethical, and therefore not being carried out by supervisors; and/or
- non-business usage being culturally tolerated and, although detection may have been occurring (via either or both of human surveillance and firewall log reports), it was not being followed up.

This highlights not only the sensitivity of the Internet monitoring issue, but also a lack of resources to implement monitoring effectively.

(iv) Each company lacked adequate awareness activities to inform and explain non-business usage policy.

None of the companies had explained its non-business usage policy to its employees, via any kind of awareness session, or other awareness activity.

10.1.1.2 Hacking

Hacking was the risk incurring the greatest variation in risk assessment amongst the companies studied. This suggests that certain conditions apply at some companies and not others, resulting in varying vulnerability.

I now discuss three Internet security policy issues that may be relevant to the differing ratings of the hacking risk.

(i) Each company relied on its monitoring policies to determine whether hacking was occurring into or out of the company.

At MSRI, Flyway, AUR and UP, logs of attempted and successful accesses into and out of the companies were maintained on firewalls, and monitored, albeit sporadically. The companies all relied on this monitoring to ascertain whether hacking was taking place. None of the companies had experienced penetration from a hacking attempt, and all had deduced that the frequency of attack was low via monitoring of the firewall logs.

(ii) Each company judged its hacking risk based on an estimate of potential impact, rather than current frequency.

All companies detected sporadic hacking attempts in and out, as mentioned in (i) above. The companies believed they had adequate technical measures in place to minimise the success rate of any hacking attacks, and unanimously referred to the *impact* of a successful hacking attack (rather than the *frequency* of hacking attacks), as the basis for their risk assessments for hacking.

MSRI rated the hacking risk as medium, on the basis of estimation of a significant (but not unrecoverable) impact on company systems, should successful penetration of company systems from outside, occur. Flyway rated the hacking risk as high, based on the existing accessibility from the outside world of several key financial applications as well as a planned data warehouse, hence increasing the severity of damage should penetration of their systems occur. Flyway also looked to the future of an online air reservation system (now in place) which could increase the impact of a successful penetration. In such circumstances, it would also rate the risk high. AUR had distributed its data and processes to lessen the impact of any penetration, and hence rated the hacking risk as low, although it believed that the hacking risk would be reassessed as high when e-commerce functionality became more substantive (AUR e-commerce functionality has been gradually increasing over the past year). UP had some corporate data

accessible via the Internet, and accordingly adjudged the potential impact of any penetration as high—consequently rating the risk of hacking as high.

(iii) Each company was at a different stage in the maturation of e-commerce, and the existing level of e-commerce functionality was a contributing factor in the rating of the hacking risk. Essentially, the increased e-commerce functionality increased

MSRI only undertook communication and collaboration via email, and the dominant reason why it considered the hacking risk as medium (rather than low) was its perception of the sensitivity of its scientific data, were it to be compromised. AUR possessed very limited e-commerce functionality at the time of study, indicating that this e-commerce immaturity was a contributing factor to rating the hacking risk as low, and indicating that its rating would change to high when e-commerce was more substantively deployed. Flyway already maintained e-commerce applications online, hence its high rating of the hacking risk at the time (and in anticipation of the increased risk associated with planned online air reservations). UP had provided company credit-card sign-up facilities on a web site, and the potential impact of penetration of this data contributed to its rating the hacking risk as high.

10.1.1.3 General comments on Internet risk assessments

The fact that companies rated certain risks differently may be an indicator of many things. Perhaps, as already suggested, risks (or their perception) increase with e-commerce maturation, and the degree of potential impact..

The fact that companies rated certain risks consistently, may also indicate different things. For example, the generally low levels of e-commerce functionality at all the companies studied may account for *fraud* and *denial-of service* being rated low risk at the time of study. *Fraud* may be considered more of a concern when online transactions were implemented, while *denial-of-service* may be considered more of a problem as more employees in the companies became Internet-connected, and company systems became Internet-dependent.

The fact that the risks were able to be ordered informally (as shown in Table 10.1) indicates some agreement across companies as to the most worrisome and least worrisome risks.

Undoubtedly, the risk assessment process that companies carried out in my studies—that is, via my consulting the opinions of the experts present—yielded data which illuminated risk management and policy issues for the companies I interviewed, and was hence a useful process from their perspective.

A final note relates to the proposed Internet risks model. Approval was given by all four companies for the Internet risks model (Figure 3-5).

10.1.2 Organisational factors

Table 3.2 suggests the following categories of organisational factors that influence Internet security policy: *organisational objectives, Internet security infrastructure, management commitment, Internet security management programme, Internet security awareness, policy integration, and principles for Internet security and policy*. I discuss each of these below.

10.1.2.1 Organisational objectives

Only one of the companies studied (Flyway) listed valid business usages of the Internet via policy, and the list supplied was not exhaustive. None of the company Internet policies directed their employees to organisational objectives, nor listed valid business usages of the Internet, nor documented an Internet strategy from which policy could be derived. As employees were excessively using the Internet for non-business purposes, it is clear that the companies would have benefited from studying their organisational objectives and stipulating usages consistent with those (as well as other valid usages for legality (eg union email may be permissable by law) and other reasons).

10.1.2.2. Internet security infrastructure

None of the companies studied possessed such an organisational infrastructure at the time of study. MSRI was not planning an infrastructure at all, Flyway and AUR were planning to have these when resources became available and electronic transactions were fully realised, and UP was not yet even planning one. Nonetheless, all companies believed such an infrastructure would be advantageous for effective Internet management and policy. A lack of resources was unanimously cited as the reason why the infrastructure was still only in the pipeline.

10.1.2.3. Management commitment

In all cases, senior management was not sufficiently committed to Internet security to supply the resources for an effective Internet security policy. The reasons cited for lack of management involvement included inadequate time allocated by managers to Internet security issues, and a lack of awareness of the problems. Inadequate management commitment clearly limited what could be achieved via a policy. It is of interest that Flyway was not convinced that management commitment would reduce certain risks such as non-business usage.

10.1.2.4 Internet security management programme

None of the companies studied possessed a formal programme of this kind, although informal programmes were in existence (in the heads of security managers). All companies believed that such a programme would be part of any eventual infrastructure. The lack of a comprehensive, formal, documented programme clearly reduced the effectiveness of existing policy (for example, there was a lack of awareness activities to support existing policy).

10.1.2.5 Internet security awareness

None of the companies studied featured adequate Internet security awareness activities. All companies agreed that increased awareness would render the policy more effective. Flyway possessed the most comprehensive awareness and training programme at the time, although the degree of effectiveness was unknown (and untested in the Flyway case study).

10.1.2.6 Policy integration

Most of the companies attempted to ensure that policies affecting Internet security were consistent. From a study of the various policies in the cases studied, the relationship between policies was not always clear. Companies agreed that better integration of related policies with the Internet security policy would improve its effectiveness.

10.1.2.7 Principles for Internet security and policy

In all cases, the need for such principles was agreed upon, and in some companies, several principles were already in place (eg enforceability).

Approval was given by all four companies for the organisations factors model (Table 3-2).

10.1.3 Administrative factors

At AUR, various administrative procedures were specified in the ISM standards (albeit at a high level), while at Flyway and UP procedures were documented sporadically, and were neither defined nor referenced within policies. At MSRI, documentation for procedures was scattered and informal. All companies agreed that procedures for auditing, applying, monitoring, reviewing and updating Internet security policy needed formal documentation, and that policy relating to these procedures should be considered and included in the Internet security policy.

10.1.4 Legal factors

Note that in Chapter 4, I discussed a selection of legal issues as summarised in Table 3.3, however this research project did not attempt to explore all listed issues in the case studies, hence I do not analyse them individually here.

All companies agreed that relevant laws (such as those relating to the issues in Table 3.3, including cryptography, censorship, defamation, etc.) should be consulted prior to setting policy, and that legal issues should be dealt with in the policy. AUR mentioned running its draft policy past its legal division for approval. Flyway mentioned a process in which their legal department forwarded matters of legal interest to the security managers. Flyway, AUR and UP already referenced selected legal issues in existing policies (for example, Flyway instructed employees not to transfer material via the Internet in breach of copyright).

10.1.5 Societal factors

All companies agreed that cultural and ethical factors were important for an Internet security policy. In some cases, selected ethical issues were already referenced in existing policies. For example, AUR referenced the company Code of Ethics in their ISM standards. Companies agreed that a section on netiquette in the Internet security policy would facilitate communications with different types of societies.

10.1.6 Technical factors

Companies agreed that high level policies for Internet security technology requirements should form part of the Internet security policy. The AUR ISM standards included such requirements, already.

10.1.7 Human issues

Human issues listed in the human issues model (Table 3.4) are: *freedom of Internet use, privacy, censorship, right to be kept informed, accountability, ownership and ethics.* These are analysed below. Note, at MSRI, only the first three issues were analysed. Many of the issues proved to be contentious, as the reader will discover.

10.1.7.1 Freedom of Internet use

There was much controversy and uncertainty over this issue in all companies. Each company studied was suffering loss of productivity, with employees spending large percentages of Internet time on personal rather than business use. It was arguable as to whether Internet use should be a privilege, a right, or a

company benefit. There was also uncertainty as to the degree and scheduling of personal Internet use, throughout the companies. The "freedom of Internet use" issue clearly affects policy.

10.1.7.2 Privacy

All companies agreed there were contentious privacy issues for themselves, their employees and their customers, to be considered prior to setting policy. For example, while the four companies mentioned the need to monitor employee Internet use, the students at Monash were firmly opposed to monitoring, believing this signalled a lack of trust between employer and employee, as well as an invasion of privacy. There were other contentious privacy issues involved, as discussed in the various case descriptions.

10.1.7.3 Censorship

There were mixed opinions regarding censorship issues, such as the filtering of employee accesses to dubious, external web sites, via company firewalls. AUR and UP did not believe in filtering, whereas Flyway filtered out selected sites. (No data on this issue was collected from MSRI.) AUR and UP believed it was up to employees to access appropriate sites as instructed in policy, and not up to the company to actively censor. Flyway was wary of the bad publicity which could eventuate if a company discovered and reported that Flyway employees had accessed their dubious sites—hence, Flyway's decision to filter**.** Students at Monash were outraged at the prospect of such censorship. The four companies under analysis recognized that the censorship issue was contentious, and needed careful consideration prior to setting policy.

10.1.7.4 Right to be kept informed

All but one company agreed with the employee's right to be kept informed about Internet security policy matters. MSRI believed, "Employee (buyer) beware", but accepted that if it developed a formal policy, it would need to inform employees regarding policy matters, for legal reasons. Hence, this was not a contentious issue, although companies found it difficult to resource awareness activities.

10.1.7.5 Accountability

All companies believed employees should be held accountable for their Internet activities via awareness, monitoring usage, and sanctions on non-compliance. Note that employers were aware that employees disliked monitoring, and consistent with this view, the students at Monash opposed monitoring. Accountability was contentious, in that employees, whilst willing to be held accountable, do not like being monitored. *The issues of* ***monitoring*** *and* ***surveillance*** *were contentious enough to warrant inclusion in the model of human issues, as separate issues.* I make a further note here that an additional

problem highlighted in discussions about accountability was the difficulty in making an employee accountable, given inadequate resources for checking the firewall logs of Internet use.

There was some discussion over the level of sanctions appropriate in a policy, with Flyway insisting that highly specific sanctions not only conveyed an attitude of distrust between employers and employees, but were politically unacceptable to unions. Instead, Flyway preferred a general sanction such as, "Disciplinary action will be taken." AUR however, were very keen on the idea of specific sanctions. UP, on the other hand, gave managers responsibility for dealing with non-compliance. This suggests that ***sanctions*** warrants inclusion in the model of human issues, as a separate issue.

The issue of trust arose many times in discussions over accountability—trust between the employer and employee—hence warranting the inclusion of ***trust*** in the model of human issues, as a separate issue.

10.1.7.6 Ownership

There was unanimous agreement that companies owned all web sites on their servers, even employee home pages, and could therefore constrain content and design if they so desired. The cases also vindicate the literature suggesting that employers regard employee email as company property, although companies expected employee contention on this issue. No data was collected in the mini cases regarding student views on this issue, however evidence from the detailed cases suggests that the issue is to some degree contentious, and should be addressed via policy.

10.1.7.7 Ethics

Ethical issues, such as the need for netiquette in email communications, were considered important influences on policy, by all companies studied.

Approval was given by all four companies for the human issues factors model (Table 3-4), however I have added four new issues as a result of this analysis: monitoring, surveillance, sanctions and trust.

10.2 Analysis of models for content of Internet security policy

I remind the reader that the MSRI study did not incorporate an analysis of the content models. Hence, this section discusses solely the Flyway, AUR and UP studies. In the interests of limiting the size of this thesis, I refer the reader to discussions showing how the three cases loaned support for the Internet security policy content model (Table 4.1), the IAUP content model (Table 4.3) and the Email policy content model (Table 4.4). The discussions are at: Flyway (Section 7.4.3); AUR (Section 8.3.2); and UP (Section 9.3.3).

The cases supported all components of the three content models, with a cautionary note from Flyway regarding the possible need to keep some sub-policies confidential from employees, in particular, the firewall sub-policy (Table 4.2).

Although no aspects of the proposed content models were contradicted by any of the studies,

two new components were suggested:

(a) Signature sub-policy to be added to the Email policy (Table 4.4) (suggested by the UP case); and
(b) Email virus protection sub-policy to be added to the Email policy (Table 4.4) (suggested by the Flyway case).

10.3 Analysis of model for development of Internet security policy

The four companies approved the development model (Figure 4-1), as discussed in the earlier Chapters describing the cases. In particular, they liked the holistic nature of the approach, which takes into account the many diverse issues involved. There was some discussion over the practicality of the risk assessment process, with Flyway needing to use professional security expert opinion to rate risks, due to the shortage of risk assessment skills amongst their security staff (again, the cause was a lack of resources to train staff in these skills).

10.4 Analysis of framework for Internet security policy

All companies approved the overall composition of the framework for Internet security policy, shown in Figure 4-2, again commenting that they liked the holistic nature of the framework. There were no suggestions for improvements to the framework. I have already analysed the individual components of the framework in earlier sections of this Chapter, and hence now move on to draw conclusions for the Chapter.

10.5 Conclusions

In this Chapter, I have analysed various types of factors in Internet security policy, and the support provided for the framework and its component models, across the cases, focusing on the four detailed case studies. Below, I draw conclusions from the analysis.

- The analysis suggests that similar conditions exist in the area of Internet security policy, in Australian companies (and the UP case study indicates a smilar situation outside Australia). There were significant Internet risks being experienced at all the companies I studied (Section 10.1.1), and a lack of adequate management of the issues via any formal Internet security

management programme or set of integrated policies. Instead, Internet security management was being treated as an informal aspect of information security management, and as a result, Internet security issues were not being addressed effectively. It was further apparent that none of the companies had spent the time thinking through the various Internet security issues, perhaps as a result of lacking the organisational Internet security infrastructure which would facilitate this.

There was significant agreement between the case companies regarding the various problem issues highlighted—for example all the companies reported excessive non-business use, and inadequate resources allocated to Internet security. Where I observed different Internet security situations between companies regarding a specific issue, the differences sometimes stemmed from the differing company cultures. For example, UP was highly trusting of its employees, and relied upon managers taking responsibility for employee Internet misuse and abuse (rather than relying on sanctions), whereas Flyway was not as trusting, but included a general disciplinary sanction in its policy, and noticeably referred to the influence of the union on policy matters.

In other instances where different Internet security situations existed between the companies I studied, the level of awareness of the company of the ramifications of Internet security breaches appeared to have influenced policy. For example, Flyway was the only company which filtered dubious sites from employee access, remarking on the possibility of the visited sites' owners recording and publicising Flyway employee visits. The other companies were apparently unaware of this possibility, or else had not thought the issue through to the same extent as had Flyway.

- The analysis suggests there are issues related to Internet security policy which are being swept under the carpet and need to be brought to light for clarification—for example, the level of Internet personal use tolerated "in practice" may differ from that tolerated "in theory". Decisions regarding policy must be appropriate, acceptable to the affected parties, and enforceable—for example, three of the major case companies prohibited non-business use entirely and one permitted it where necessary, yet each company was unable to enforce its non-business use policy, in no small part due to the lack of acceptance of the non-business usage policy by employees.

- The analysis suggests a lack of resources for Internet security policy—a salient example being the lack of human resources for monitoring logs of Internet usage. Another interesting example of the extent to which the resource shortage affects policy, was the inability at one company to train staff in formal risk assessment process due to a limited training budget, hence resulting in expert opinion of risks, rather than risk assessment, being the de facto method for assessing risks.

- The analysis indicates the need for significantly increased Internet security policy awareness activities for employees.

- With respect to the Internet risks across the companies:

  - The analysis suggests that *non-business usage* and *viruses* (malicious code) are the two most significant Internet risks, being rated as high risks across all the companies I studied.

  - Different risk assessment values for each Internet risk, by each company, suggests that not all risks are considered of equal concern. Because managers may choose to spend their limited resources on managing the more highly rated risks, the analysis supports the need for the risk assessment process shown in the policy development model (Figure 4-1).

  - The analysis suggests that companies currently focus on Internet security policy decisions that reduce the potential *impact* of risks—which appears to be more internally controllable than the *frequency* (the frequency may be the level of attack from an external source, for example, and hence not be under company control). For example, distributing Internet-accessible data and processes, and storing sensitive corporate data away from the Internet, are two decisions a company can take to reduce the impact of any penetration.

  - The analysis suggests that as companies plan for increased e-commerce functionality, they should review their policies to ensure that any increased risk is adequately managed. For example, although the hacking risk was rated low by AUR at the time of study, AUR believed that hacking would become a high risk when full e-commerce functionality eventuated.

  - The analysis suggests that firewall systems are critical measures for managing the hacking risk, with all the companies I studied successfully stopping attacks at their firewalls. The discussions further indicate that monitoring all access attempts from external parties, via firewall logs, is an important aspect of managing Internet risks—for example, companies relied on these logs to determine the level of hacking attacks currently being experienced.

- With respect to the various factors (other than Internet risks) affecting Internet security policy, and their respective models from the proposed framework:

  - The analysis provides support for the organisational factors model (Table 3.2) as discussed in Section 10.1.2.

  - The analysis suggests that the major organisational limitations on effective Internet security policy in companies are: lack of a formal organisational Internet infrastructure and Internet security management programme, featuring a comprehensive Internet security policy; lack of a clearly articulated relationship between business objectives, Internet strategy and

Internet acceptable usages; lack of adequate resources for Internet security (as already mentioned); lack of senior management commitment to Internet security; and inadequate integration between Internet policies and other related policies.

- The analysis reveals: a need in companies for documented administrative procedures for implementing Internet security policy (Section 10.1.3); a growing awareness by companies of the need for the Internet security policy to be legally correct, and for employees to be made aware of relevant laws (Section 10.1.4); a need for greater awareness in companies of the relationship between the Internet security policy and company cultural and ethical standards (Section 10.1.5); and a need for specifying high level Internet security technological requirements as policy (Section 10.1.6).

- The analysis provides support for the human issues model (Table 3.4) as well as suggesting four new human issues—*monitoring*, *surveillance*, *sanctions* and *trust* (as discussed in Section 10.1.7).

- The analysis reveals the importance and contentiousness of human issues in setting Internet security policy (Section 10.1.7).

- The analysis supports the three content models (Tables 4.1, 4.3 and 4.4) through the discussions in Section 10.2, with two new sub-policies being added to the model for Email policy (Table 4.4), namely a *signature* sub-policy and an email *virus protection* sub-policy.

- The analysis supports the Internet security policy development framework (Figure 4-1), as discussed in Section 10.3. The companies particularly liked the holistic nature of the approach.

- Finally, the analysis provides support for the proposed framework for Internet security policy (Figure 4-2) and its component models and discussed in Section 10.4, as well as suggesting several additions to selected models (as already mentioned). No contradictions to the proposed framework were indicated by this analysis, other than the abovementioned additions to selected models.

In the next Chapter, I describe the Focus Group, and present a revised framework.

Part IV

Theory Validation

Chapter 11
Focus Group and Revised Framework

In Chapter 6, 7, 8 and 9, I described the *in-depth analysis* sub-project, in which I explored and provided support for the proposed framework via four detailed case studies. In Chapter 10, I analysed the case results across these four cases, as well as including earlier results from the two mini cases (Chapter 5), where relevant. The cross-case analysis provided further support for my proposed framework.

