e-Everything: e-Commerce, e-Government, e-Household, e-Democracy

14th Bled Electronic Commerce Conference

Bled, Slovenia, June 25 - 26, 2001

Effective Management and Policy in e-Business Security

Sharman Lichtenstein

School of Information Management and Systems, Monash University, Level 7, 26 Sir John Monash Drive Caulfield East, Australia, 3145
Sharman.Lichtenstein@infotech.monash.edu.au

Paula M. C. Swatman

Institute for Management, University of Koblenz-Landau
Rheinau 1, 56075 Koblenz, Germany
Paula.Swatman@uni-koblenz.de

Abstract

The use of the Internet in organisations and companies for carrying out various business activities is becoming an increasingly major component of e-business. Accidental and deliberate misuse and abuse of the Internet by internal employees and external parties, combined with the increasingly vulnerable global Internet infrastructure and the paucity of Internet regulation, has led to an Internet security problem for organisations. This paper reports the major findings from a four year study (1996 – 2000) which included substantial exploration of e-business security issues via six case studies at five medium-to-large organisations, as well as a focus group of industry leaders. The research results include an holistic framework for e-business security policy. The research also highlights the importance of human issues and the need for changes, in current practices in e-business security management and policy.

Keywords: *e-business security management, e-business security policy, Internet acceptable usage*

1. Introduction

The widespread adoption of e-business has brought with it serious new organisational security concerns. The Internet has, from the beginning, exhibited multifarious vulnerabilities—in its underlying communications network and nodes, Internet protocols, network administration and host systems. Hackers, competitors, disgruntled employees and others have exploited the Internet's ever-changing vulnerabilities, leading to loss of security and privacy, financial damage, loss of customers, corporate embarrassment, disruption and uncertainty (CSI 2000). Further, the CSI and others have reported that many employees granted Internet connection for valid business purposes have misused or abused the tool, either from a lack of understanding of its insecurities, a lack of awareness of valid, value-adding business Internet usages, or purely from malicious intent.

Experts state that management of e-business security issues at different levels is urgently needed (for example, Pethia et al. 2000)—including at the organisational level, which is the focus of this paper. However until recently, few guidelines for e-business security management in organisations have been available. Policies, procedures, standards and other management instructions are regarded as critical in the management of internal e-business security issues such as employee misuse and abuse of the Internet, being aimed at controlling the decisive human factor—the company's employees (Bernstein et al. 1996, Guttman and Bagwill 1997, Overly 1999). The aim of this paper is to identify e-business security management practices which will render such policies and procedures more effective. In particular, the paper focuses on the importance of the human issues in determining such policies and procedures, and the use of an holistic e-business security policy to manage the risks and other issues.

The discussions and recommendations reported here are based on the research findings of a four year PhD research project (1996 – 2000). The interested reader will find details of the background, the models developed and the research issues for the project in Lichtenstein (2000).

After the completion of that project, we recognized that the Internet security policy as treated in the project was, in effect, an e-business security policy (that is, the medium by which e-business security requirements for the organisation are specified, and the means by which security guidance and rules are provided to e-business participants within the business). This policy—which includes the Internet acceptable usage policy (IAUP) informing and instructing employees in Internet acceptable usage (Lichtenstein, 1996a)—underpins e-business security management. Similarly, Internet security management as treated in the project is more properly termed e-business security management. We therefore use the terms *e-business security policy* and *e-business security management* in this paper.

We provide in this paper:

- an holistic framework to guide the handling of factors, development and content in e-business security policy for organisations;

- a discussion of the special role of human issues in e-business security management and policy for organisations;
- a discussion of significant issues found in e-business security management and policy in companies, accompanied by suggestions for achieving more effective management and policy.

2. Methodology

Over the four year research project, we explored Internet risks and other issues affecting e-business policy and management section through existing literature (for example, Bernstein *et al*. 1996, Gaskin 1998, Guttman and Bagwill 1997, Heard 1996, Pethia *et al*. 1991). The issues identified were then brought together as a number of models, resulting in an initial framework for organisational e-business security policy, comprised of many components. As guidelines in this area were scarce at the time of the study (example guidelines can be found in Heard 1997, Guttman and Bagwill, 1997), and few companies possessed such policies, we considered the most suitable methodfor testing the initial framework was in-depth case studies of medium to large organisations having at least a reasonably significant history of Internet and e-business activity—followed by a focus group of experts in the field, to further explore the results obtained from the case studies.