This Chapter describes the *theory validation* sub-project, in which I test the proposed framework for validity. In Section 2.3.6.1, I noted that a focus group would be appropriate for this sub-project (enabling triangulation).

I begin by presenting the objectives of the focus group in Section 11.1. I then describe the focus group procedures in Section 11.2. I describe and analyse the focus group in Section 11.3, and present the revised framework in Section 11.4—taking into account the case results obtained in earlier Chapters, as well as the results of the focus group. I draw conclusions for the research project in Section 11.5.

11.1 Focus group objectives

The focus group objectives were:

(i) To determine whether an Internet security policy was considered an important policy for Internet-connected companies.
(ii) To determine whether the proposed framework (Figure 4-2) and its component models could be useful to companies.
(iii) To determine any changes to the framework which would improve it.
(iv) To elicit recommendations regarding the presentation of the framework as a commercial methodology.
(v) To determine the overall usefulness of the research project.

11.2 Focus group procedures

I first described the focus group procedures in Section 2.3.6.2. A more detailed description follows.

A moderator led the focus group. The person I selected as moderator is a respected academic in the area of electronic commerce, with good communication skills and familiarity with the topic area.

There were five participants in the group. For reasons of anonymity, I do not cite the company names here.

- an analyst/programmer from a large IT outsourcing provider;
- an IT auditor from a large, international telecommunications firm;

- a telecommunications consultant from a large Australian telecommunications company;
- a computer systems officer/network administrator from an informtaion technology department at a large University; and
- an analyst/programmer from a large IT outsourcing provider (different company to the earlier-mentioned one).

I initially recruited the participants by telephone, following up with a mail out of:

- a confirmation letter providing details of the meeting date, time and location;
- a form to be completed by each participant, providing relevant background for the moderator; and
- a statement of the focus group objectives.

Prior to the meeting, the moderator reviewed the supplied background data for each participant, in order to gain some level of familiarity with each person. At the start of the meeting, I provided a document containing an introduction to the research topic and issues, as well as the Framework and its various models.

The meeting took place as a three hour session, in June, 1998, in a special observation laboratory designed for such activities, located at Monash University. The room possessed video cameras and audio recording facilities, as well as a one-way window through which participants could be observed from the room next door. The meeting was video-recorded for later study. I was able to view the meeting from the room next door through the one-way window, as well as listen to the proceedings through speakers. I was also able to communicate with the moderator via a microphone which transmitted to an earpiece worn by the moderator. I used this communication facility to request the moderator to follow up issues of particular importance, as well as to ask the moderator to seek clarification on occasion.

The moderator began the meeting by requesting introductions, and explaining the focus group objectives. He then asked each participant to explain his/her company's interest in the research project, and queried participant positions regarding the research topic. The moderator led the group through a review of the document containing the topics, issues, framework and component models, always encouraging a free flow of ideas, and steering the discussion when necessary to determine support or lack thereof for the framework and its models, or to elicit suggestions for changes.

A lively and fruitful meeting, reported in the next section, ensued.

11.3 Focus group description

In this section, I summarise discussions and results from the meeting, in the order in which the discussions took place.

11.3.1 Initial views of Internet security policy

11.3.1.1 Importance of Internet security policy

All participants agreed at the start of the meeting that an Internet security policy was a critical component of Internet security management in organisations connected to the Internet.

11.3.1.2 Low level of diffusion of Internet security policy in organisations

None of the five companies concerned possessed an Internet security policy, although each company possessed other types of policies covering some of the issues. For example, one of the companies had an Internet acceptable use policy.

11.3.1.3 Difficulties in monitoring and enforcing policies

All participants mentioned the difficulty in monitoring and enforcing existing or future policy. One participant mentioned that infractions of his company's current Internet acceptable use policy were rarely acted upon, and hence the power of the policy was minimal.

The moderator introduced the model of three components for Internet security policy (Figure 3-2), then led participants through a review of each component model from that diagram, eventually reviewing the overall Framework for Internet security policy (Figure 4-2).

Participants began their review by considering the model of three components for Internet security policy (Figure 3-2), giving it their approval.

They next reviewed the Factors in Internet security policy model (Figure 3-3).

11.3.2 Factors in Internet security policy model (Figure 3-3)

11.3.2.1 Standards

Participants proposed an additional factor, *standards*. This factor was a component of the *societal* factor in the existing factors model, but the focus group believed it was sufficiently significant to warrant constituting a factor in its own right.

Participants believed the *standards* factor should encompass industry, national or international standards which might influence policy, for example the Australian and New Zealand risk management standard: AS/NZS 4360:1999, developed by Standards Australia and New Zealand. Technical standards such as

encryption standards were also considered by the meeting under this new *standards* heading, however there was some discussion as to whether technical standards were, rather, a component of the *technical* factors contributing to policy. Participants did not reach a consensus on this last issue.

11.3.2.2 Human issues: why consider these as a special factor?

The group discussed at length the special position of the *human issues* factor in the Factors model. One participant was convinced that *human issues* did not need to be treated differently to the various other factors. In other words, he did not see why all other issues had to be considered in light of the human issues involved.

The remaining four participants were adamant that *human issues* should remain in its current, special position in the Factors model. For example, one participant pointed out that if *human issues* were treated as just another factor to be considered in policy setting, then not as many human issues would be identified as if the various other factors were seen *through* the filter of human issues. Another participant stressed that his company would not accept the model unless human issues were highlighted as shown in the existing model.

Participants agreed with the remaining factors in the model (Figure 3-3).

11.3.2.3 Interacting factors

There was a discussion about the various factors being interrelated, and a jigsaw model was proposed by one participant as a possible alternative model to show this interaction, with each factor being represented by one piece of the jigsaw. The interlocking of the pieces into the finished jigsaw would show the interaction of the factors.

The next model that the meeting reviewed was the Internet risks model (Figure 3-5).

11.3.3 Internet risks model (Figure 3-5)

11.3.3.1 Corrupted or erroneous software

Participants believed the *corrupted or erroneous software* risk hid from view the important *malicious code* risk, and suggested instead the two risks: *erroneous software* to cover accidental use of buggy software, and *malicious code*, covering viruses, worms, and other deliberately damaged software.

11.3.3.2 Hacking

Participants believed the *theft of information* risk was a subset of *hacking*, and suggested subsuming the *theft of information* risk under the *hacking* risk.

11.3.3.3 Fraud

Participants suggested that scams were more appropriately covered by the *fraud* risk, rather than by the *low quality data* risk.

Participants agreed with the remaining Internet risks in the model (Figure 3-5).

The meeting then reviewed the Organisational factors model (Table 3.2).

11.3.4 Organisational factors model (Table 3.2)

11.3.4.1 Internet security infrastructure

There was a discussion over the use of the term *Internet security infrastructure* for soft organisational issues such as Internet strategy. Participants believed that infrastructure implied hardware architecture, which should be independent of policy. They suggested the term *organisational Internet security framework* to replace the term *Internet security infrastructure.* As the word *framework* may cause some confusion with the use of the word for my overall framework for Internet security policy, and as the word *infrastructure* is increasingly being used for organisational aspects of the Internet, I decided to rename this factor *organisational Internet security infrastructure*.

11.3.4.2 Internet security awareness

Participants suggested that an additional factor *Internet security training* be included in the model, rather than subsuming it under the heading *Internet security awareness.*

11.3.4.3 Organisational culture

Participants believed an additional factor *organisational culture* should be added to the model, to ensure that the final policy was suited to the organisational climate.

Participants agreed to the remaining organisational factors in the model (Table 3.2).

The next model discussed by the meeting was the Human issues model (Table 3.3).

11.3.5 Human issues model (Table 3.3)

11.3.5.1 Organisational culture

There was some discussion as to whether *organisational culture* belonged in the model for *human issues* rather than, or in addition to, the model for *organisational* factors (see Section 11.3.4). The meeting eventually decided that *organisational culture* belonged in the model for *organisational factors*.

11.3.5.2 Freedom of use

Participants engaged in a heated debate about whether there should be restrictions, or even any policy at all, on the freedom to use the Internet for personal use, or for a limited time per day for any purpose, in the workplace. All present considered *freedom of use* to be an extremely important and controversial issue for organisations, in Internet security policy.

Salient comments made by participants included:

- "If a manager is being charged for employee Internet use, s/he will get onto it (ie manage personal Internet use)"
- "No-one in my company would accept one hour per day as a limit on Internet use."
- "Why should employees have *any* free (personal Internet) use?"
- "The cost of monitoring use might be greater than the cost of abuse."
- "Limited personal use of the telephone in the workplace is accepted, so limited personal use of the Internet should be, too."
- "Personal Internet use should be part of the overall employment package… (it) should indicate that an employee is valued."

Participants agreed with the remaining human issues listed in Table 3.4, with various absorbing discussions taking place (in the interests of limiting the size of this thesis, I have omitted reporting these discussions.) There was sufficient discussion of the issues of trust, monitoring, surveillance and sanctions, to support my earlier thoughts expressed in the cross-case analysis (Section 10.1.7.5) regarding including these four issues as separate issues, in the model.

The meeting then proceeded to review the framework for the development of Internet security policy (Figure 4-1).

11.3.6 Framework for development of Internet security policy (Figure 4-1)

The discussion focused on the need for, and type of, risk assessment process required.

11.3.6.1 Risk assessment

There was some discussion regarding whether the risk assessment process—which all agreed was necessary—should be qualitative or quantitative. Participants finally agreed that the Internet security technology implemented should be cost-justified, and that the policy should not specify sub-policies which would be too expensive to implement. Therefore a *quantitative* risk assessment process is required as part of policymaking. Further, the risk assessment results should be fed not only into the policy, but also into the technology and procedures selected to implement that policy.

For example, the risk assessment results may suggest a policy of a firewall to control certain risks, and, due to low exposure values for related risks, may suggest that the implementation of that policy be an inexpensive firewall.

11.3.6.2 Code of Ethics

One participant suggested that the company Code of Ethics should form an input into the policymaking process whenever human issues were being considered, as many of these issues were already covered in the Code of Ethics.

Apart from the issues discussed above, the meeting concurred with the development framework presented (Figure 4-1).

The meeting then reviewed the models for Internet security policy content (Table 4.1) and Internet acceptable use policy (Table 4.3)

11.3.7 Internet security policy content model (Table 4.1) and Internet acceptable use policy content model (Table 4.3)

11.3.7.1 Internet acceptable use policy content model (Table 4.3) (IAUP)

All except one participant saw the need for an IAUP. The differing participant pointed out that telephone use in the workplace did not require an acceptable use policy or "signing off" of such a policy, so why did the Internet?

Some important differences between telephone usage and Internet usage were then highlighted by another participant:

"The Internet stores information communicated, whereas the phone does not. Also, the Internet disseminates information to multiple recipients in a very short time."

Eventually, all participants agreed to the need for an IAUP.

They then discussed the possible requirement that employees sign off the IAUP in order that they could be held accountable for subsequent abuse. One participant mentioned the common system of issuing escalating warnings for employees on successive breaches of policy, hence obviating the need for signing off. However, most participants felt that signing off the IAUP was part of Internet security awareness, and hence a good idea.

Participants agreed with the subpolicies in the IAUP content model in Table 4.3.

The meeting proceeded to review the other aspects of the Internet security policy content model (Table 4.1).

11.3.7.2 Internet security infrastructure sub-policy

Infrastructure implied hardware, according to one participant. A better name for this sub-policy was suggested as *organisational Internet security framework*. For the same reasons I gave in Section 11.3.4.1, I decided to rename this sub-policy *organisational Internet security infrastructure.*

11.3.7.3 Accessibility of the Internet security policy by employees

Participants noted that not all sub-policies of the Internet security policy should be accessible by the employees (for example, the firewall sub-policy).

11.3.7.4 Frequency of review of policy

In order for the Internet security policy to be implemented, at least one year was recommended between reviews of the policy and consequent change. A year was regarded as the ideal period between reviews. This period would be stipulated as part of the Internet security policy review sub-policy.

11.3.7.5 Internet security technology sub-policy

A suggestion was made to remove this sub-policy, in order to keep the policy lasting longer, as technology changed so rapidly. However, general policy which did not specify specific technology (for example, it would be allright to stipulate, "a firewall is required") was considered appropriate.

11.3.7.6 Internet publication sub-policy

Participants were uncertain whether this should be part of the Internet security policy, or whether it should exist elsewhere (for example, it could be a policy owned by the Marketing department of the organisation).

Participants agreed with the remaining sub-policies of the Internet security policy content model (Table 4.1).

11.3.7.7 Duplication between Internet security policy model and IAUP model

Participants noted the overlap or duplication between the sub-policies of the IAUP model, and the (non-IAUP) sub-policies of the Internet security policy model (for example, the IAUP model lists a *privacy* sub-policy, while the Internet security policy also has an *Internet privacy* sub-policy). Through discussion, participants recognised the need for the IAUP to be a stand-alone document which employees could take away with them, containing all the information they needed to know, and eliminating the need for referring to the Internet security policy for guidance. The level of duplication between the two policies was deemed appropriate.

The meeting then reviewed the framework for Internet security policy (Figure 4-2).

11.3.8 Framework for Internet security policy (Figure 4-2).

Participants agreed with the framework in its existing form, but noted that the various models reviewed thus far had become sufficiently complex that confusion threatened the application of the framework and associated models, in practice.

Discussion then took place to resolve this concern, resulting in two suggestions: the development of a *content map* for guidance to the various models, and the securement of the services of a document design expert to produce a *guide or overview for the framework.*

11.3.9 Converting the framework into a methodology

Participants thought that if the framework was intended as a methodology, a set of Guidelines to the Methodology was required—these to include a content map, an overview, detailed explanations for each model and model component, and author guidelines for each component indicating who should be involved in the development of that component (for example, IT personnel, CEO, Human Resources personnel, legal personnel, technical writers). Alternatively and ideally, required skills and expertise could be specified for a *team* to develop the policy. The team effort should ideally be driven from the top (senior management).

11.3.10 Focus group research outcome

The moderator concluded the meeting by asking participants whether they thought the Framework was a good starting point for an organisation to develop an Internet security policy, and whether the framework would have a useful outcome in practice.

One participant responded that the framework would be useful as a commercial methodology when polished and expanded as suggested in Section 11.3.9 above.

A second participant commented that the required content was present in the framework, and that the framework met the research objectives, but that its presentation could be improved by a Document design expert (as suggested earlier), to make the framework more useable for an organisation.

A third participant, an auditor, advised that he wished to use the framework, with permission, as a guide for an impending Internet audit.

A fourth participant commented, "It (the framework) was great," but added that it needed to be worked over by a legal team and a publicising team, prior to finalisation.

The fifth participant believed the framework was very comprehensive, and mentioned that if a particular company wanted to use it, they would surely find the means to handle the practicalities that had been mentioned to date—such as the need to set up an appropriate team to develop the policy.

11.3.11 Conclusion

The focus group provided significant support for the proposed framework and its component models. Below, I restate the focus group objectives, and summarise how these were met by the meeting.

(i) To determine whether an Internet security policy is considered an important policy for Internet-connected companies: The focus group responded with a resounding "yes".

(ii) To determine whether the proposed framework (Figure 4-2) and its component models could be useful to companies: The focus group responded "yes", provided that changes were made as they had suggested.

(iii) To determine any changes to the framework which would improve it: The focus group made a number of suggestions for improvements.

(iv) To elicit recommendations regarding the presentation of the framework as a commercial methodology: Participants made a number of recommendations regarding such presentation.

(v) To determine the overall usefulness of the research project: Participants considered the project to be highly relevant and potentially useful for practical application in businesses.

How did this focus group help answer the original research questions from Chapter 1, for this project?

•. *What are the factors influencing effective Internet security policy for an organisation?*

Participants clearly indicated support for the factors listed in the various models, as well as nominating additional factors (such as *standards*), and making changes in several factors (such as replacing the *corrupted or erroneous software* risk by the *erroneous software* risk and the *malicious code* risk). The focus group also highlighted the controversial nature of certain issues, as I will discuss in my conclusions Chapter which follows.

• *Is an holistic approach to an Internet security policy more effective than the piecemeal approach adopted to date?*

Participants mentioned the need for a team possessing diverse skills to set the policy, due to the wide-ranging scope of the issues involved. Participants also pointed out that the factors influencing policy are interrelated, suggesting that an holistic approach is required. The group also believed it was important to consider the many diverse factors during the development of policy (as shown in my model for policy development—Figure 4-1), again favouring an holistic approach. Finally, in the many discussions that took place, it was clear that there were various stakeholders holding different views on policy matters—again supporting an holistic approach

• *Can a framework be specified for the development, issues and content in effective Internet security policy for organisations?*

Participants fundamentally approved the proposed framework (Figure 4-2) for development, issues and content in Internet security policy, hence answering in the affirmative to this question.

Participants made a number of useful suggestions for changes to the framework to improve it, which I incorporate, in conjunction with the case results obtained earlier, in the revised framework which follows.

11.4 Revised framework for Internet security policy

In the case studies and focus group, I explored and tested all models from the framework except the firewall policy content model (Table 4.2).

I now present and discuss the revised framework, highlighting changes which have been made to the original version. *The models for the revised framework are included in Appendix E*, however for the reader's convenience, I repeat here the overall framework for Internet security policy (Figure 11-1, also found as Figure E-2). I initially discuss each model from the framework individually, then return to discuss the overall framework (Figure 11-1, Figure E-2), in Section 11.4.11.

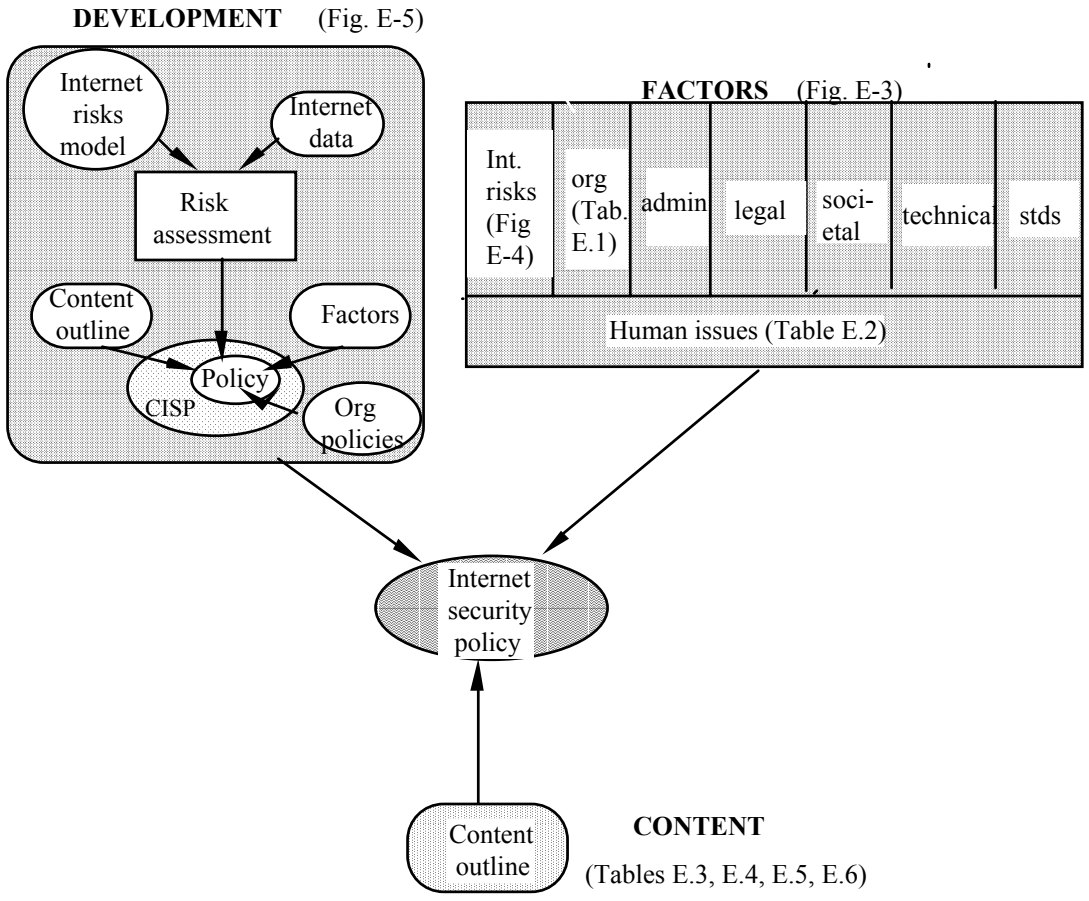

Figure 11-1 Framework for Internet security policy for organisations

11.4.1 Three components for Internet security policy (Fig. E-1, formerly Fig. 3.2)

Case study participants and focus group participants approved the model showing the three components of Internet security policy: Development guidelines, factors guidelines and content guidelines. Hence, I have left this model unchanged.

11.4.2 Factors in Internet security policy model (Fig. E-3, formerly Fig. 3.3)

The case study participants approved the various factor types shown in the model. The focus group also approved (see Section 11.3.2), but proposed an additional factor type, *standards*. The group also argued about the special position of *human issues* in the model, agreeing finally to leave this factor type in its special role of filter, through which all other issues should be considered. The group believed the different factors in the model were interrelated, but after I attempted a jigsaw model and reviewed it together with a member of the focus group, I chose to retain the original presentation as the jigsaw pieces, while showing the interrelations, detracted from the clarity and comprehension of the model.

11.4.3 Internet risks model (Fig. E-4, formerly Fig. 3-5)

Case participants approved the model and did not make suggestions for changes. However, as discussed in Section 11.3.3, the focus group suggested that *corrupted or erroneous software* be replaced by two risks: *malicious code* and *erroneous software*. The group also suggested subsuming the *theft of information* risk under the title of *hacking*, however *theft of information* covers more than merely the hacking of corporate databases, for example, it also covers the copying (stealing) of copyrighted web site material. Hence, I have retained *theft of information* in the model. *Scams* were considered to be a sub-risk of *fraud* rather than of *low quality data*, although that does not affect the model per se.

11.4.4 Organisational factors model (Table E.1, formerly Table 3.2)

The focus group made various suggestions (see Section 11.3.4), one of which was that *Internet security infrastructure* implied hardware architecture rather than soft issues. The group thought a better term was *organisational Internet security framework*, which I revised to *organisational Internet security infrastructure*, and added to the model. Other suggestions made, which I adopted, were to add the factors *Internet security training* and *organisational culture* to the model

Note that the Legal issues table (Table 3.3) was not intended as a comprehensive model, and hence was not tested in this project. Hence, the human issues model (formerly Table 3.4) is the next model I discuss.

11.4.5 Human issues model (Table E.2, formerly Table 3.4)

There was much discussion of these issues in the cases and focus group alike. In the cross-case analysis in Section 10.1.7.5, I suggested that four additional human issues, *sanctions, trust, monitoring and surveillance*, be added to the model. The focus group discussions further vindicated this decision.

11.4.6 Framework for development of Internet security policy (Fig. E-5, formerly Fig. 4-1)

The focus group thought the Code of Ethics should form an input into the policymaking process, as whenever human issues were under consideration, the Code of Ethics would be relevant. This suggests that other *organisational policies* may also form useful input, and hence I have modified the development framework as shown in Figure E-5.

11.4.7 Internet security policy for organisations—content model (Table E.3, formerly Table 4.1)

Suggestions made by the focus group were:

- rename the *Internet security infrastructure* sub-policy as *organisational Internet security framework* sub-policy; and
- possibly remove *Internet publication* sub-policy.

As discussed earlier (Section 11.3.4), I chose to rename the *Internet security infrastructure* sub-policy as *organisational Internet security infrastructure* sub-policy. I chose not to implement the second suggestion, as if companies wish to specify the publication policy elsewhere, a reference to its existence could be made in the Internet security policy.

11.4.8 Firewall policy content model (Table E.4, formerly Table 4.2)

As I did not test this model in this project, I have left the model unchanged**.**

11.4.9 IAUP content model (Table E.5, formerly Table 4.3)

No suggestions were made for changes to this model.

11.4.10 Email policy content model (Table E.6, formerly Table 4.4)

Note that explanations of the sub-policies were not provided in the original table (Table 4.4) in the interest of limiting thesis size, and the reader was (and is) referred to the sources from which the original

table was compiled (Barker *et al*., 1995; Denning, 1993; Farrow, 1998) for further details. Two additional sub-policies were suggested by two of the case studies, and have been included in the revised model:

(a) Signature sub-policy; and
(b) Email virus protection sub-policy

11.4.11 Framework for Internet security policy (Figure 11-1, also found as Figure E-2, formerly Figure 4-2)

I have suggested a revised overall framework, incorporating all the changes to the component models described above, in Figure 11-1 (also Figure E-2). The component models for the framework are all included in Appendix E. The focus group commented on the need for additional supporting documents (*content map* and *overview*) to make the framework clearer and simpler to use in practice.

11.5 Conclusion

In this Chapter, I have reported the focus group which tested my proposed framework and its sub-models. The focus group turned out to be an extremely valuable technique for my project, leading to a number of suggestions for changes to my framework, and raising some important issues which I will discuss in my conclusions Chapter which follows. I have now made a number of significant changes to the original framework and sub-models as a result of the earlier *in-depth analysis* project (case studies), as well as the *theory validation* sub-project (focus group). Accordingly, I presented a revised framework in Section 11.4 (the complete set of models for the framework appears in Appendix E).

The changes I have made to the original framework mean that:

- important issues originally hidden in the framework have now been highlighted for attention by being made explicit, namely—*standards*, *trust*, *monitoring*, *surveillance*, and *sanctions*;
- important Internet risks, whose importance was diluted by their being combined in the original framework, have now been separated, namely—*malicious code* and *erroneous software*;
- important issues which were overlooked in the original framework have now been added, namely—*organisational policies* (added to the policy development model), *Internet security training* and *organisational culture* (added to the organisational factors model);
- a model component was renamed to better reflect its intended meaning, namely— *organisational Internet security infrastructure*; and
- two new components for the email policy content model have improved the comprehensiveness of the model, namely—*email virus protection* sub-policy, *signature* sub-policy.

In the next Chapter, I draw final conclusions for the research project.

Part V

Conclusion

Chapter 12
Summary and Conclusions

Commercia piratis expulsis restituta

[The pirates were driven out and commerce restored] (Motto of Bahamas)

12.1 Introduction

In this, the final Chapter, I summarise the research project and thesis (Section 12.2), answer the research questions (Section 12.3), summarise the main contributions of the project (Section 12.4), present conclusions drawn from the research findings (Section 12.5) and suggest avenues for further research (Section 12.6).

12.2 Summary

In a research project which addresses the issues of organisational Internet security policy, I have produced:

- a contextual analysis of Internet security policy within the reference fields of e-commerce, Internet risks, human issues in Internet usage in the workplace, Internet security management and information security management (Chapters 3 and 4);
- a framework for the issues, development and content in Internet security policy (Appendix E), which features a holistic approach to the policy, and a series of models (Appendix E) as follows (the framework forms the basis for a commercial methodology):
- a model of the factors in Internet security policy, which can be used to help companies identify the various influences, and ensure that they are considered;
- a model of Internet risks, which can be used by companies to help companies identify, assess, and manage the risks via appropriate policy;
- a model of organisational issues in Internet security policy, which can be used to ensure companies consider these issues in setting policy;
- a model of human issues in Internet security policy, which can be used by companies to ensure they consider all other issues in light of the different sensitive human issues involved;
- a model for the development of Internet security policy, which can be used by companies to develop their Internet seucity policy;
- a model for an Internet security policy, which can be used by companies as a structure for their Internet security policy;
- a model for an Internet acceptable usage policy which can be used by companies to ensure Internet acceptable usage by employees;
- an (untested) model of a firewall policy, which can be used as guidance for companies in setting firewall policy, and;
- a model of an email policy, which can be used by companies as a structure for their email policy;

- summaries of the conflicts between societal, company and employee needs in Internet security policy, which will help companies identify potential trouble spots for resolution, when deciding policy (Chapter 3);
- a table of the potential impacts of Internet risks, and possible technical countermeasures to address the risks—which will help companies identify possible technical countermeasures for specific risks (Chapter 3);
- suggestions for specific content for the Internet security policy, which can be used by companies to guide them regarding policy content (Chapter 3);
- a series of case studies which alert companies to the existence of the Internet security problem for businesses, and permit an analysis of the issues facing companies when setting Internet security policy (Chapters 5 – 9);
- a cross-case analysis which highlights for companies how similar the issues are across different (primarily Australian) organisations and industry sectors; and
- a focus group which highlights for companies the fact that there is substantial agreement on *what* should be included in the Internet security policy, and *how* it should be developed, but indicates that there are many controversial aspects to be dealt with in policy-setting, and issues which will prove difficult to resolve (Chapter 11).

12.3 Research questions

In this section, I return to the original research questions, and show how the research project has answered them. In Chapter 1, I posited the research question:

Can an holistic set of guidelines for Internet security policy for organisations be developed?

This, in turn, required the answering of three subsidiary research questions which I discuss below, before returning to the overall research question.

- *What are the factors influencing effective Internet security policy for an organisation?*

In this research, I identified a set of factors to consider in the development of an organisational Internet security policy. The factor types are (Sections 3.4 and 11.4.2, Figure E-3): *Internet risks* (Sections 3.4.3 and 11.4.3, Figure E-4, Table E.7), *organisational* (Sections 3.4.4 and 11.4.4, Table E.1), *administrative* (Section 3.4.5), *legal* (Section 3.4.6), *societal* (Section 3.4.2), *technical* (Section 3.4.7), *standards* (Section 11.3.2.1) and *human issues* (Sections 3.4.8 and 11.4.5, Table E.2). For individual factors, refer to the relevant sections and models above.

- *Is an holistic approach to an Internet security policy more effective than the piecemeal approach adopted to date?*

Clearly, the answer is yes. An holistic approach involves consideration of the many diverse factors influencing an Internet security policy, as a prerequisite to developing the Internet security policy itself. In all the cases I studied, an holistic approach had not been taken, which had led to an ineffective policy.

- *Can a framework be specified for the development, issues and content in effective Internet security policy for organisations?*

Yes. The framework (Appendix E) is composed of: a model of the three components of guidelines (Figure E-1), a detailed framework for Internet security policy in organisations referencing models for development, issues and content (Figure E-2), models for the factors which influence the policy (Figures E-3 and E-4, Tables E.1, E.2 and E.7), a risk assessment-based approach to developing the policy (Figure E-5), an outline of the content of the policy (Table E.3), and outlines of a number of key sub-policies: the firewall policy (Table E.4), Internet acceptable usage policy (Table E.5) and email policy (Table E.6).

I now return to the original research question.

Can an holistic set of guidelines for Internet security policy for organisations be developed?

Clearly, the answer is yes. In this research project, I produced a conceptual framework featuring an holistic approach to developing an Internet security policy for organisations.

12.4 Research contributions

I summarise the *main* contributions of this thesis to theory and practice, in Tables 12.1 and 12.2.

SUMMARY OF KEY CONTRIBUTIONS TO THEORY
1. This is the very first attempt to explore organisational Internet security policy on the basis of a broad analytical framework. This is also the first study examining and integrating key reference fields, in order to identify important influences on organisational Internet security policy.
2. The findings add substantively to existing theory in Internet security policy for organisations. The research provides a holistic framework for the development, issues and content of an Internet policy, using a combination of subjective / argumentative and empirical research methods.
3. This study yields important empirical evidence of the seriousness of the Internet security problem for Australian organisations (as well as, to a limited extent, organisations outside Australia), and the need for an effective Internet security policy. This is the first research project collecting and analysing in-depth case data about Internet security risks and policy in Australian companies, highlighting the need for improved Internet security management via an effective Internet security policy. The findings also suggest a similar situation in other countries.
4. The findings highlight the importance of human issues in setting an effective Internet security policy. This study reveals the main issues of concern for employees in Internet usage as: *freedom of Internet use*, with employers needing to restrict Internet usage to manage the non-business usage risk; and *privacy*, with employees believing in the *right* to privacy of Internet use, hence opposing the monitoring of web accesses and email—which employers claimed the right to read. Other issues of concern are: censorship, the right to be kept informed, accountability, trust, ownership and other ethical issues. The study highlights the fact that human issues for employees affect all areas of policy, and need careful attention throughout policy setting.
5. The study reveals the need for an holistic methodology for the development of an effective organisational Internet security policy. This study highlights the importance of considering a variety of diverse factors when setting Internet security policy, and provides an holistic approach for setting the policy, where organisational, contextual and human issues are given equal consideration to technical issues.
6. Finally, this research identifies issues which add to the topic area of information security management. This study identifies and examines issues in Internet security policy which may be useful in the development of other types of information security policies—for example, the human issues.

Table 12.1 Summary of main original contributions of thesis to theory

Firstly, this is the very first attempt to explore organisational Internet security policy on the basis of a broad analytical framework. This is also the first study examining and integrating key reference fields, in order to identify important influences on organisational Internet security policy.

Secondly, the findings add substantively to existing theory in Internet security policy for organisations. The research provides a holistic framework for the development, issues and content of an Internet security policy, using a combination of subjective / argumentative and empirical research methods.

Thirdly, this study yields important empirical evidence of the seriousness of the Internet security problem for Australian organisations (as well as, to a limited extent, organisations outside Australia), and the need for an effective Internet security policy. This is the first research project collecting and analysing in-depth case data about Internet security risks and policy in Australian companies, highlighting the need for improved Internet security management via an effective Internet security policy. The findings also suggest a similar situation in other countries.

A fourth significant contribution is that the findings highlight the importance of *human issues* in setting an effective Internet security policy. This study reveals the main issues of concern for employees in Internet usage as: *freedom of Internet use*, with employers needing to restrict Internet usage to manage the non-business usage risk; and *privacy*, with employees believing in the *right* to privacy of Internet use, hence opposing the monitoring of web accesses and email—which employers claimed the right to read. Other issues of concern are: censorship, the right to be kept informed, accountability, trust, ownership and other ethical issues. The study highlights the fact that human issues for employees affect all areas of policy, and need careful attention throughout policy setting.

A fifth important contribution is that the study reveals the need for an holistic methodology for the development of an effective organisational Internet security policy. This study highlights the importance of considering a variety of diverse factors when setting Internet security policy, and provides an holistic approach for setting the policy, where organisational, contextual and human issues are given equal consideration to technical issues.

Finally, this research identifies issues which add to the topic area of information security management. The study identifies and examines issues in Internet security policy which may be useful in the development of other types of information security policies—for example, the human issues.

SUMMARY OF KEY CONTRIBUTIONS TO PRACTICE
1. Viewed collectively, the findings support the need for a well-resourced formal organisational Internet security infrastructure, centered on the Internet security policy. The discovery that businesses are disorganised in their knowledge of, and handling of, their Internet security issues, provided the insight that lead to my suggesting a formal approach to the management of Internet security, beginning with a formal organisational Internet security infrastructure—and featuring an Internet security management programme, centred on the Internet security policy. The research strongly suggests a lack of resources allocated to Internet security, a situation which needs redressing.
2. The study provides holistic guidelines for companies to use for the development of an effective organisational Internet security policy. This study has revealed the importance for a company of considering a variety of diverse factors when setting Internet security policy. The study has not only illuminated the need for an holistic approach to policy setting, but has provided a holistic set of guidelines for developing the policy. Additionally, these guidelines may prove useful in developing other kinds of information security policies.
3. The findings provide compelling support for regarding the employee as a critical component of maintaining secure Internet systems. The study suggests that businesses adopt a four way approach to controlling the all-important employee contribution to the Internet security problem, involving: tightening the security of company systems; paying special attention to human issues for employees in Internet usage; making employees accountable for their Internet behaviours and actions; and minimising reliance upon employee behaviours and actions for security assurance, through the deployment of powerful Internet security management software.
4. Finally, the study highlights the need for greater Internet regulation at all levels. This study clearly reveals an out-of-control Internet security situation at many levels, significantly affecting the trust placed by many different parties in e-commerce as a viable and promising business venture. Clearly, increased regulation is needed at company, national and international levels.

Table 12.2 Summary of main original contributions of thesis to practice

Firstly, viewed collectively, the findings support the need for a well-resourced formal organisational Internet security infrastructure, centered on the Internet security policy. The discovery that businesses are disorganised in their knowledge of, and handling of, their Internet security issues, provided the insight that lead to my suggesting a formal approach to the management of Internet security, beginning with a formal organisational Internet security infrastructure—and featuring an Internet security management programme, centered on the Internet security policy. The research strongly suggests a lack of resources allocated to Internet security, a situation which needs redressing.

Secondly, the study provides holistic guidelines for companies to use for the development of an effective organisational Internet security policy. This study has revealed the importance for a company of considering a variety of diverse factors when setting Internet security policy. The study has not only

illuminated the need for a holistic approach to policy setting, but has provided an holistic set of guidelines for developing the policy. Additionally, these guidelines may prove useful in developing other kinds of information security policies.

Thirdly, the findings provide compelling support for regarding the employee as a critical component of maintaining secure Internet systems. The study suggests that businesses adopt a four way approach to controlling the all-important employee contribution to the Internet security problem, involving: tightening the security of company systems; paying special attention to human issues for employees in Internet usage; making employees accountable for their Internet behaviour and actions; and minimising reliance upon employee behaviour and actions for security assurance, through the deployment of powerful Internet security management software.

Finally, the study highlights the need for greater Internet regulation at all levels. This study clearly reveals an out-of-control Internet security situation at many levels, significantly affecting the trust placed by many different parties in e-commerce as a viable and promising business venture. Clearly, increased regulation is needed at company, national and international levels.

I now present conclusions from the findings of this research project. In this section, I discuss the "value-added" findings which emerged from the empirical research. Note that although the empirical research was conducted almost entirely in Australia, the results may not therefore be generalisable to other countries, but are, however, indicative of the current situation worldwide.

12.5 Conclusions

23 The project clearly reveals high levels of non-business usage in companies, a natural consequence of the immaturity of Internet diffusion in the workplace (employees are highly tempted at work to use the Internet for personal purposes). I arrived at the following conclusions:

- Firstly, employees and managers alike are uncertain as to the nature of genuine business uses of the Internet. An organisation should develop an Internet strategy to include planned, value-adding or otherwise valid uses of the Internet. It was very evident from my studies that companies are not always sure of what constitutes valid or value-adding Internet use—a salient example being a recent case of managers believing that the circulation of union email did not constitute a value-adding business use of the Internet (restrictions on non-value adding usage was in their policy), and thus unfairly dismissing an employee, who promptly took the company concerned to court and won, on the grounds that union email is considered a valid medium, *legally*, for communicating union material (Carson, 2000a). Senior managers not only need education in the diverse opportunities which the Internet offers their company, but also in the legal and other valid Internet uses which the company must allow.

- Secondly, it is clear from the cases that employees, for the most part, *are aware* of the extent of their non-business usage, and *are simply taking advantage of the system*. In order to stop this, companies must set and enforce more stringent policies, and also utilise powerful Internet security management technological tools for filtering out selected undesirable sites, and monitoring employee web accesses and emails for personal usage. Companies must set stricter sanctions for non-business use policy non-compliance—and follow through with the specified sanctions, on every breach, to achieve the necessary deterrent value. There is evidence that companies are beginning to tighten the reins, in accord with these conclusions (for example, Xerox dismissed 40 employees in the US in October, 1999, and Centrelink dismissed six call centre employees in Australia for email misuse (Carson, 2000b)).

- Thirdly, companies must establish a level of non-business use which both they and their employees regard as acceptable. It is increasingly evident that email is replacing the telephone as the preferred medium of personal communication in the workplace (this phenomenon is worthy of study in its own right). In addition, employees now peruse the news online, rather than in the printed media, in order to obtain the latest, breaking news, and the other benefits of a multimedia news approach. Interestingly, skills gained by employees in personal use are likely to benefit the company when the employee uses the Internet for work reasons. Another issue is that employees increasingly regard a limited amount of personal Internet use as a perk of the job, and this "benefit" may be sold as part of an employee package, on hiring (as was suggested to me by one focus group participant). Considering all these benefits arising from personal use, employees are unlikely to accept total barring of personal Internet use, as official policy. To determine exactly how much, and what kind, of personal use should be permitted, there must, in the end, be a process of discourse and negotiation between employee representatives and managers. The bottom line, however, must be that employees should know that *any* Internet use in the workplace is a privilege—not a right.

- With respect to the noticeable employee misuses of the Internet in all the cases I studied, the companies remarked many times on the serious shortage of human resources for the purpose of checking Internet access logs, and for human surveillance of Internet screen activity (the reliance on business unit managers for surveillance obviously does not work). Senior managers should be informed of the growing Internet security problem which may require additional resourcing, in the form of purchasing the necessary Internet security management technology for monitoring, as well as the necessary human resources to check resulting reports, and take action. Business unit managers must also be educated with respect to taking action when Internet misuse or abuse is evident. However, I make an important comment here. It is no longer realistic to rely on "enough" human resources, in the kind of downsized, stressed employee world we now live in, and hence companies must increasingly look to new Internet security management

technologies to perform as many of the filtering, logging, monitoring, reporting, and alerting, tasks as possible.