In undertaking the cases, we mainly used semi-structured interviews for data collection, focusing on the views of the network administrators, who appeared to have the most knowledge of what was actually occurring, as well as most of the decision-making power with respect to the relevant issues. We also explored the views of the security managers, and were hence able to identify important managerial issues relating to decision-making processes in setting and implementing policy. We analysed the data collected for each case, using the initial framework as a guide, then carried out a cross-case analysis across the six cases, to determine commonalities, trends and differences, and to draw conclusions from these for the research project.

Next, we conducted a focus group composed of six experts in different specialised positions, to obtain a range of views. Employees and technical experts were well-represented in the group, as the views of the employers had already been heavily polled via the case studies. Participants in the group were taken through the proposed framework for policy and all related issues by a moderator, in a three hour session. We obtained important feedback from the often heated discussions which took place at the meeting, for the project.

The outcome of the project was a framework for organisational e-business security policy (discussed in the next section), as well as a comprehensive set of findings for management and policy in e-business security (summarised later in this paper).

3. Holistic Framework for e-Business Security Policy

Our framework for e-business security policy (Figure 1) comprises three sets of guidelines—a set of *factors* to be considered when developing the policy, a method for the *development* of the policy, and a framework for the *content* of policy. In this section, we focus on the diverse *factors*—particularly the human issues—which influence policy, and provide only summaries of the development and content guidelines.

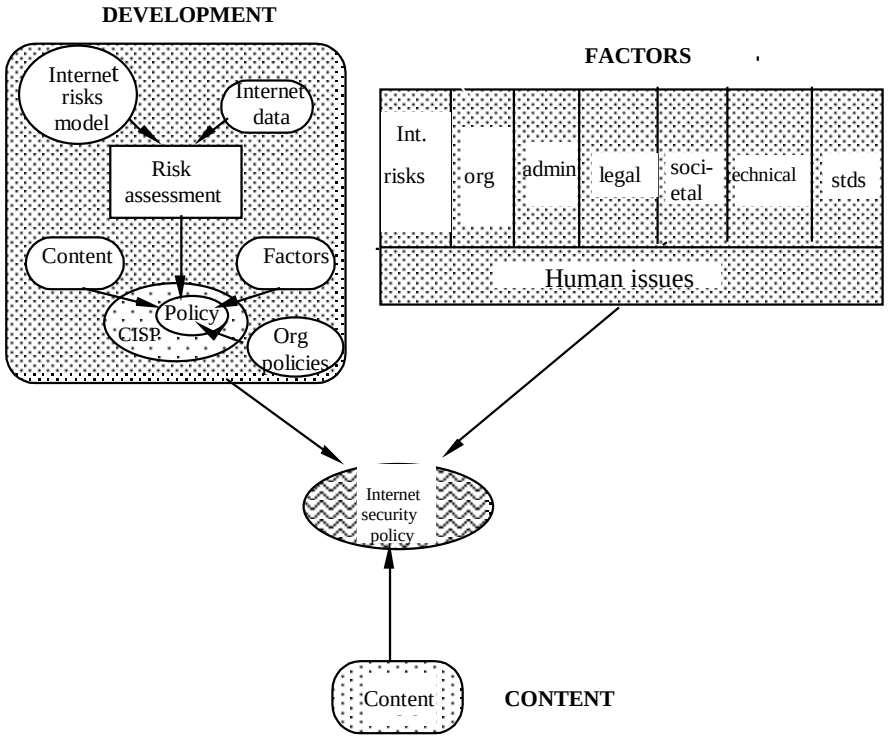

Figure 1: *Framework for e-business security policy (Lichtenstein, 2000)*

We now discuss each of the three components of the framework.

Over the past decade, a number of researchers have argued for an holistic perspective for information security and e-business security (see, for example, Brunnstein 1997; Yngstrom 1995; Lichtenstein 1997, 2000; Lichtenstein and Swatman 1997). We identified in our study a number of diverse factors to consider when setting e-business security management and policy: *Internet risks, organisational, administrative, legal, societal, technical, standards* and *human issues* (Figure 2).

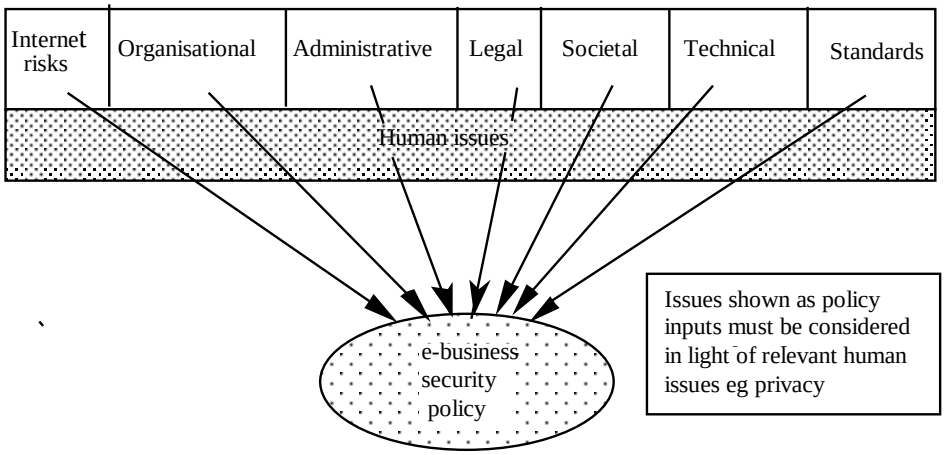

Figure 2: *Factors in e-business security policy*

Our model for *Internet risks* faced by companies engaged in e-business is a set of Internet risk types: non-business Internet usage, malicious code, erroneous software, denial of service, accidental erroneous business transactions (for example, misdirected email), fraud, hacking, inaccurate advertising (for example, personal email opinion assumed to be the company's official view), inappropriate email (for example, harassing email), low quality data (for example, company use of low quality web site information for business purposes), pirated media, theft of information (for example, via interception), and accidental disclosure (for example, company email leaking confidential business information). Clearly, a major function of the e-business security policy is to provide policies to control the significant Internet risks for the company.

Organizational and *administrative issues* can affect the policy. For example, those usages of the Internet which are considered valid by the company, and therefore acceptable uses, should be articulated in the policy. These usages should be aligned with organisational objectives in order to maximise benefits to the company. Administrative and operational tasks must be defined—for example, procedures for applying, monitoring and auditing policies.

A company needs to be aware of relevant *legal issues* when setting its policy (see for example, Cavazos et al. 1994, Saunders Thomas et al. 1998, Smith 1996). The policy must reflect current laws (such as copyright laws), while the IAUP notifies employees of illegal e-business actions.

Societal issues should be considered in situations where the company perceives that the larger, global society is affected by its e-business security management. For example, setting netiquette standards can take into account a company's interactions with other cultures.

Technical issues include technical constraints that affect the outcome of the e-business security policy. For example, available workstation technology places

constraints on those Internet services which the workstations will reasonably be able to utilise. The company must also consider likely expenditure on additional technologies to improve security, and formulate a policy which 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.

Standards must be considered, as policy must adhere to relevant industry, national and other standards.

With respect to *human issues*, it was clear from our empirical work—both the case studies, and in particular the focus group discussions, during which a heated debate took place over the distinguishing of the *human issues* factor from the various other factors in the factors model—that the human issues affecting internal employees play a critical role in e-business security policy. Indeed, an important finding in our research was that the human issues should be the filter though which all other factors are viewed, during policy development (Figure 2). We elaborate on this finding, below:

- *Freedom of Internet use:* The project drew attention to high levels of personal (as distinct from business) use of the Internet in the workplace by employees (in some cases, 80% of Internet use was for non-business purposes), indicating a need for restrictions on use—yet employees resist having such freedoms curtailed, with significant implications for policy.
- *Privacy:* The project highlighted employees' privacy expectations for email, implicating the possibility of use of monitoring as a mechanism for company control of the email business confidentiality risk, the risk of harassment through email, and various other risks. Employees also expected privacy of their web accesses, thereby implicating the use of logging as a mechanism for controlling personal Internet use and other risks such as internal attempts at hacking of external sites (which was reported in a number of the cases we studied). a discussion of significant issues found in e-business security management and policy in companies, accompanied by suggestions for achieving more effective management and policy.
- *Trust:* The project highlighted employee expectations that their companies would trust them to behave appropriately and securely in their Internet usage. Such trust conflicts with the company need for policies to limit personal Internet use, as well as policies to control all kinds of risks.
- *Monitoring:* The project showed significant employee resistance to email and web access monitoring via logging and reporting of logs, thereby reducing the opportunity to use such monitoring to reduce various risks, such as hacking and non-business usage.
- *Surveillance:* The study showed that employees balked at the concept of surveillance of their net activities, hence reducing power of the policy for internally caused risk minimization.