- It is very clear from my research that some employees are always going to "behave badly"—as it were—no matter *what* kind of policy, awareness, monitoring, and sanctions, are employed. Hence, a multifaceted approach is now needed, featuring: (i) development of very secure systems; (ii) paying attention to the important human issues associated with Internet security and usage; (iii) making employees accountable for their actions through appropriate policies, awareness activities, monitoring and sanctions (as mentioned above), and (iv) minimising reliance on employee behaviour and actions through the deployment of powerful Internet security management software. I address this need further, below, in a second context.

- Some employees committing Internet security breaches are not "behaving badly", but rather are making innocent mistakes, due to ignorance, carelessness, or oversight. For example, in the cases I studied, employees accidentally: misdirected important emails, sent out confidential emails, downloaded viruses as email attachments (in one of my case studies, Aus-Retail, it took three weeks for the company's email system to recover fully from the Lovebug virus in May, 2000), and so forth. As before, reliance on the employee following policy, or behaving securely, is a fruitless and frustrating security strategy. Technology companies are, fortunately, beginning to respond to a newly perceived demand by developing Internet security management tools that prevent these accidents. For example, customisable email text filters that scan emails for confidential information, are available. Email clients which automatically add disclaimers to employee emails have been available for some time. Firewall software which scans attachments for virus-like code in email attachments, is available. I recommend that a company investigate the technical options available, as an important part of their Internet security policy – hence minimising, yet again, reliance on the employee.

- My case studies clearly indicate an absence of coordinated Internet security management programmes within companies, rather suggesting that a piecemeal approach is currently taken by companies to managing Internet security. An organisation requires a well-resourced, formal organisational Internet security infrastructure, featuring a comprehensive, holistic Internet security management programme, containing a range of coordinated elements, including: an Internet security policy (featuring an Internet acceptable usage policy); ongoing policy education and awareness sessions; monitoring; and a formal compliance process which handles instances of non-compliance. Policies should be implemented via firewalls and other technical security mechanisms, and should be supported by other components of the programme. The policies must be reviewed frequently, due to the dynamic, highly fluid nature of the global Internet security situation.

- In all cases studied, some element of initial Internet training had taken place (in some cases, even this was voluntary), although what component of this was security-related, I did not investigate. However dynamic and ongoing training or awareness was noticeably absent at each company. Firstly, there should be mandatory Internet security training, with testing, for each employee, prior to being granted Internet-access privileges. Furthermore, in today's fast-changing Internet environment, with new types of risks emerging seemingly daily, Internet security awareness activities must be diverse to capture attention, be of an ongoing nature, and must be presented in highly noticeable forms (for example, awareness information appearing on the screen when a browser begins executing; this information must be read and understood, before the employee may continue). Awareness of Internet security issues must be provided to senior managers, in order to secure their commitment to Internet security matters—beginning with resourcing the organisational infrastructure, through to setting a good example via exemplary personal Internet behaviour.

- In my case studies, I discovered that the non-technical managers responsible for Internet security issues (as well as for general information security issues) had very little knowledge of, or interest in, the existing implementation and state of Internet security, at a detailed level. These managers, during interviews, continually redirected my questions about such issues to the technical system administrator present, and there obviously existed an awkward relationship between the two parties, on such occasions, due to the inappropriateness of the power and knowledge being vested in the systems administrator. There was a block in knowledge of Internet security matters in the company, at this point in the managerial chain to the top, with senior managers hence having no hope of receiving accurate information about Internet security issues in order to make good decisions.

- Evidently, the system administrator had somehow assumed the power and responsibility for day-to-day Internet matters (perhaps this had even been explicitly delegated), and was neither taking direction for major Internet security issues and decisions, nor reporting these, to the supervising non-technical manager. Furthermore, the technical systems administrator was typically making reactive, rather than proactive, decisions, about many important Internet security matters. Clearly, non-technical managers need to possess the decision-making power in these matters. Hence, they need to consult with the technical systems administrators more closely and frequently, in order to have detailed knowledge of the various Internet security issues, and hence be able to plan and make important Internet security decisions, as well as being able to review their final implementation. An argument could also be made for educating non-technical information security managers about current Internet security technology, architectures and other Internet-related technical issues, to encourage them to become more involved and confident about making the important technical and non-technical decisions (which are often

difficult to separate). At a higher level, senior managers should make it their business to review the management of Internet security by the non-technical managers assigned this responsibility.

- From my research, clearly companies are fighting an uphill battle with an inherently insecure Internet infrastructure. Hence, external parties (other than individual businesses) must also take some responsibility for improving Internet security levels. I believe there should be increased and stronger laws and regulations to deter and prosecute the types of criminals who are sending extraordinarily damaging viruses such as the Lovebug and Melissa into companies, stealing credit card details from innocent consumers, or a myriad of the other crimes we are now seeing with increasing frequency and impact. Technology companies need to provide Internet software that provides security features as a high priority, particularly at configuration. Educational bodies need to run Internet security courses for members of the public and for schoolchildren, so they will be security-conscious and aware when they reach the workplace. Companies need to form conglomerates which rally around one another when a virulent Internet attack first appears on the horizon (such a group of banks has recently been formed in the US). Finally, the fundamental, underlying Internet infrastructure should be made more secure.

12.6 Further research

This research programme has made apparent the need for future research—some of which concerns further testing of the models and development of the as-yet-untested models, and some of which stems from the research findings and conclusions.

- First and foremost, further exploration and testing of the current framework is needed. I intend to develop a selection of Internet security policies for companies, using the framework produced by this research, in order to test, further explore, and develop, the framework. Additional case studies would also assist in achieving this goal.
- Two models for sub-policies of the Internet security policy were not fully explored or tested in this study, due to the limited time and scope of the project—the sub-policies being the firewall policy and the email policy. Furthermore, other sub-policies were not developed into models at all in this project—for example, the legal policy. Further literature exploration and case research would enable the firewall and email models to be developed further, and models for the remaining sub-policies to be developed. Clearly, companies would benefit from having such models to consult when developing the various sub-policies of the Internet security policy.
- The human issues model currently consists of a list of issues—but that is all. As these issues are clearly highly sensitive and critical for the development of effective policy, it would be advantageous for a company to have at hand further guidelines for each of the human issues in the model.

- As companies are uncertain as to what constitutes valid business uses of the Internet, research is needed to link acceptable Internet business uses to a company's objectives and Internet strategy, and also to other elements such as legal constraints.
- The role of the Internet for valid non-business usage should be studied, particularly now that email is emerging as the dominant method for personal communication in the workplace. It would prove illuminating to study analogies between the telephone and the Internet as personal communications tools in the workplace.
- The focus group strongly believed that the framework developed in this project could be converted into a commercial methodology to be used by businesses, and I intend to investigate this possibility.
- Now that the Internet is more pervasive in the Australian workplace, clearly there is an opportunity to survey companies, to determine the types and levels of risks being experienced, and the types and levels of policies currently in place. Questions such as: "To what extent do employees contribute to the risk of viruses entering the company systems via email attachments?" , "What are the restrictions on Internet non-business use?" and "What level of email monitoring is currently implemented?" are timely and vital questions, whose answers would assist other companies in making related Internet security policy decisions. Many other equally important issues could be researched via such a survey.
- In this project, I only obtained the employee perspective of Internet security policy in the two preliminary mini cases, via studying the views of final year Monash university students about to enter the workplace. The other four cases explored the employer perspective. It would be illuminating to study the employee perspective further, through detailed case studies of employee views in companies—in order to further explore and test the framework. In particular, it could be productive to examine the critical human issues affecting the employees, in order to produce policy guidelines for business—for example, suggested limits on non-business usage, which may well take the form of a set of feasible options. Such guidelines would need to be acceptable to employees and employers alike, as well as implementable.
- It is clear from the findings that companies should not depend on employee behaviour and actions for Internet security, but rather that technology should be relied upon as far as is possible (although the employee should, as I have already recommended, always be held accountable via policies, awareness, monitoring and sanctions). It would be useful to articulate the many errors employees could make that threaten Internet security, in order to identify the technological requirements for technologies (to be developed or implemented) that might make up the shortfall.
- I also pointed out in my findings that employees need to be made more accountable for their Internet behaviour and actions. I pointed to the lack of adequate and ongoing awareness activities. Clearly, a useful piece of research would be to develop a range of dynamic Internet security awareness activities for a business.

- I intend to conduct longtitudinal studies of the organisations which were studied in this project, in order to ascertain whether their Internet risks will have changed over a period of several years, and if so, identify the factors which have led to these changes. In particular, if Internet-related policies have changed, it would be illuminating to study the effects of policy changes on the Internet security situation. Other interesting findings may also arise out of these studies.
- An important conclusion which arose from this research was that the systems administrator typically holds too much of the power for Internet security decisions, when, in fact, it is his/her immediate manager who should retain that power. A study of this role imbalance is urgently needed.
- The research also casts a shadow over societal ethical standards. Why are more and more people attacking or abusing the Internet? Are global ethical standards in general on the decline, or is it just that the community has not yet established clear rights and wrongs for the Internet (a salient example being the popular argument that hacking is ethical if it is carried out purely with the intention of helping a company discover its vulnerabilities—a view with which I entirely disagree)? Is there hence a need within communities to educate people regarding ethical use of the Internet? A study of the ethical issues for the Internet community is urgently needed.
- One of the findings from this project has been that there needs to be increased Internet regulation at all levels, to reduce the Internet risks being experienced by companies. It would be useful, therefore, to study regulation requirements at different levels.
- In this project, if there was one single question which companies sought the answer to most keenly—if there was one single question I was asked at every presentation (and there were many) that I gave on this research topic—if there was one single question which every colleague and friend with whom I discussed my research, asked—it was this:

  How does a company make an Internet security policy work?

  In other words, there is much cynicism over whether awareness, monitoring, sanctions and technology can truly prevent a determined, ignorant, lazy or merely unwary employee from breaching a policy. Although I believe my framework may go a long way toward answering the above question, clearly further research is needed to arrive at a complete solution.

In this exciting era of expanding e-commerce opportunities and ventures, one of the biggest barriers to progress is undoubtedly the Internet security problem for organisations. In this research project, I have focused on an organisational solution to this problem—the Internet security policy—for which I have developed a framework that features an holistic approach, accounting for the many diverse and often complex issues that influence the policy.

It has long been remarked that companies ignore their information security issues until that first major breach acts as a wake up call. In an era where a single Internet risk can severely impact any Internet-connected company, businesses need to become proactive, and be prepared, by employing preventative solutions such as the policy that the framework in this research provides.

Hinc robur et securitas!

[From here, strength and security] (Motto of the Swedish National Bank)

Bibliography

AARNet (1995) *Policy on Allowed Access to the Internet via AARNet Members*, http://www.avcc.edu.au/avcc/aarnet/aarnpols/access.htm (accessed July 18 1997).

ABA (Australian Broadcasting Authority) (1999) *Dealing With Risks*, http://www.aba.gov.au/family/family/dealing_risks.html#Laws (accessed January 14 2000).

Abrams, M.D. and Bailey, D. (1995) "Abstraction and refinement of layered security policy", in Abrams, M.D., Jajodia, S. and Podell, H.J. (Eds.), *Information Security - an Integrated Collection of Essays*, IEEE Computer Society Press, Los Alamitos, California.

Abrams, M.D., Podell, H.J. and Gambel, D.W. (1995) "Security engineering", in Abrams, M.D., Jajodia, S. and Podell, H.J. (Eds.), *Information Security - an Integrated Collection of Essays*, IEEE Computer Society Press, Los Alamitos, California.

ABS (1999) (Australian Bureau of Statistics) *8129.0 - Business Use of Information Technology, Australia, 1997-98*, http://www.abs.gov.au/ (accessed October 18 1999).

ACCC (1997) *The global enforcement challenge: enforcement of consumer protection laws in a global marketplace*, Australian Competition and Consumer Commission, Canberra, Australia.

ACLU (1997) *Supreme Court Rules: Cyberspace Will be Free! ACLU Hails victory in Internet Censorship Challenge*, ACLU Press Release, June 26, http://www.aclu.org/news/n062697a.html (accessed April 6 1998).

Adams, A. and Sasse, M.A. (1999) "Users are not the Enemy", *CACM*, Vol. 42, No. 12, December.

AGD (Attorney General's Department) (1999a) *Electronic Transactions Act passed by Parliament 25 November 1999*, Information Section, Attorney-General's Department, Canberra, Australia, http://law.gov.au/publications/ecommerce/interim3.html (accessed January 8 2000).

AGD (1999b) *A privacy scheme for the private sector: Release of Key Provisions*, December 14, http://law.gov.au/privacy/finalrelease.rtf (accessed January 15 2000).

AGD (1999c) *Broadcasting Services Amendment (Online Services) Act 1999*, Attorney General's Department, Canberra, Australia.

AGD (1999d) *Summary of the Electronic Transactions Act 1999*, Attorney General's Department, Canberra, Australia, http://law.gov.au/publications/ecommerce/ETactsummary.html (accessed January 23 2000).

Agre, P.E. and Rotenberg, M. (1997) *Technology and Privacy: the New Landscape*, MIT Press.

Aldridge, A., White, M. and Forcht, K. (1997) "Security considerations of doing business on the Internet: cautions to be considered", *Internet Research: Electronic Networking Applications and Policy*, Vol. 7, No. 1.

ALIA (2000) *ALIA National Office Acceptable Usage Policy*, ALIA National Office, www.alia.org.au/staff/usage.policy.html (not accessible online by unauthorised users, due to confidential nature of the document).

Allison, L. (1998) "Personal email in the workplace", Private Communication, March 12.

Alston, R. (1997) *National framework for online content regulation*, http://www.dca.gov.au/nsapi-graphics/?MIval=dca_dispdoc&ID=366 (accessed August 10 1999).

Anon (1996) "Risks of anonymity", *CACM*, Vol. 39, No. 12, December.

AntiFraud.com (1998) *AntiFraud.com*, http://www.antifraud.com/ (accessed January 16 2000).

AP (1999) *Hackers Break in to AP Web Site*, http://www.washingtonpost.com/wp-srv/aponline/19991031/aponline164929_000.htm (accessed March 10 2000).

Arnott, D. and Shanks, G. (1993) *Information Systems as a Discipline,* Working Paper 5/93, School of Information Management and Systems, Monash University, Melbourne, Australia.

Asenjo, P.B. (1997) "Key ethical concepts for the Internet and for ethical codes of computer professionals", *Australian Computer Journal*, Vol. 29, No. 1, February.

Ashton-Davies (1997) "Trusted staff blamed for cyber crime", *The Australian*, December 16, pp. 29.

Attaran, M. and VanLaar, I. (1999) "Privacy and security on the Internet: how to secure your personal information and company data", *Information Management & Computer Security*, Vol. 7, No. 5.

Baker, C.R. (1999) "An analysis of fraud on the Internet", *Internet Research*, Vol. 9, No. 5.

Baker & McKenzie (1999) *Intellectual Property Law Newsletter*, August, UK, http://www.bakerinfo.com/Publications/Documents/1038_tx.html (accessed October 15 1999).

Barker, G. and Gettler, L. (2000) “E-mail privacy shock”, *The Age*, February 25.

Barker, R.M., Karcher, J.N. and Meade, N.L. (1995) "E-mail issues", *Internal Auditor*.

Baskerville, R. (1988) *Designing Information Systems Security*, John Wiley.

Baskerville, R. (1994) "Research directions in information systems", *International Journal of Information Management*, Vol. 14, No. 5.

Baskerville, R. (1997) "New organisational forms for information security management", in Yngstrom, Y. and Carlsen, J. (Eds.), *Information Security in Research and Business - Proceedings 13th International Conference on Information Security (SEC'97)*, IFIP, Denmark, Chapman & Hall.

Baskerville, R. and Smithson, S. (1995) "Information technology and new organisational forms: choosing chaos over panaceas", *European Journal of Information Systems*, Vol. 4.

Bayuk, J. L. (1996) "Security through process management", in *Proceedings Nineteenth National Information Systems Security Conference*, Baltimore, U.S.

BCG (1997) *eTrust Internet Privacy Study*, Boston Consulting Group, http://www.etrust.org/news/bcg/index.html (accessed September 17 1997).

Beeson, A. Rose, L. and Volokh, E. (1998) “After the Communications Decency Act decision”, *CFP98 - Eighth Annual Conference on Computers, Freedom and Privacy*, http://www.cfp98.org/ (accessed March 12 1998).

Beker, H. (1994) "Security research for the financial sector", in *Proceedings Third European Symposium on Research in Computer Security*, Brighton, UK.

Bellovin, S. (1997) "Stock-market overloads", *Risks-forum Digest*, Vol. 19, No. 44.

Benassi, P. (1999) “TRUSTe: an Online Privacy Seal Program”, *CACM*, Vol. 42, No. 2, February.

Benbasat, I., Goldstein, D.K. and Mead, M. (1987) "The case research strategy in studies of information systems", *MIS Quarterly*, Vol. 11, No. 3, September.

Benbasat, I. and Zmud, R.W. (1999) "Empirical Research in Information Systems: The Practice of Relevance", *MIS Quarterly*, Vol. 23, No. 1, March.

Benjamin, R., Gladman, B. and Randell, B. (1998) “Protecting IT Systems From Cyber Crime”, *The Computer Journal*, Vol. 41, No. 7.

Berman, J. and Weitzner, D.J. (1997) "Directing policy-making beyond the net's metaphor", *CACM*, Vol. 40, No. 2, February.

Bernstein, T., Bhimani, A.B., Schultz, E. and Siegel, C.A. (1996) *Internet Security for Business*, John Wiley & Sons, Inc.

Bhimani, A. (1996) "Securing the commercial Internet", *CACM*, Vol. 39, No. 6, June.

Bjorn-Andersen, N. (1985) "IS research - a doubtful science", in Mumford, E., Hirschheim, R.A., Fitzgerald, G. and Wood-Harper, A.T. (Eds.), *Research Methods in Information Systems*, North-Holland, Amsterdam.

Blili, S. and Raymond, L. (1993) "Information technology: threats and opportunities for small and medium-sized enterprises", *International Journal of Information Management*, Vol. 13.

Bloch, M., Pigneur, Y. and Segev, A. (1996) "Leveraging electronic commerce for competitive advantage: a business value framework", in Swatman, P.M.C., Gricar, J. and Novak, J. (Eds.), *Electronic Commerce for Trade Efficiency and Effectiveness — Proceedings of the Ninth International Conference on EDI-IOS*, Bled, Slovenia, June 10-12, Moderna Organizacija Kranj, Slovenia.

Bloustein, E.J. (1964) "Privacy as an aspect of human dignity: an answer to Dean Prosser", *39NYU Law Review*, 962, p. 1001.

Boar, B.H. (1994) *Practical Steps for Aligning Information Technology With Business Strategies: How to Achieve a Competitive Advantage*, John Wiley & Sons, N.Y., U.S.

Bonoma, T.V. (1985) "Case research in marketing: opportunities, problems and a process", *Journal of Marketing Research*, Vol. 22, May, pp.199-208.

Borenstein, N.S. (1996) “Perils and pitfalls of practical cyb”, *CACM*, Vol. 39, No. 6, June.

Branigin, W. (1991) "Australia to try computer hacker accused of damaging NASA network", *The Washington Post*, August 15, p. A31.

Branstad, D., Oldehoff, A., Aiken, R. *et al.* (1995) *Security Policy for Use of the National Research and Education Network*, in FNC (1995a), Appendix 4.

Branton, P. (1997) "Man accused of being UK's first Internet pirate", *Computer Weekly*, October 30, p. 2.

Broadbent, M., Butler, C., Hansell, A. and Dampney, C.N.G. (1995) "Business value, quality and partnerships: Australasian information systems management issues", *Australian Computer Journal*, Vol. 27, No. 1, February.

Brockway, D.W. (1996) "Knowledge technologies and business alignment", *Information Management & Computer Security*,Vol. 4, No. 1.

Brunker, M. (2000) "Vast online credit card theft revealed", *MSNBC*, March 19, http://www.msnbc.com/news/382561.asp?cp1=1 (accessed March 19 2000).

Brunnstein, K. (1997) "Towards a holistic view of enterprise information and communication technologies: Adapting to a changing paradigm", in Yngstrom, Y. and Carlsen, J. (Eds.), *Information Security in Research and Business - Proceedings 13th International Conference on Information Security (SEC'97)*, IFIP, Denmark, Chapman & Hall.

Bryan, J. (1995) "Build a firewall", *Byte*, April, pp. 991-996.

Carson, A. (2000a) "Work e-mail ruling a victory for free speech", *The Age*, April 8.

Carson, A. (2000b) "Workers axed for abuse of e-mail", *The Age*, March 22.

Carson, A. and Farrant, D. (2000) "Saving Private email", *The Age,* March 4.

Carvajal, D. (2000) "Internet Shows Signs of Becoming Top Marketplace in the Book Business", *New York Times*, January 10, http://www.nytimes.com/library/tech/00/01/biztech/articles/10book.html (accessed January 10 2000).

Cash, J.I. and Lawrence, P.R. (1989) *The Information Systems Research Challenge*: *Qualitative Research Methods. 1,* Boston, Massachusetts: Harvard Business School.

Cavazos, E.A. and Morin, G. (1994) *Cyberspace and the Law: Your Rights and Duties in the On-Line World*, MIT Press.

Chapman, B. and Zwicky, E.D. (1995) *Building Internet Firewalls*, O'Reilly & Associates.

Chartwell Bass (1998) *Methods & Applications, Focus Groups, Market Research & New Product Development*, http://chartwellbass.com/consulting/innovative.html (accessed June 1 1998).

Cheswick, W. and Bellovin, S. (2000) *Firewalls and Internet Security: Repelling the Wily Hacker*, Ed. 2, Addison-Wesley Publishing Company, Massachusetts, U.S.

Chua, W.F. (1986) "Radical Developments in Accounting Thought," *The Accounting Review*, Vol. 61.

Cifuentes, C. and Fitzgerald, A. (1997) "Copyright in shareware programs distributed on the Internet", *Australian Computer Journal*, Vol. 29, No. 1, February.

Citibank (2000) *Citibank Privacy Policy*, http://www.citibank.com/privacy/ (accessed January 15 2000).

Clarke, R. (1999) "Internet Privacy Concerns Confirm the Case for Regulation", *Communications of the ACM*, Vol. 42, No. 2, February.

Clarke, R. (2000) *Submission to the Commonwealth Attorney-General Re: 'A privacy scheme for the private sector: Release of Key Provisions' of 14 December 1999*, http://www.anu.edu.au/people/Roger.Clarke/DV/PAPSSub0001.html (accessed January 18 2000).

Clausing, J. (2000) "White House Eases Rules on Encryption Exports", *NYTimes*, January 12, http://www.nytimes.com/library/tech/00/01/cyber/articles/12encrypt.html (accessed January 13 2000).

CNN (1999) "Hackers retaliate by invading FBI, Senate, Web sites", *CNN*, May 28, http://www.cnn.com/TECH/computing/9905/28/senate.hackers/
(accessed January 18 2000).

CNN (2000) "Instant messaging account linked to 'ILOVEYOU' virus", *CNN*, May 7, http://www.cnn.com/2000/TECH/computing/05/07/iloveyou.02/index.html

CNNfn (1998) "Internet robber sentenced", *CNNfn*, February 24,
http://cnnfn.com/digitaljam/9802/24/robber/ (accessed March 4 1998).

Cochrane, N. (1998) "Visa defends banks", *The Age*, June 2, Melbourne, Australia.

Cockburn, C. and Wilson, T.D. (1996) "Business use of the world-wide web", *International Journal of Information Management*, Vol. 16, No. 2.

Condon, J.C. and Yousef, F. (1985), *An Introduction to Intercultural Communication*, MacMillan.

Cooper, C. (1997) “Cyber commerce: one step back, two steps forward”, *ZDNET News channel*, http://www5.zdnet.com/zdnn/content/zdnn/0523/zdnn0014.html (accessed September 17 1997).

Cooper, L.K., Duncan, D.J. and Whetstone, J. (1996) "Is electronic commerce ready for the Internet?", *Information Systems Management*, Summer.

Credit Control (1998) “Concerns over Internet security”, *Credit Control*, Vol. 19, Issue 11/12.

Crocker, S. (1997) "Major security flaw in CyberCash 2.1.2", *Risks-forum Digest*, Vol. 19, No. 47.

Cronin, B., Overfelt, K., Fouchereauz, K., Manzvanzvike, T., Cha, M. and Sona, E. (1994) "The Internet and competitive intelligence: a survey of current practice", *International Journal of Information Management*, Vol. 14.

CSI (Computer Security Institute) (1997a) *Computer crime continues to increase, reported losses total over $100 million*, CSI Special Report, CSI, March 6, San Francisco, U.S., http://www.gocsi.com/preleas2.htm (accessed September 1 1997).

CSI (Computer Security Institute) (1997b) *Salgado case reveals darkside of electronic commerce*, CSI Special Report, CSI, August 25, San Francisco, U.S.,
http://www.gocsi.com/preleas4.htm (accessed September 1 1997).

CSI (Computer Security Institute) (1999a) *Cyber attacks rise from outside and inside corporations: Dramatic increase in reports to law enforcement*, CSI Special Report, CSI, March 5, San Francisco, U.S., http://www.gocsi.com/prelea990301.htm (accessed January 10, 2000).

CSI (Computer Security Institute) (1999b*) Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey*, CSI, San Francisco, USA.

CSI (Computer Security Institute) (2000*) Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey*, CSI, San Francisco, USA.

Daley, W.M. and Irving, L. (1997) *Privacy and Self-Regulation in the Information Age*, U.S. Department of Commerce,
http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm (accessed March 25 1998).
D'Alotto, L.J. (1996) "Internet firewalls policy development and technology choices", *Proceedings of 19th National Information Systems Security Conference*, Baltimore, MD, U.S.

Davis, D. (1998) "International Aspects of the Internet", *Journal of IS Audit & Control*, Vol. III.

Decision Analyst (1998) *Qualitative Research*,
http://www.decisionanalyst.com/qualitat.htm (accessed June 1 1998).

Del Torto, D., Castagnoli, C., Daniel, H., Shipley, P. and Green, L. (1998) "Net Hacks and Defenses", *CFP98 - Eighth Annual Conference on Computers, Freedom and Privacy*, http://www.cfp98.org/ (accessed March 15 1998).

Denning, D.E. (1996) *Protection and defense of intrusion*,
http://guru.cosc.georgetown.edu/~denning/infosec/USAFA.html (accessed March 6 1998).

Denning, D.E. and Denning, P.J. (1998) *Internet Besieged: Countering Cyberspace Scofflaws*, Addison Wesley, Reading, Massachusetts.

Denning, P.J. (1993) "A world lit by flame", *CACM*, Vol. 36, No. 12.

De Zwart. M. (1997) "Electronic piracy", *The Monash Alumni*, October, Monash University, Melbourne, Australia.

Dinnie, G. (1999) "The Second Annual Global Information Security Survey", *Information Management & Computer Security*, Vol. 7, No. 3.

Doddrell, G.R. (1995) "Information security and the Internet", *Information Management & Computer Security*, Vol. 3, No. 4.

Drake, D. and Morse, K.L. (1996) "Applying the eight-stage risk assessment methodology to firewalls", *Proceedings Nineteenth National Information Systems Security Conference*, Baltimore, U.S.

EC (1995) "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal of the European Communities*, November 23, No. L. 281, http://www2.echo.lu/legal/en/.

ECLab (1998) *Labnews January - February 1998*, European Commission Legal Advisory Board, Chapter 7, http://www2.echo.lu/legal/en/news/9802/Chapter7.html#1
(accessed March 25 1998).

EC (European Commission) (1997) *European Initiative in Electronic Commerce*, *Communication to the European Parliament, the Council, the Economic and Social Committee of the Regions,* April 15.

Edupage Editors (1997) "New Internet law attacks non-profit pirating", *Risks-forum Digest*, Vol. 19, No. 52.

Edwards, J. (1996) "A sure, secure thing", *CIO*, July.

Eisenberg, T., Gries, D., Hartmanis, J., Holcomb, D., Stuart Lynn, M. and Santoro, T. (1989) "The Cornell commission: on Morris and the worm", *CACM*, Vol. 32, No. 6.

Ekenberk, L. and Danielson, M. (1995) "Handling imprecise information in risk management", in Eloff, J.H.P. and Von Solms, H.S., (Eds.), *Information Security - the Next Decade, IFIP/Sec '95*, *Proc. of the IFIP TC11 Eleventh International Conference on Information Security*, Chapman & Hall.

Electronic Commerce Working Group (1999) *Towards Digital e-Quality*, The White House, U.S., http://www.ecommerce.gov/ecomrce.pdf (accessed January 10 2000).

Ellison, C. and Schneier, B. (2000) “Risks of PKI: E-Commerce”, *CACM*, Vol. 43, No. 2, February.

EPIC (1997a) *Surfer Beware: Personal Privacy and the Internet*, Electronic Privacy Information Center, Washington, U.S., http://www.epic.org/reports/surfer-beware.html, (acccessed September 10 1997).

EPIC (1997b) “Groups Establish Internet Free Expression Alliance”, *EPIC Alert*, Vol. 1, No. 16.

EPIC (1997c) “Survey Shows Internet Users Want Privacy Laws”, *EPIC Alert*, Vol. 4, No.17.

EPIC (1997d) “Court Rules AOL Not Liable for Posted Material”, *EPIC Alert*, Vol. 4, No. 16.

EPIC (1997e) “Global Coalition Urges Rejection of PICS”, *EPIC Alert*, Vol. 4, No. 17.

EPIC (1998a) “New BW/Harris Poll Shows Support for Privacy Legislation”, *EPIC Alert*, Vol. 5, No. 3.

EPIC (1998b) “State Department Releases World Human Rights Report”, *EPIC Alert*, Vol. 5, No. 2.

EPIC (1999) “Report Slams Privacy Policies; Poll Finds Privacy is Top Concern”, *Epic Alert*, Vol. 5, No. 15.

Erickson, J. (1996) “Junk Mailers Discover the Internet”, *The New York Times Syndicate*, June 25.

Ernst & Young (1996) "The Ernst & Young international information security survey 1995", *Information Management & Computer Security*, Vol. 4, No. 4.

Feher, A. and Towell, E. (1997) "Business use of the Internet", *Internet Research*, Vol. 7, No. 3.

Fennelly, C. (1999) “Wizard’s Guide to Security”, *SunWorld*, December, http://www.idg.net/go.cgi?id=206917 (accessed April 23 2000).

Fink, K., Griese, J., Roithmayr, F. and Sieber, P. (1997) "Business on the Internet - some (r)evolutionary perspectives", in Vogel, D.R., Gricar, J. and Novak, J. (Eds.), *Proceedings of Tenth International Bled Electronic Commerce Conference*, Bled, Slovenia.

Finucane, M. (2000) “Student Faces Government Hacking Charges”, *Yahoo! News*, http://dailynews.yahoo.com/h/ap/20000224/sc/nasa_hacker_3.html (accessed February 24 2000).

FNC (Federal Networking Council) (1995a) *FEDERAL INTERNET SECURITY - A Framework for Action - Draft*, Federal Networking Council, Security Working Group, U.S.

FNC (Federal Networking Council) (1995b) *Federal Internet Security Plan (FISP)*. Federal Networking Council, Security Working Group, U.S.

FNC (Federal Networking Council) (1996) *Proceedings Internet Privacy and Security Workshop*, Mass.

Forcht, K., Saunders Thomas, D., Usry, M.L. and Egan, K. (1997) "Control of the Internet", *Information Management & Computer Security*, Vol. 5, No. 1.

Ford, W. and Baum, M. (1997) *Secure Electronic Commerce*, Prentice Hall, Upper Saddle River, N.J.

Foroughi, A. and Perkins, W.C. (1996) "Ensuring Internet security", *Journal of Computer Information Systems*, Vol. XXXVII, No. 1.

Foster, W. (1997) "Copyright: Internet service provider rights and responsibilities", in *Proceedings INET97, ISOC, http://info.isoc.org/inet97/proceedings/B1/B1_2.* (accessed March 2 1998).

Freehill, Hollingdale & Page (2000) *Freehills Internet Privacy Survey*, Freehill, Hollingdale & Page, Melbourne, Australia.

Fried, L. (1995) *Managing Information Technology in Turbulent Times*, New York: Wiley.

FTC (1998) *Privacy Online, a Report to Congress*, U.S. Federal Trade Commission, http://www.ftc.gov/reports/privacy3/ (accessed September 18 1999).

FTC (1999a) *Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress*, July, http://www.ftc.gov/os/1999/9907/privacy99.pdf (accessed September 15 1999).

FTC (1999b) *FTC Establishes Advisory Committee on Online Access and Security*, U.S. Federal Trade Commisssion, Press Release, December 16, http://www.ftc.gov/opa/1999/9912/accesssectf.htm (accessed January 12 2000).

Furnell, S. M. and Karweni, T. (1999) "Security implications of electronic commerce: a survey of consumers and businesses", *Internet Research,* Vol. 9, No. 5.

Furnell, S.M. and Warren, M. (1999) "Computer Hacking and CyberTerrorism: The real threats in the new millenium?", *Computers & Security*, Vol. 18, No. 1.

Gallegos, F. (1998) "Security and Control Concerns: Digital Money", *IS Audit & Control*, Vol. III.

Galliers, R.D. (Ed.) (1992) *Information Systems Research: Issues, Methods and Practical Guidelines*, Blackwell Scientific Publications, Oxford.

Galliers, R.D. (1991) "Choosing information systems research approaches" in Nissen, H.E., Klein, H.K. and Hirschheim, R. (Eds.) *Information Systems Research: Contemporary Approaches and Emergent Traditions*, Proc. IFIP TC8/WG8.2 Working Conference, December 1990, North-Holland.

GAO (General Accounting Office) (1996) *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,* U.S. General Accounting Office, May, GAO/AIMD-96-84, U.S.

GAO (1998) *Executive Guide Information Security Management*, U.S. General Accounting Office, May, U.S.

Garceau, L., Matos, V. and Santosh, K.M. (1998) "The Use of Electronic Money in Electronic Commerce Transactions", *IS Audit & Control*, Vol. III.

Garcia, D.L. (1997) "Networked commerce: public policy issues in a deregulated communication environment", *The Information Society*, Vol. 13.

Garfinkel, S. and Spafford, G. (1997) *Web Security and Commerce*, O'Reilly and Associates, U.S.

Garfinkel, S. (1997) "Problems with AOL", *Risks-forum Digest*, Vol. 19, No. 47.

Gartner Group (2000), *GartnerGroup Forecasts Worldwide Business-to-Business E-Commerce to Reach $7.29 Trillion in 2004*, http://www.gartnerweb.com/public/static/aboutgg/pressrel/pr012600c.html (accessed March 31 2000).

Gaskin, J.E. (1998) "Internet acceptable usage policies", *Information Systems Management*, Vol. 15, No. 2, Spring.

Gassman, B. (1998) *Internet Appropriate Use Policy Guidelines*, Gartner Group, Connecticut, U.S.

Ghosh, A.K. (1998) *E-Commerce Security: Weak Links, Best Defenses,* John Wiley & Sons.

Giglio, C. (1998) "Avoid getting tangled on the Web by creating an Internet usage policy", *Infoworld*, Vol. 20, No. 41, October 12.

Godwin, M. (1998) "Free speech, the constitution, and privacy in Cyberspace", *CFP98 - Eighth Annual Conference on Computers, Freedom and Privacy*, http://www.cfp98.org/ (accessed March 12 1998).

Gray, P. (1996) "The global information infrastructure", *Information Systems Management*, Summer.

Greene, T. C. (2000) "Janet Reno proposes online police squad", *The Register*, January 12, http://www.theregister.co.uk/000112-000016.html (accessed January 15 2000).

Griffiths, D. (1996) "Internet firewall policy", *Proceedings EDPAC 96*, Perth, Australia.

Guardian (2000) "ISP pays in UK libel case", *The Age*, April 4, Melbourne Australia.

Guttman, B. and Bagwill, R. (1997) *Internet Security Policy: a Technical Guide*, NIST, Special Publication 800-XXX, http://csrc.nist.gov/isptg/html/ (accessed March 10 1999).

GVU (1998) *GVU's 10th WWW User Survey,* Graphic, Visualization and Usability Center, Georgia Tech, Atlanta, Georgia, http://www.gvu.gatech.edu/user_surveys/survey-1998-10/

(accessed February 12 2000).

Hartmann, A. (1995) "Comprehensive information technology security": a new approach to respond ethical and social issues surrounding information security in the 21st Century, in Eloff, J.H.P. and Von Solms, H.S. (Eds.), *Information Security - the Next Decade, IFIP/Sec '95*, *Proc. of the IFIP TC11 Eleventh International Conference on Information Security,* Chapman & Hall.

Hasan, H. and Tibbits, H. (1999) "Multiple Perspectives on Electronic Business: A Case Study of a Financial Planning Service", *Proceedings of ACIS99*, Wellington, New Zealand.

Heard, F.T. (1996) "Internet security policies and Internet appropriate use policies", in *Proceedings of EDPAC 96 Conference*, Perth, Australia.

Highland, H.H. (1996) "Random bits and bytes", *Computers & Security*, Vol. 15, No. 1.

Hilvert, J. (1996) "Private lies", *The Information Age*, May.

Hinde, S. (1998) "CyberWars and other threats", *Computers & Security*, Vol. 17, No. 2.

Hitchings, J. (1995) “Achieving an integrated design: the way forward for information security”, in Eloff, J.H.P. and Von Solms, H.S. (Eds.), *Information Security - the Next Decade, IFIP/Sec '95*, *Proc. of the IFIP TC11 Eleventh International Conference on Information Security,* Chapman & Hall.

Hitt, L.M. and Brynjolfsson, E. (1996) "Productivity, business profitability, and consumer surplus: three different measures of information technology value", *MIS Quarterly*, Vol. 20, No. 2, June.

Hoffman, D.L., Novak, T.P. and Chatterjee, P. (1995) "Commercial scenarios for the web: opportunities and challenges", *Journal of Computer-Mediated Communication*, Vol. 1, No. 3.

Hoffman, D.L., Novak, T.P. and Peralta, M. (1999) “Building Consumer Trust Online”, *Communications of the ACM*, Vol. 42, No. 4, April.

Hogan, J.M. and James, P.C. (1997) "Australian approaches to Internet content regulation", *Australian Computer Journal*, Vol. 29, No. 1, February.

Horning, R., Schollenberger, D., Kahn, D.P. and Wong, W. (1998) “International crypto”, *CFP98 - Eighth Annual Conference on Computers, Freedom and Privacy*, http://www.cfp98.org/ (accessed March 14 1998).

Hsieh, C., Schubert, S. and Lin, E. (1996) “Potential risks of Internet access and some management strategies”, *Journal of Computer Information Systems*, Fall.

Hudoklin, A. and Stadler, A. (1997) "Security and privacy in electronic commerce", in Vogel, D.R., Gricar, J. and Novak, J. (Eds.), *Proceedings of Tenth International Bled Electronic Commerce Conference*, Bled, Slovenia.

Hughes, G. and Ryle, G. (1997) "1200 on secret police list", *The Age*, Year No. 44, Issue 404, October 7.

IDC (1997) *Study by International Development Corporation*, September 1997, in "Net used by millions", *The Age*, No. 44, Issue 404, October 7.

Identity withheld (1998) "Yes, Virginia, no classified information is ever leaked", *Risks-forum Digest*, Vol. 19, No. 70.

IETF (1991) *Site Security Handbook* (Holbrook P. and Reynolds, J. (Eds.), IETF RFC 1244.

IFW (1999a) *Internet Fraud Watch*, http://www.fraud.org/internet/intset.htm (accessed January 15 2000).

IFW (1999b) *Going once, going twice...scammed!*, Internet Fraud Watch, February 23, http://www.fraud.org/internet/9923stat.htm (accessed January 15 2000).

IITF (1996) *A Framework for Global Electronic Commerce — Executive Summary*, Information Infrastructure Task Force, U.S.
http://www.iitf.nist.gov/eleccomm/execsu.htm, December 11 (accessed October 7 1997).

Internet Security Survey Results (1996)
http://guide p.infoseek.com/www/ns/tables/Btitles?qt=Internet+security+col=WWWS
st=10 (accessed January 15 1997).

Interstar (1999) *Interstar Communications Acceptable Usage Policy*,
http://www.intrstar.net/policy/abuse.html (accessed February 24 2000).

ITA (1999) *International Safe Harbor Privacy Principles*, International Trade Administration, http://www.ita.doc.gov/td/ecom/shprin.html (accessed January 21 2000).

Jackson, M. (1998) “Keeping Secrets: International developments to protect undisclosed business information and trade secrets”, *Information Communication and Society*, Vol. 1, No. 4, Winter.

Janal, D. (1998) *Risky Business: Protect Your Business from being Stalked, Conned or Blackmailed on the Web*, John Wiley & Sons.

Jonsson (1991), *Action Research*, IFIP, Elsevier Science Publishers.

Kabay, M.E. (1999) "1999 Year-in-Review", *Information Security Magazine*, December, ICSA, http://www.infosecuritymag.com/ (accessed January 20 2000).

Kalakota, R. and Whinston, A.B. (1996) *Electronic Commerce: A Manager's Guide*, Addison-Wesley.

Kaspersen, H. (1992) "Security measures, standardisation and the law", in Aiken, R. (Ed.), *INFORMATION PROCESSING 92 - Proceedings of the IFIP 12th World Computer Congress*.

Kaye, R. and Little, S.E. (1996) "Global business and cross-cultural information systems", *Information Technology & People*, Vol. 9, No. 3.

Kennedy, D. (1997) "US DoD Break-in Statistic", *Risks-forum Digest*, Vol. 19, Issue 43.

Khare, R. and Rifkin, A. (1997) "Weaving a web of trust", *World Wide Web Journal*, Vol. 2, No. 3, Summer, O'Reilly, U.S.

King, W., Hufnagel, E. and Grover, V. (1988) "Using information technology for competitive advantage", in Earl, M. (Ed.), *Information Management: the Strategic Dimension*, Clarendon Press, Oxford, UK.

Klein, H. K. and Myers, M.D. (1999) "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly*, Vol. 23, No. 1, March.

Klein, H.K., Nissen, H.E. and Hirschheim, R. (Eds.) (1991a) *Information Systems Research: Contemporary Approaches and Emergent Traditions*, Proc. IFIP TC8/WG8.2 Working Conference, December 1990, North-Holland.

Klein, H.K., Nissen, H.E. and Hirschheim, R. (Eds.) (1991b) "A pluralist perspective of the information systems research arena", in *Information Systems Research: Contemporary Approaches and Emergent Traditions*, Proc. IFIP TC8/WG8.2 Working Conference, December 1990, North-Holland.

Koerner, B.I. (1999) "Can hackers be stopped*?"*, *U.S. News Online*, http://www.usnews.com/usnews/issue/990614/14hack.htm (accessed August 14 1999).

Kohl, U. (1995) "From social requirements to technical solutions - bridging the gap with user-oriented data security", in Eloff, J.H.P. and Von Solms, H.S., (Eds.), *Information Security - the Next Decade, IFIP/Sec '95*, *Proc. of the IFIP TC11 Eleventh International Conference on Information Security*, Chapman & Hall.

Kovacich, G. (1998) "Electronic-Internet business and security", *Computers & Security*, Vol. 17, No. 2.

KPMG Forensic Accounting (1998) "Internet abuse – the hazards of e", *Fighting Fraud*, No. 8, November, KPMG Forensic Accounting, UK.

Krebs, B. (2000) "Cybersecurity or Bust: The Auditors Cometh", *Ecommerce Times*, April 11, http://www.ecommercetimes.com/news/articles2000/000411-nb2.shtml (accessed April 12 2000).

Kwok, L. (1997) "Code of practice: a standard for information security", in Yngstrom, Y. and Carlsen, J. (Eds.), *Information Security in Research and Business - Proceedings 13th International Conference on Information Security (SEC'97)*, IFIP, Denmark, Chapman & Hall.

Kyas, O. (1997) *Internet Security*, International Thomson Computer Press.

Landau, S. *et al*. (1994) *Codes, Keys and Conflicts: Issues in U.S. Crypto Policy*, Report of Special Panel of the ACM U.S. Public Policy Committee (USACM), June, http://info.acm.org/reports/acm_crypto_study.html (accessed March 14 1998).

Lau, T., Etzioni, O. and Weld, D.S. (1999) "Privacy Interfaces for Information Management", *CACM*, Vol. 42, No. 10, October.

Lawrence, E., Murry, J. and Tidwell, A. (1996) "Cyberpresence strategies for business executives" in *Proceedings AUSWEB 96*, Australia.

Lawrence, M. (1997) "The anthropology of software theft", *The Age*, Year No. 44, Issue 404, October 7.

Lee, A.S., Liebenau, J., and DeGross, J.I. (Eds.) (1997) *Information Systems and Qualitative Research*, Chapman and Hall, London.

Lee, G.B. (1996) "Addressing anonymous messages in cyberspace", *Journal of Computer Mediated Communication*, Vol. 2, No. 1.

Lichtenstein, S. (1995a) "Information system security for adaptive organisations", *Proceedings 6th Australian Conference on Information Systems*, School of Information Systems, Curtin University of Technology, Perth, Australia.

Lichtenstein, S. (1995b) "Information system security design principles for adaptive organisations", *Proceedings EDPAC 95 Conference*, Melbourne, Australia.

Lichtenstein, S. (1996a) "Internet acceptable usage policy", *Computer Audit Update*, December, Elsevier Advanced Technology, UK.

Lichtenstein, S. (1996b) *Internet acceptable usage policy: human issues*, Working Paper 10/96, School of Information Management and Systems, Monash University, Melbourne, Australia.

Lichtenstein, S. (1996c) "Internet security policy: a holistic and organisational approach", *2nd Joint Conference Proceedings AUUG 96/APWWW Conference,* Bossomaier, T. and Chubb, L. (Eds.), AUUG'96 and Asia Pacific World Wide Web, World Congress Centre, Melbourne, Australia.

Lichtenstein, S. (1996d) *Information security principles: a holistic view*, Working Paper 3/96, School of Information Management and Systems, Monash University, Melbourne, Australia.
(also provisionally accepted by journal: *Computers & Security*, UK)

Lichtenstein, S. (1996e) "Information security design principles for adaptive organisations", *Computer Audit Update*, June, Elsevier Advanced Technology, UK.

Lichtenstein, S. (1997a) "Developing Internet security policy for organisations", in *Proceedings of the Thirtieth Annual Hawaii International Conference on Systems Sciences,* Nunamaker, J.F. and Sprague, R.H. (Eds.), Hawaii, IEEE Computer Society Press, Los Alamitos, California.

Lichtenstein, S. (1997b) "A review of information security principles", *Computer Audit Update*, December, Elsevier Advanced Technology, UK.

Lichtenstein, S. (1998) "Internet risks for companies", *Computers & Security*, Vol. 17, No. 2.

Lichtenstein, S. and Swatman, P.M.C. (1997a) "Internet acceptable usage policy for organisations", *Information Management and Computer Security*, Vol. 5, No. 5.

(also published as Lichtenstein, S. and Swatman, P.M.C. (1997) “Effective Internet acceptable usage policy for organisations”, in Vogel, D.R., Gricar, J. and Novak, J. (Eds.), *Tenth International Electronic Commerce Conference*, Bled, Slovenia.)

Lichtenstein, S. and Swatman, P.M.C. (1997b) “Internet acceptable usage policy: arguments and perils”, in Swatman, P.M.C, Swatman, P. and Cooper, J., (Eds.), *Proceedings of PAWEC’ 97*, Brisbane, Australia.

Liddy, C. (1996) "Commercial security on the Internet", *Internet Research*, Vol. 6, No. 2/3.

Litchko, J. (1999) *‘‘*“Holistic” Security: Circles, Pies, or Crystals?*’ Proceedings of 22nd National Information Systems Security Conference*, Baltimore, MD, U.S.

Logan R. (1995) *The Fifth Language*, Toronto: Stoddart.

Logan M. and Logan R. (1996) "Alignment: how to do business on the Internet", *Proceedings INET 96*, Montreal, Canada.

Loundy, M. (1998) “An introduction to copyright and trademark law”, *CFP98 - Eighth Annual Conference on Computers, Freedom and Privacy*, http://www.cfp98.org/ (accessed March 12 1998).

Loveman, G.W. (1994) "An assessment of the productivity impact on information technologies", in Allen, T.J. and Scott Morton, M.S. (Eds.), *Information Technology and the Corporation of the 1990s: Research Studies*, Oxford University Press, Oxford.

Lo Verso, J.R. (1996) "Unintentional accesses", *Risks-forum Digest*, Vol. 18, No. 57.

Markoff, J. (2000) "An Online Extortion Plot Results in Release of Credit Card Data", *New York Times*, January 10,
http://www.nytimes.com/library/tech/00/01/biztech/articles/10hack.html (accessed January 10 2000).

Marsan, C.D. (2000) “Employee study cites rampant Internet abuse*”, Network World Fusion*, http://www.cnn.com/2000/TECH/computing/04/20/work.surf.idg/index.html (accessed April 26, 2000).

Mason, R. (1986) "Four ethical issues of the information age", *MIS Quarterly*, Vol. 10, No. 1, March.

Mathieu, R.G. and Woodard, R.L. (1995) "Data integrity and the Internet: implications for management", *Information Management & Computer Security*, Vol. 3, No. 2.

McClearn, M. (2000) *‘*‘Firms wage electronic war on industrial espionage”, *Calgary Herald*, January 18, Calgary, Canada.

McMillan, R. (1996) *Site Security Policy Development*, Information Technology Services, Griffith University, Queeensland, Australia.

Mehta, R. (2000) “Secure E-Business”, *Information Systems Control Journal*, Vol 1.

Mellor, S. (1999) *Guidelines for Appropriate Internet Usage Policies for ISP Organisations*, Honours Thesis, School for Information Management and Systems, Monash University, Melbourne, Australia.

Mesenbourg, T. (1999) *Measuring Electronic Business: Definitions, Underlying Concepts, and Measurement Plans*, Census Bureau, U.S.,
http://www.ecommerce.gov/ecomnews/e-def.html (accessed January 7 1999).

META Group (1999) “Electronic Commerce Security Framework”, *META Group Inc.,* April 6, http://www.metagroup.com (accessed March 15 2000).

Miers, D. and Hutton, G. (1996) *The Strategic Challenges of Electronic Commerce*, Enix Consulting Limited, UK.

Miller, S. (1997) "Privacy and the Internet", *Australian Computer Journal*, Vol. 29, No. 1, February.

Milunovic, S. (1997a) "Hacking cost businesses $800 million worldwide", *Risks-forum Digest*, Vol. 19, No. 47.

Milunovic, S. (1997b) "Web sites open companies to computer fraud risk", *Risks-forum Digest*, Vol. 19, No. 44.

Mitton, J. (1997a) *NCSA Web Host Compliance Program significantly reduces Web hosting risks*, Computer Security Canada Incorporated,
http://www.csci.ca/whatsnew/Oct28-97.htm (accessed November 12 1997).

Mitton, J. (1997b) *Web Security Certification Prevents Rash of Banking Security Breaches*, Computer Security Canada Incorporated,
http://www.csci.ca/whatsnew/Sept22-97.htm (accessed November 12 1997).

Morgan, D.L. (1998) *Focus Groups as Qualitative Research*, Qualitative Resaerch Methods Series, Vol. 16, SAGE Publications, UK.

Moulton, M. (1998) "Reducing charges of E-comm harassment", *Computers & Security*, Vol. 17, No. 2.

Müller, G. and Rannenberg, K. (1999a) "Multilateral Security – Empowering Users, Enabling Applications – The Ladenburger Kolleg, Security in Communication Technology", in Müller, G. and Rannenberg, K. (Eds*.), Multilateral Security in Communications – Technology, Infrastructure, Economy*; Addison-Wesley-Longman, Reading, Massachusetts.

Müller, G. and Rannenberg, K. (Eds*.)* (1999b) *Multilateral Security in Communications: Technology, Infrastructure, Economy*, Addison-Wesley-Longman, Reading,
Massachusetts.

Mumford, E., Hirschheim, R.A., Fitzgerald, G. and Wood-Harper, T.A. (Eds.) (1985) *Research Methods in Information Systems*, Amsterdam: North-Holland.

Myers, M.D. (1997) "Qualitative Research in Information Systems," *MIS Quarterly*, Vol. 21, No. 2, June.

Nance, K.L. and Strohmaier, M. (1995) "Ethical Information Security in a Cross-Cultural Environment", in Eloff, J.H.P. and Von Solms, H.S. (Eds.), *Information Security - the Next Decade, IFIP/Sec '95*, *Proc. of the IFIP TC11 Eleventh International Conference on Information Security*, Chapman & Hall.

NCC (1996) *The Information Security Breaches Survey 1996*, National Computing Centre, UK.

Needham, R.M. (1994) "Denial of service: an example", *CACM*, Vol. 37, No. 11.

Needham, K. (1997) "Courier enters cyberspace with online freight service", *The Age*, Year No. 44, Issue 404, October 7.

Neely, M. (1995) "Monitoring the Internet", *Internet Australasia*, May.

Nemzow, M. (1999) "Planning for Insecurities", *Webserver Online*, January, http://webserver.cpg.com/wb/4.1/index.html (accessed February 18 1999).

NETrageous (1998) *Internet Scambusters*, Vol. 23, May 31,
http://www.scambusters.org/Scambusters23.html (accessed February 10 2000).

Neuman, W.L. (1994) *Social Research Methods: Qualitative and Quantitative Approaches*, Allyn and Bacon, Massachusetts.

Neumann, P. (1993) "Risks of surveillance", *CACM*, Vol. 36, No. 8, August.

Neumann, P. (1995) "Computer vulnerabilities:exploitation or avoidance", *CACM*, Vol. 38, No. 6, June.

Neumann, P. (1996a) "CIA disconnects home page after being hacked", *Risks-forum Digest*, Vol. 18, No. 49.

Neumann, P. (1996b) *Security Risks in the Emerging Infrastructure*, Adaptation of Senate Report, June 25, http://www.csl.sri.com/neumannSenate.html (accessed September 9 1997).

Neumann, P. (1997a) *Security Risks in Key Recovery*, Report of Senate Testimony, July, http://www.csl.sri.com/neumann/judiciary.html (accessed September 9 1997).

Neumann, P. (1997b) "Pac*Bell Internet cites sabotage for blockade", *Risks-forum Digest*, Vol. 19, No. 44.

Neumann, P. (1997c) "AOL strikes again!", *Risks-forum Digest*, Vol. 19, No. 44.

Neumann, P. (1997d) *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology*, ftp://www.csl.sri.com/pub/illustrative.PS (accessed September 10 1998).

Neumann, P. (1998a) "CyberAttack on the Pentagon", *Risks-forum Digest*, Vol. 19, No. 60.

Neumann, P. (1998b) "The Computer Anti-Defamation Law", *Risks-forum Digest*, Vol. 19, No. 64.

Neumann, P. (2000) Note associated with “Hacking credit cards is preposterously easy”, *Risks-forum Digest*, Vol. 20, No. 85.

Neumann, P. and Weinstein, L. (1999) “Risks of Content Filtering”, *Communcations of the ACM*, Vol. 42, No. 11, November.

NIIAC (1995) *Commentary on the Privacy and Related Security Principles*, Mega Project III of the National Information Infrastructure Advisory Council, U.S.

NIST (1994a) *Computer Security Policy*, Computer Systems Laboratory Bulletin, Gaithersburg, MD, U.S.

NIST (1994b) *Reducing the Risks of Internet Connection and Use*, Computer Systems Laboratory Bulletin, Gaithersburg, MD, U.S.

NIST (1996a) *The World Wide Web: Managing Security Risks*, Computer Systems Laboratory Bulletin, Gaithersburg, MD, U.S.

NIST (1996b) *Generally Accepted Principles and Practices for Securing Information Technology Systems*, (Special Pub 800-14), NIST, September, http://csrc.nist.gov.au/publications.html (accessed September 18 1997).

Noack, D. (2000) "Computer Viruses Cost $12 Billion in 1999", *APBNews*, January 20, http://www.apbnews.com/newscenter/internetcrime/2000/01/20/virus0120_01.html (accessed January 23 2000).

Nouwens, J. and Bouwman, H. (1995) "Living Apart Together In Electronic Commerce: The Use Of Information And Communication Technology To Create Network Organizations", *Journal of Computer-Mediated Communication*, Vol. 1, No. 3.

NPR (National Performance Review) (1993), *Reengineering Through Information Technology: Accompanying Report of the National Performance Review*, Office of the Vice-President, Washington, D.C.: Government Printing Office, September.

NRC (1991) *Computers at Risk. Safe Computing in the Information Age*, System Security Study Committee Computer Science and Telecommunications Board Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press.

Nucifora, A. (1997) "Focus groups offer candid feedback", *American City Business Journals*, April 14.

NYTimes (New York Times) (1999) "Man Pleads Guilty to Creating the Melissa Virus", *New York Times*, December 10, http://www.nytimes.com/ (accessed January 14 2000).

O'Connell, B.M. (1997) "Law, ethics and the Internet: finding solid ground in virtual spaces", *Australian Computer Journal*, Vol. 29, No. 1, February.

OECD (1980) *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, OECD, Paris.

OECD (1992) *Guidelines for the Security of Information Systems*, OECD/GD(92)190, Paris.

OECD (1997) *Electronic Commerce: Opportunities and Challenges for Government (`The Sacher Report')*, http://www.oecd.org/dsti/sti/it/ec/act/SACHER.htm (accessed October 10 1999).

OECD (1998) *Ministerial Declaration on the Protection of Privacy on Global Networks*, OECD, Paris.

OECD (1999) *Guidelines for Consumer Protection in the Context of Electronic Commerce*, http://www.oecd.org/dsti/sti/it/consumer/prod/guidelines.htm (accessed January 15 2000).

OED (1992) *The Shorter Oxford English Dictionary of Historical Principle,* Clarendon Press, Oxford.

Oliver, R. W. (1997) "Corporate policies for electronic commerce", in Nunamaker, J.F. and Sprague, R.H. (Eds.), *Proceedings of the Thirtieth Annual Hawaii International Conference on Systems Sciences*, Hawaii, IEEE Computer Society Press, Los Alamitos, California.

Olivier, W. and van de Haar, H. (1997) "Controlling Internet access at an educational institution", in Yngstrom, Y. and Carlsen, J. (Eds.), *Information Security in Research and Business - Proceedings 13th International Conference on Information Security (SEC'97)*, IFIP, Denmark, Chapman & Hall.

Olnes, J. (1994) "Development of security policies", *Computers & Security*, Vol. 13, No. 8.

Olson, I.M. and Abrams, M.D. (1995) "Information security policy", in Abrams, M.D., Jajodia, S. and Podell, H.J. (Eds.), *Information Security - an Integrated Collection of Essays*, IEEE Computer Society Press, Los Alamitos, California.

Orlikowski, W.J. and Baroudi, J.J. (1991) "Studying Information Technology in Organizations: Research Approaches and Assumptions", *Information Systems Research*, Vol. 2.

Overly, M.R. (1999) *E-Policy: How to Develop Computer, E-Mail, and Internet Guidelines to Protect Your Company and Its Assets*, AMACOM, New York.

Parker, C.M., Swatman, P.A., Swatman, P.M.C. and Wafula, E.N. (1994) "Information systems research methods: the technology transfer problem", *5th Australasian Conference on Information Systems,* Monash University, Melbourne, Australia.

Pathak, J.P. (2000) "Are e-mails boon or bane for organisations*?" Information Systems Control Journal*, Vol. 1.

Pattison, M. (1997) "Legal implications of doing business on the Internet", *Information Management & Computer Security*, Vol. 5, No. 1.

Pethia, R. (1999) *The Melissa Virus: Inoculating Our Information Technology from Emerging Threats*, http://www.cert.org/congressional_testimony/pethia9904.html (accessed January 21 2000).

Pethia, R., Crocker, S. and Fraser, B. (1991) *Guidelines for the Secure Operation of the Internet*, IETF RFC1281, http://www.faqs.org/rfcs/rfc1281.html (accessed May 4 1998).

Pethia, R., Paller, A. and Spafford, G. (2000*) Consensus Roadmap for Defeating Distributed Denial of Service Attacks*, Global Institute Analysis Center, SANS Institute, U.S., http://www.sans.org/ddos_roadmap.htm (accessed April 13 2000).

Pitkow, J. and Kehoe, C. (1997) *GVU's 7th WWW User Survey Online Report*, Graphic, Visualization, & Usability Center, Georgia Institute of Technology, Atlanta, U.S., http://www.gvu.gatech.edu/user_surveys/survey-1997-04/ (accessed September 11 1997).

Poon, S. and Swatman, P.M.C. (1995) "The Internet for small businesses: an enabling infrastructure for competitiveness", *Proceedings of the Fifth Internet Society Conference*, Hawaii, June.

Poon, S. and Swatman, P.M.C. (1996) "Electronic networking among small business in Australia - an exploratory study", in Swatman P.M.C., Gricar J. and Novak J. (Eds.), *Electronic Commerce for Trade Efficiency and Effectiveness — Proceedings of the Ninth International Conference on EDI-IOS*, Bled, Slovenia, June 10-12, Moderna Organizacija Kranj, Slovenia.

Porter, M.E. and Millar, V.E. (1985) "How information gives you competitive advantage", *Harvard Business Review*, July-August.

Prakash, A. (1996) "The Internet as a global strategic tool", *Information Systems Management*, Summer.

Quelch J.A. and Klein L.R. (1996) "The Internet and international marketing", *Sloan Management Review*, Spring.

Rannenberg, K. (1994) "Recent development in information technology security evaluation - the need for evaluation criteria for multilateral security", in Sizer,R., Yngstrom, L., Kaspersen, H. and Fischer-Hubner, S. (Eds.), *Proceedings, Security and Control of Information Technology in Society,* IFIP Transactions A43, Elsevier Science B.V. (North-Holland).

Rannenberg, K. Pfitzmann, A. and Müller, G. (1999) "IT Security and Multilateral Security" in Müller, G. and Rannenberg, K. (Eds*.)*, *Multilateral Security in Communications: Technology, Infrastructure, Economy*, Addison-Wesley-Longman, Reading, Massachusetts.

Reagle, J. and Cranor, L.F. (1999) "The Platform for Privacy Preferences", *CACM*, Vol. 42, No. 2, February.

Reichenbach, M., Damker, H., Fedderath, H. and Rannenberg, K. (1997) "Individual management of personal reachability in mobile communication", *in Proceedings of the IFIP TC11 13th International Information Security Conference*, Copenhagen.

Reichenbach, M. Grzebiela, T., Koltsch, T. and Pippow (2000) “Individual Risk Management for Digital Payment Systems”, *ECIS 2000 Conference Proceedings*.

Reuters (2000) *U.S. Web poll finds fear of hackers and government*, Silicon Valley News, Reuters Limited, http://www.mercurycenter.com/svtech/news/breaking/internet/docs/214580l.htm (accessed February 15 2000).

RiskWatch (1999) *The Need for Information Security Policies*, http://www.riskwatch.com/whitepaper/sec_policy_whitepaper.html (accessed March 30 2000).

Romm, C. and Sudweeks, F. (Eds) (1998) *Doing Business Electronically: a Global Perspective of Electronic Commerce*, Springer-Verlag New York.

Ross, S. (2000) “Clinton Takes Up Web Security”, *Washington Post,* February 15, http://www.washingtonpost.com/wp-srv/aponline/20000215/aponline141730_000.htm (accessed February 15 2000).

Rouse, A. and Dick, M. (1994) "The use of computerised tools in qualitative information systems studies", *5th Australasian Conference on Information Systems*, Monash University, Melbourne, Australia.

Sandberg, J. (1998) "Internet vandals pose threat by using new attack mode called 'smurfing'", *Computers & Security*, Vol. 17, No. 2.

Sanford, C.C. (1993) "Computer viruses: symptoms, remedies and preventative measures", *Journal of Computer Information Systems*, Vol. 35, No. 3, Spring.

Saunders Thomas, D., Forcht, K. A. and Counts, P. (1998) "Legal considerations of Internet use - issues to be addressed", *Internet Research*, Vol. 8, No. 1.

Scheuermann, L. and Taylor, G. (1997) "Netiquette", *Internet Research*, Vol. 7, No. 4.

Schwartau, W. (1996) "Information warfare: chaos on the electronic superhighway", *IS Audit & Control Journal*, Vol. I.

Schwartau, W. (1997) “Surviving denial-of-service on the Internet”, *Proceedings Twentieth National Information Systems Security Conference*, Baltimore, U.S.

Schwartau, W. (2000) *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption*, Thunder's Mouth Press, U.S.

Senn, J.A. (1996) "Capitalizing on electronic commerce", *Information Systems Management*, Summer.

Shanks, G., Rouse, A. and Arnott, D. (1993) *A Review of Approaches to Research and Scholarship in Information Systems*, Working Paper 3/93, School of Information Management and Systems, Monash University, Melbourne, Australia.

Sinclair, J. (1997a) "Senate committee to monitor change", *The Age*, Year No. 44, Issue 404, October 7.

Sinclair, J. (1997b) "Agency to surf Net in search of scams", *The Age*, Year No. 44, Issue 404, October 7.

Sipior, J.C. and Ward, B.T. (1995) "Legal quandary of email privacy", *CACM*, Vol. 38, No. 12.

Sipior, J.C. and Ward, B.T. (1999) "The dark side of employee email", *CACM*, Vol. 42, No. 7, July.

Siyan, K. and Hare, C. (1995) *Internet Firewalls and Network Security*, New Riders Publishing.

Smith, J.H. (1993) "Privacy policies and practices: inside the organisational maze", *CACM*, Vol. 36, No. 12, December.

SKYWRITING (1997) "eTRUST Internet privacy study results announced", *SKYWRITING*, Issue 20, April 3.

Smith, G.J.H. (1996) "Setting up a Web site - managing the legal risks", *Internet Research,* Vol. 6, No. 2/3.

Smith, C.N., Everett-Church, R. and MacKinnon, R. (1998) "Net vengeance: the law and ethics of self-help remedies for on-line harms", *CFP98 - Eighth Annual Conference on Computers, Freedom and Privacy*, http://www.cfp98.org/ (accessed March 12 1998).

Sobirey, M., Fischer-Hubner, S. and Rannenberg, K. (1997) "Pseudonymous audit for privacy-enhanced intrusion detection", in Yngstrom, Y. and Carlsen, J. (Eds.), *Information Security in Research and Business - Proceedings 13th International Conference on Information Security (SEC'97)*, IFIP, Denmark, Chapman & Hall.

Spar, D. and Bussgang, J. (1996) "Ruling the net", *Harvard Business Review*, Vol. 74, No. 3, May-June.

Spurling, P. (1995), "Promoting security awareness and commitment", *Information Management & Computer Security*, Vol. 3, No. 2.

SRI (1997) *Intrusion Detection Home Page*, SRI International, Computer Science Laboratory, Menlo Park, California, url: http://www.csl.sri.com/intrusion.html
(accessed September 9 1997).

Stanley, A.K. (1997) "Information security-challenges for the next millenium", in Yngstrom, Y. and Carlsen, J. (Eds.), *Information Security in Research and Business - Proceedings 13th International Conference on Information Security (SEC'97)*, IFIP, Denmark, Chapman & Hall.

Stout, D. (1999) "U.S.I.A Says Invader Killed Web Site and Damaged Computer", *New York Times,* January 21, http://www.nytimes.com/library/tech/99/01/biztech/articles/21hack.html (accessed September 18 1999).

Sullivan, B. (1999) "Cyberwar: the threat of chaos", *MSNBC*, August 6, http://www.msnbc.com/news/295227.asp?cp1=1 (accessed September 17 1999).

Sullivan, B. (2000) "Stealing cards easy as Web browsing", *MSNBC*, January 14, http://www.msnbc.com/news/357305.asp (accessed January 15 2000).

Sutterfield, L. and Schell, L. (1997) "Corporate information protection program: concept of operations", *Computer Security Journal*, Vol. XIII, No. 1.

Svigals, J. (1997) "SET risk", *Risks-forum Digest*, Vol. 19, Issue 31.

Tan, M. and Thompson, S. H. T. (1998) "Factors influencing the adoption of the Internet", *International Journal of Electronic Commerce*, Vol. 2, No. 3, Spring.

Taylor, D. and Resnick, R. (1995) "Better safe", *Internet World*, February.

TechLaw (2000a) *Kathleen R. v. City of Livermore*, Tech Law Journal, http://www.techlawjournal.com/courts/kathleenr/Default.htm (accessed January 16 2000).

TechLaw (2000b) *Blumenthal v. Drudge and AOL*, Tech Law Journal, http://www.techlawjournal.com/courts/drudge/Default.htm (accessed January 16 2000).

TechLaw (2000c) *Summary of Internet Privacy Bills in the 106th Congress*, Tech Law Journal, http://www.techlawjournal.com/cong106/privacy/Default.htm (accessed January 15 2000).

TechMedia (1997) "Germany approves first law in the world to regulate the Internet", in Trautman, P.S. (Ed.), *Internet Operator Europe*, Techmedia, US.

Tedeschi, B. (2000) "Government Struggles to Shed Light on Online Sales", *New York Times*, January 10, http://www.nytimes.com/library/tech/00/01/cyber/commerce/10commerce.html (accessed January 10 2000).

The Age (2000a) "Trio held over e-mail virus", *The Age*, May 9, Melbourne, Australia.

The Age (2000b) "Private Parts", in Online IT News, *The Age*, April 4, Melbourne, Australia.

The White House (1997) *A Framework for Global Electronic Commerce*, White House, U.S., July 1.

The White House (1999) *Vice President Gore Announces Efforts to Expand and Improve On-line Services*, Press Release, White House, Office of the Vice President, U.S., December 17.

Timmers, P. (1998) "Business Models for Electronic Markets", *International Journal of Electronic Markets*, July.

TIOcom (1996) *Terms and Conditions for User Access and User Services*, The Internet Outsourcing Group, April 27, http://www.tio.com/terms.html (accessed October 18 1996).

TRUSTe (1998) *TRUSTe Press Conference*, http://www.truste.org/partners/about_internetworld.html (accessed February 24 2000).

TRUSTe (1999) *Comments on the Georgetown Internet Privacy Policy Survey*, http://www.msb.edu/faculty/culnanm/GIUPS/truste.PDF (accessed February 20 2000).

TRUSTe (2000) *TRUSTe,* http://www.truste.org (accessed January 22 2000).

Turban, E., Lee, J., King, D. and Chung, H.M. (2000*) Electronic Commerce: A Managerial Perspective*, Prentice Hall.

UNCITRAL (United Nations Commission on International Trade Law) (1996*) Model Law on Electronic Commerce*, UN.

U.S. Department of Justice (2000a) *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, President's Working Group on Unlawful Conduct on the Internet, March,
http://www.usdoj.gov/criminal/cybercrime/unlawful.htm (accessed March 18 2000).

U.S. Department of Justice (2000b) *US Launches Cybercrime Web Site*,
http://www.infowar.com/law/00/law_031300a_j.shtml (accessed March 18 2000).

Vadapalli, A. and Ramamurthy, K. (1997) "Business use of the Internet: an analytical framework and exploratory case study", *International Journal of Electronic Commerce*,
Vol. 2, No. 2, Winter.

Valente, G. (1996) "Hackers, crackers and sniffers", *Internal Auditor*, October.

Vanbokkelen, J. (1990) *The Internet Oral Tradition*, IETF RFC1173.

van Heck, E. and van Bon, H. (1997), "Business value of electronic commerce case study: the expected costs and benefits of electronic commerce scenarios for a Dutch exporter", in Vogel, D.R., Gricar, J. and Novak, J. (Eds.), *Proceedings of Tenth International Bled Electronic Commerce Conference*, Bled, Slovenia.

Verisign (2000) *Verisign Internet Trust Services*, http://www.verisign.com (accessed January 21 2000).

Von Bertalanffy, L. (1956) "Main currents in modern thought", in *Yearbook of the Society for General Systems Research,* Vol. 1.

von Solms, R. (1997) "Driving safely on the information superhighway", *Information Management & Computer Security*, Vol. 5, No. 1.

Wack, J.P. and Carnahan, L.J. (1995) *Keeping Your Site Comfortably Secure: an Introduction to Internet Firewalls*, U.S. Department of Commerce, U.S.

Walsham, G. (1993) *Interpreting Information Systems in Organizations*, Wiley, Chichester.

Wang, H., Lee, M.K.O. and Wang, C. (1998), "Consumer privacy concerns about Internet marketing", *CACM,* Vol. 41, No. 3, March.

Warman, A. (1992) "Organizational computer security policy: the reality", *European Journal of Information Systems*, Vol. 1, No. 5.

Weaver, J. (1999) “Should ISPs be stopping spammers?” *MSNBC*, June 20, http://www.msnbc.com/news/280607.asp (accessed July 14 1999).

Webb, S. (2000) “Crimes and misdemeanours: how to protect corporate information in the Internet age”, *Computers & Security*, Vol. 19, No. 2.

Weisband, S.P. and Reinig, B.A. (1995) “User perceptions of email privacy”, *CACM*, Vol. 38, No. 12, December.

Welsh, M. (1998) "Update on Windows NT denial-of-service attacks", *Risks-forum Digest*, Vol. 19, No. 62.

Westphal, H. and Towell, E. (1998) "Investigating the future of Internet regulation", *Internet Research*, Vol. 8, No. 1.

Wigand, R. T. (1997) "Electronic commerce: definition, theory, and context", *The Information Society*, Vol. 13, No. 1.

Williams, D. (1998) *Agreement on National Laws for Electronic Commerce*, http://law.gov.au/aghome/agnews/1998newsag/478a_98.htm (accessed January 10 2000).
Williams, D. (2000) “Canberra to tighten safety Net”, *The Age*, April 4, Melbourne, Australia.

Wilson, M. (1996) *Marketing and Implementing Computer Security*, National Institute of Standards & Technology, Gaithersburg, MD, U.S.

Wood, C.C. (1997a) *Information Security Policies Made Easy*, Baseline Software Inc., U.S.

Wood, C.C. (1997b) *How to Handle Internet Electronic Commerce Security: Risks, Controls & Product Guide*, Baseline Software Inc., U.S.

Woodward, D. (2000) “Smart security*”, British Journal of Administrative Management*, No. 18, Jan/Feb.

www.consult (2000) *Newsletter*, January 11,
http://www.consult.com.au/index.shtml (accessed January 11 2000).

Yin, R.K. (1994) *Case Study Research: Design and Methods*, Revised Edition, Sage Publications, Newbury Park, London.

Yngstrom, L. (1995) “A holistic approach to IT security”, in Eloff, J.H.P. and Von Solms, H.S. (Eds.), *Information Security - the Next Decade, IFIP/Sec '95*, *Proc. of the IFIP TC11 Eleventh International Conference on Information Security*, Chapman & Hall.

Zakon, R.H. (2000) *Hobbes' Internet Timeline v3.1*,
http://info.isoc.org/guest/zakon/Internet/History/HIT.html (accessed January 10 2000).

Zwass, V. (1996) "Electronic commerce: structures and issues", *International Journal of Electronic Commerce*, Vol. 1, No. 1, Fall, http://www.cba.bgsu.edu/ijec/
(accessed April 4 1997).

Zwass, V. (1999) *Structure and Macro-level impacts of Electronic Commerce: From Technological Infrastructure to Electronic Marketplaces*, http://www.cba.bgsu.edu/ijec/ (accessed January 12 2000) (also in Kendall, K. (Ed.), *Emerging Information Technologies: Improving Decisions, Cooperation and Infrastructure*, Sage Publications).

Appendices
A - E

Appendix A

Internet security policy
Questionnaire for mini case A
October, 1996

INTERNET SECURITY POLICY AT MONASH UNIVERSITY

Research aim: This questionnaire is designed to assist with a research project in Internet security policy for organisations.

Participation in this project is voluntary. There is no compunction on students to participate.

Questionnaire structure: There is one section per Internet risk type. The questions are designed to assist in identifying the Internet risks that you encounter in your Internet usage at this university, and to determine whether a policy would assist in reducing these risks and improving Internet usage accordingly.

Instructions: There is one question for each possible Internet risk type.
For each question, please write a rating (0 – 10) next to the corresponding Internet risk where indicated, estimating the likelihood of that risk occurring at Monash University. Use the Likert scale below as a guide. Each question also has several parts to be completed, in which you can provide additional information about the risk type.

Likert Scale:
0 - 2 Rarely
3 - 5 Occasionally (once a month)
5 - 7 Often (once a week)
7 Once a day
8 Once an hour
9 Once every 5 minutes
10 Once a minute or more

(i) Detection of corrupted or erroneous software downloaded via the Internet (eg viruses, or programs with errors)

Likelihood --------

Has this risk happened in the past at this university? **(Yes / No)**
If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students)
(Yes / No)

If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(ii) Hacking

Likelihood --------

Has this risk happened in the past at this university? **(Yes / No)**
If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students)
(Yes / No)

If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(iii) Accidentally sending email to the wrong person(s)

Likelihood --------

Has this risk happened in the past at this university? **(Yes / No)**
If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students.)
(Yes / No)

If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(iv) Low quality data (data which a student reads is incorrect)

Likelihood --------

Has this risk happened in the past at this university? **(Yes / No)**

Tick whichever of the following have occurred, and rate its likelihood in the range 0 - 10:

- You have read inaccurate Web pages [ ] --------
- You have read inaccurate data from some organisation's database [ ] --------
- You have read inaccurate email [ ] --------
- Other [ ] ---------

If you ticked one or more of the above, please provide a brief description of *one* such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students) **(Yes / No)**

If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(v) Non-university related Internet activities

Likelihood --------

Has this risk happened in the past at this university? **(Yes / No)**
Tick whichever of the following has occurred, and rate it as a risk in the range 0 - 10
- Excessive personal email [ ] ----------
- Surfing [ ] ---------
- Downloading games and images [ ] ---------
- Newsgroups and mailing lists [ ] ---------
- Internet relay chatting [ ] ----------

If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students)
(Yes / No)
If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(vi) Accidental disclosure of information

Likelihood --------

Has this risk happened in the past at this university? **(Yes / No)**
If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students) **(Yes / No)**

If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(vii) Inappropriate email
(for example, junk email, spamming)

Likelihood --------

Has this risk happened in the past at this university? **(Yes / No)**
If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students)
(Yes / No)
If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(viii) Inaccurate advertising (eg via opinion-based email)

Likelihood --------

Has this happened in the past at this university? **(Yes / No)**

If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students)

(Yes / No)

If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(ix) Denial-of-service

(eg slowed Internet traffic)

Likelihood --------

Has this risk happened in the past at this university? **(Yes / No)**

If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students)
(Yes / No)
If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(x) Pirated software (do students pirate software via the Internet?)

Likelihood --------

Has this happened in the past at this university? **(Yes / No)**
If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students)
(Yes / No)

If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(xi) Fraud

Likelihood --------

Has this happened in the past at this university? **(Yes / No)**
If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students)
(Yes / No)

If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

(xii) Theft of information
(eg do students steal information via the Internet?)

Likelihood --------

Has this happened in the past at this university? **(Yes / No)**
If Yes, please provide a brief description of one such incidence of this risk occurring:

Would a written policy, giving students guidance to avoid or reduce this risk, help in reducing the risk? (Assume that the policy will be explained verbally to all students)
(Yes / No)

If Yes, what advice would you recommend in the policy?

If No, why wouldn't a policy help?

Appendix B

Human Issues in Internet security policy
Questionnaire for mini case B
October, 1996

HUMAN ISSUES IN INTERNET SECURITY POLICY
AT MONASH UNIVERSITY

Research aim: This questionnaire is designed to assist with a research project in Internet security policy for organisations.

Participation in this project is voluntary. There is no compunction on students to participate.

These questions are designed to assist in identifying the human issues involved in Internet usage in the workplace, and to determine how a company and its policy could address these issues.

Instructions: Imagine that you are a full-time employee in a company. In your position, you need to access the Internet for business communication and collaboration purposes. For example, you may need to use email to discuss business matters with customers and company personnel. You may need to join mailing lists which provide useful information in your area, and through which you can contribute your own views. The company has granted you Internet connection via the computer on your desk at work.

1. Internet usage

(i) How do you feel about your right to freely use the Internet at work?

For example, do you think you should be able to use the Internet freely for non-business purposes as well as business purposes all day? Do you think you should be restricted to, say, two hours per day Internet usage in total? Or some other time limit?

(ii) How many hours a day of non-business usage would you accept as reasonable, if a limit were to be imposed?

(iii) Do you believe in your right to use personal email across the Internet during work hours?
(Yes / No)

(iv) Would you do so if given the opportunity? (Yes / No)

(v) Do you believe in your right to download games and nonbusiness images across the Internet during work hours? (Yes / No)

(vi) Would you do so if given the opportunity? (Yes / No)

(vii) Do you believe in your right to have an employee home page for which you have complete freedom in its design? (Yes / No)

---

2. Internet privacy

What concerns do you have about Internet privacy?

(i) Are you concerned that your personal data may be collected by other sites? (Yes / No)

(ii) Are you concerned that you don't know what the data collected would be used for? (Yes / No)

(iii) Would you send credit card details across the Internet to a vendor site? (Yes / No)

(iv) Do you believe in your right to access sites anonymously? (Yes / No)

(v) Any other privacy concerns?

---

3. Censorship

(i) Would you approve of your company filtering out Internet content via a firewall? (Yes / No)

---

4. Monitoring

How do you feel about your company monitoring your Internet activities via a firewall logging your activities?

---

5. Compliance and Sanctions

(i) If your company had an Internet security policy, how could they make it work?

(ii) Which one of the following would be the most appropriate sanction if an employee in your company was found guilty of excessive personal surfing of the Internet during work hours?

None (Yes)
A warning (Yes)
Suspend Internet connection for one week (Yes)
A fine (Yes)
Dismissal (Yes)
Other (please specify)

---

6. Netiquette

(i) Would you like company guidelines for correct etiquette in Internet usage?
(Yes / No)

---

7. Responsibilities, duties and accountability

(i) Would you expect to have your Internet responsibilities made clear in a policy of some kind? (Yes / No)

(ii) Would you like to have an Internet security awareness session to clarify all Internet usage policies? (Yes / No)

Appendix C

Published Papers Resulting Directly from this Research

Lichtenstein, S. (1996a) "Internet acceptable usage policy", *Computer Audit Update*, Elsevier Advanced Technology, UK, December.

Lichtenstein, S. (1996b) *Internet acceptable usage policy: human issues*, Working Paper 10/96, School of Information Management and Systems, Monash University.

Lichtenstein, S. (1996c) "Internet security policy: a holistic and organisational approach", *2nd Joint Conference Proceedings AUUG 96/APWWW Conference,* Bossomaier, T. and Chubb, L. (Eds.), AUUG'96 and Asia Pacific World Wide Web, World Congress Centre, Melbourne, Australia.

Lichtenstein, S. (1997a) "Developing Internet security policy for organisations", in *Proceedings of the Thirtieth Annual Hawaii International Conference on Systems Sciences* (Nunamaker, J.F. and Sprague, R.H., Eds), Hawaii, IEEE Computer Society Press, Los Alamitos, California.

Lichtenstein, S. (1998) "Internet risks for companies", *Computers & Security*, Vol. 17, No. 2.

Lichtenstein S. and Swatman P.M.C. (1997a) "Internet acceptable usage policy for organisations", *Information Management and Computer Security*, Vol. 5, No. 5.

(also republished in revised form as “Effective Internet acceptable usage policy for organisations”, in Vogel, D.R., Gricar, J. and Novak, J. (Eds.), *Tenth International Electronic Commerce Conference*, Bled, Slovenia.)

Lichtenstein, S. and Swatman, P.M.C. (1997b) “Internet acceptable usage policy: arguments and perils”, in Swatman, P.M.C, Swatman, P. and Cooper, J., (Eds.), *Proceedings of PAWEC’ 97*, Brisbane, Australia.

Appendix D

Published Papers Indirectly Related to this Research

Lichtenstein, S. (1995a) "Information system security for adaptive organisations", *Proceedings 6th Australian Conference on Information Systems*, School of Information Systems, Curtin University of Technology, Perth, Australia.

Lichtenstein, S. (1995b) "Information system security design principles for adaptive organisations", *Proceedings EDPAC 95 Conference*, Melbourne, Australia.

Lichtenstein, S. (1996d) *Information security principles: a holistic view*, Working Paper 3/96, School of Information Management and Systems, Monash University, Melbourne, Australia.

Lichtenstein, S. (1996e) "Information security design principles for adaptive organizations", *Computer Audit Update*, Elsevier Advanced Technology, UK, June.

Lichtenstein, S. (1997b) "A review of information security principles", *Computer Audit Update*, Elsevier Advanced Technology, UK, December.

Appendix E

Framework for Internet security policy for organisations

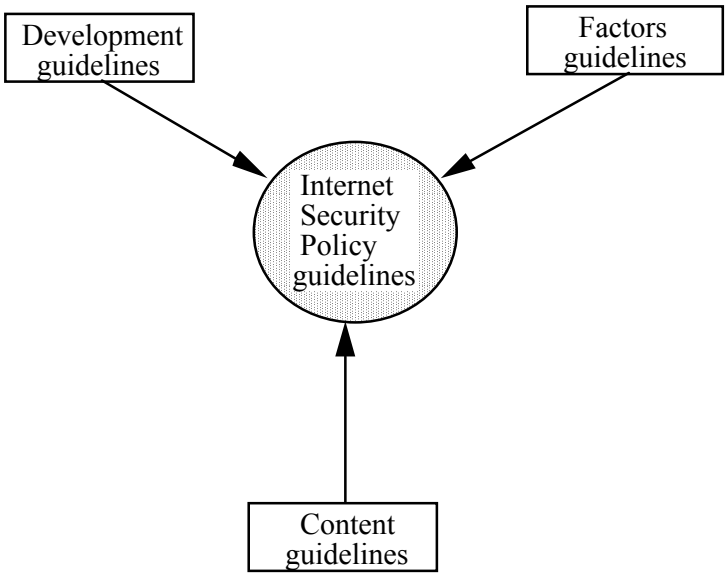

Figure E-1 The three components of guidelines for Internet security policy

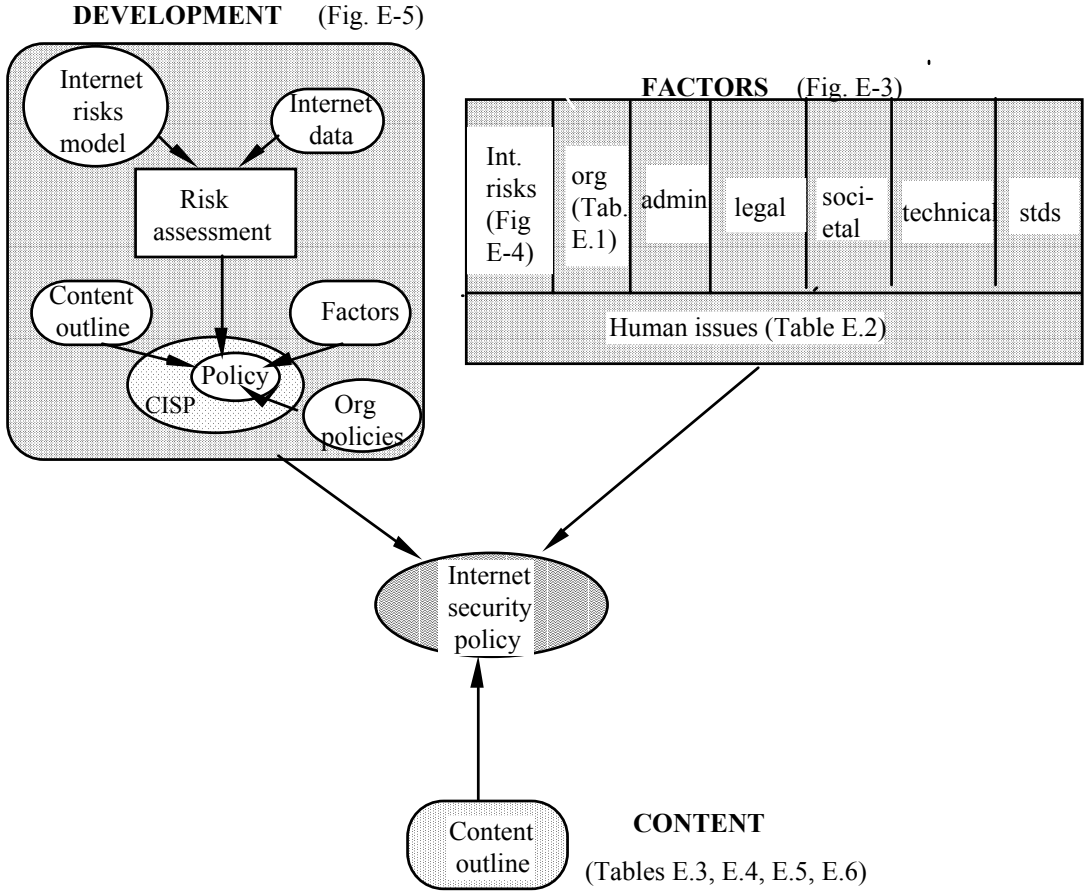

Figure E-2 Framework for Internet security policy for organisations

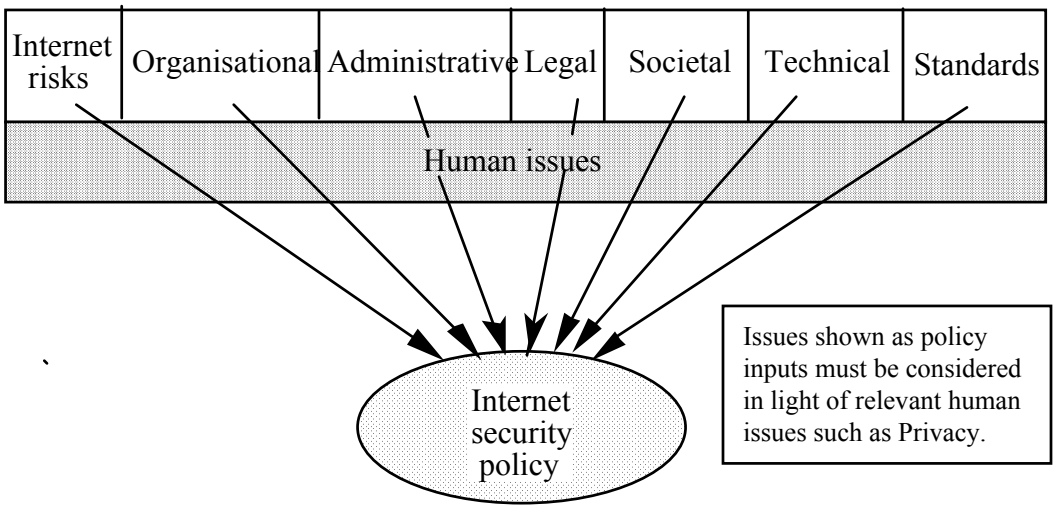

Figure E-3 Factors in Internet security policy

Organisational factors in Internet security policy	Source section
Organisational objectives	3.4.4.1
Organisational Internet security infrastructure	3.4.4.2, 11.3.4.1
Organisational culture	11.3.4.3
Internet security management programme	3.4.4.4
Internet security training	11.3.4.2
Internet security awareness	3.4.4.5
Policy integration	3.4.4.6
Management commitment	3.4.4.3
Principles for Internet security and policy	3.4.4.7

Table E.1 Organisational factors in Internet security policy

Human issues in Internet security policy	Source section
Freedom of Internet use	3.4.8.1
Privacy	3.4.8.2
Trust	10.1.7.5
Monitoring	10.1.7.5
Surveillance	10.1.7.5
Censorship	3.4.8.3
Right to be kept informed	3.4.8.4
Accountability	3.4.8.5
Sanctions	10.1.7.5
Ownership	3.4.8.6
Ethics	3.4.8.7

Table E.2 Human issues in Internet security policy

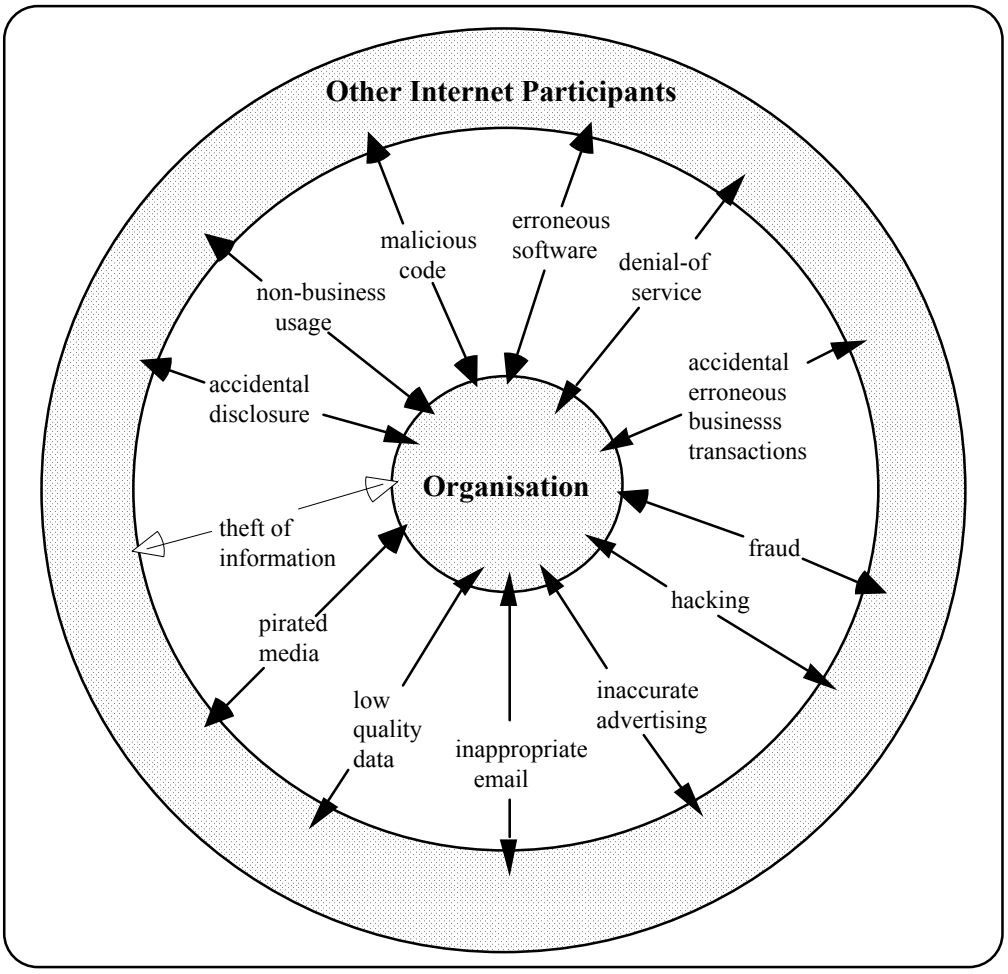

Figure E-4 Internet risks for an organisation

(sources are listed in Table E.7)

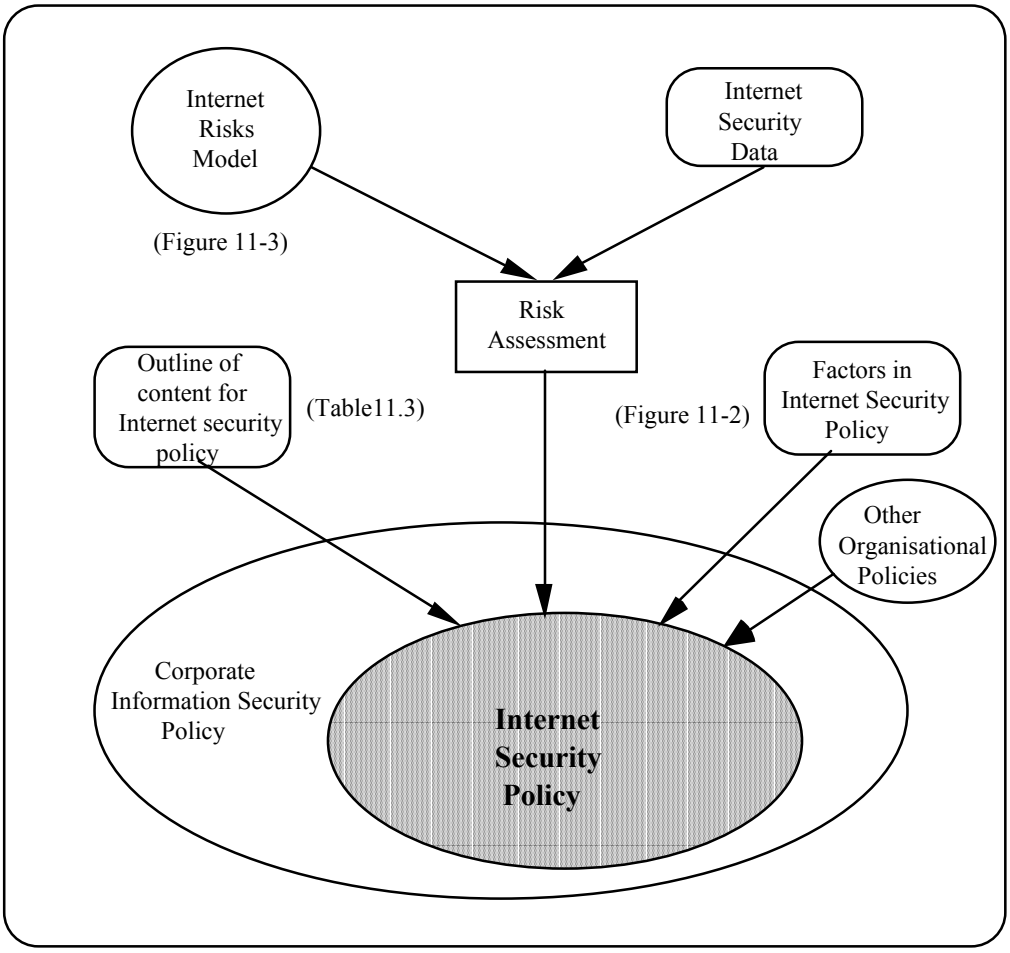

Figure E-5 Development of Internet security policy for organisations

Internet security policy content	Source section
Purpose and scope of policy	4.1.1
Philosophy of policy	4.1.2
Organisational Internet security infrastructure	4.1.3, 11.3.7.2
Internet security management programme	4.1.4
Other applicable policies	4.1.5
Internet privacy policy	4.1.6
Internet censorship policy	4.1.7
Internet accountability policy	4.1.8
Internet information protection policy	4.1.9
Internet information access policy	4.1.10
Internet firewall policy	4.1.11
Internet security technology policy	4.1.12
Password policy	4.1.13
Internet acceptable usage policy (IAUP)	4.1.14
Internet publication policy	4.1.15
Email policy	4.1.16
Internet virus policy	4.1.17
Internet audit policy	4.1.18
Internet incident policy	4.1.19
Internet legal policy	4.1.20
Internet security policy review policy	4.1.21

Table E.3 Internet security policy for organisations—content

Firewall policy content
security boundary statement
firewall policy stance
access method
access rules
firewall maintenance policy
firewall new access request policy
firewall roles and responsibilities

Table E.4 Firewall policy content

(compiled from Bryan, 1995; D'Alotto, 1996; Drake and Morse, 1996; and Griffiths, 1996)

Internet acceptable use policy content	Source section
purpose and scope of policy	4.1.14.1
ethics policy	4.1.14.2
Internet services policy	4.1.14.3
confidentiality policy	4.1.14.4
acceptable uses	4.1.14.5
unacceptable uses	4.1.14.6
Internet risks	4.1.14.7
legal policy	4.1.14.8
roles and responsibilities	4.1.14.9
privacy	4.1.14.10
accountability	4.1.14.11
monitoring and surveillance	4.1.14.12
sanctions	4.1.14.13
awareness	4.1.14.14
user consent	4.1.14.15

Table E.5 Internet acceptable use policy content

Email policy content
email ownership
acceptable email usage
email privacy
email encryption
email monitoring
email netiquette
emotional email
avoidance of references to third parties
duties to third parties (eg auditors)
external interception of email
email virus protection
signature
email deletion after usage
distribution of email copies
copyright implications of copy distribution
legal issues
enforcement and dissemination of email policy

Table E.6 Email policy content

(partly compiled from Barker *et al*., 1995; Denning, 1993; Farrow, 1998; also refer Section 11.4.10)

Internet risk	Source section
Accidental disclosure	3.4.3.1
Accidental erroneous business transactions	3.4.3.2
Accidental disclosure	3.4.3.1
Malicious code	3.4.3.3, 11.4.3
Erroneous software	3.4.3.3, 11.4.3
Denial of service	3.4.3.4
Fraud	3.4.3.5
Hacking	3.4.3.6
Inaccurate advertising	3.4.3.7
Inappropriate email	3.4.3.8
Low quality data	3.4.3.9
Non-business usage	3.4.3.10
Pirated media	3.4.3.11
Theft of information	3.4.3.12

Table E.7 Sources for Internet risks in Figure E-4