- *Censorship*: 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, employee access to indecent and criminal Web sites, defamation and harassment of others by their own employees, damage to company image caused by recorded employee accesses to indecent or criminal sites, and 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). Our study indicated that employees are opposed to such censorship. Nor did employees approve of their emails being scanned for censorship purposes. Such requirements would clearly reduce the power of the policy to comply with the societal and company Internet requirements discussed above.
- *Right to be kept informed:* The study highlighted a lack of awareness of policy by employees, and clearly all policy decisions would need to be clear, communicable and explainable.
- *Accountability*: Policies which clarify employee accountability (ie place the blame) for Internet actions are extremely difficult to formulate. Typically, authentication, non-repudiation, and visibility through monitoring and surveillance, are the mechanisms by which such accountability can be achieved. Our study indicated a lack of resources in companies for monitoring actions, in every case. Clearly, all policy decisions need to be made with a view to the feasibility of implementing and enforcing employee accountability for Internet actions.
- *Sanctions:* The study indicated contentiousness and vagueness of sanctions for Internet misuse and abuse. Clearly all policy sanctions need to be linked to the relevant risks and other issues.
- *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. Policy decisions must always consider the ownership issue.
- *Ethics:* A sense of ethics within global society should be expected in employee Internet use. 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 policy is desirable.

Our identification of the importance of human issues in e-business security management and their relevance to all other issues, is consistent with previous

findings regarding the importance of the human element in information security management (see, for example, Kohl 1995; Rannenberg 1994; Yngstrom 1995).

Content of e-Business Security Policy

Pu Purpose and scope of policy
Philosophy of policy
organisational e-business security infrastructure
e-business security management programme
other applicable policies
e-business privacy policy
e-business censorship policy
e-business accountability policy
e-business information protection policy
e-business information access policy
firewall policy
e-business security technology policy
password policy
Internet acceptable usage policy (IAUP)
e-business publication policy
email policy
Internet virus policy
e-business audit policy
e-business incident policy
Internet legal policy
e-business security policy review policy

Table 1: *Content of e-business security policy*

The e-business security policy consists of subpolicies (summarized and shown here as Table 1).

Development of e-Business Security Policy

The Internet risks model is used in conjunction with company-specific e-business security data as input into a risk assessment process (which may be quantitative or qualitative), in order to identify and prioritise significant e-business risks for the company. These risks are then considered in conjunction with other influential factors in e-business security policy, in order to construct the policy itself, in line with the structure suggested by the e-business security policy content model. The e-

business security policy is positioned within the Corporate Information Security Policy (oval labeled CISP). The risk assessment results are considered in conjunction with a consideration of other factors in Internet security policy, the outline of the content for an e-business security policy, and various organizational policies such as the company's code of ethics, in order to determine the e-business security policy.

4. Findings

In this section, we summarize the findings of the research project:

(a) In all companies studied (four Australian and one American), we discovered evidence of Internet risks of various types, routinely occurring. These risks were affecting the companies to differing degrees, indicating the existence of a serious e-business security problem in Australian companies (with the sole American case study providing support for the view that this situation is global). The research study highlighted particularly high levels of non-business use and malicious code (viruses), consistent with the alarmist reporting of these trends by the media over recent times. In most of the companies studied, employees had been dismissed for significant non-business use, although the companies had, during the period of the study, only recently begun to come to grips with the problem. Viruses were regularly encountered, with companies becoming aware too late of the serious viruses hitting their firewalls (for example, the Melissa virus). Furthermore, all the Internet risks depicted in Figure 1 were identified with varying degrees of risk across the companies studied. Clearly, Internet risks are impinging on secure e-business and require improved management. An e-business security policy is a suitable high-level vehicle to underpin such management.

(b) There has been a tendency to focus almost exclusively on technical security needs in policy—for example, the availability of specific security technologies such as intrusion detection software. The companies studied possessed many nontechnical security needs, for example the requirement for legality of e-business security policy—that is, compliance with existing relevant laws such as copyright. It was clear that companies were unable to ignore certain sensitive nontechnical issues, such as employee rights to privacy in their Internet usage. Overall, there must be reasonable accommodation of non-technical factors in policy, suggesting that an *holistic methodology* is required for policy development—an approach where the organisational, contextual and human issues are given equal consideration to the technical issues.

(c) A major finding in the project was the importance of human issues (for employees) in e-business security. The two main human issues are: *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. It has been interesting to observe in the media (in tandem with the conduct of the research project and consistent with the actions

being taken by the companies studied), the tide of disciplinary action being taken against employees for violations of nonbusiness policy (involving the freedom of Internet use and privacy issue) and confidentiality policy (involving the privacy issue)—with each conviction necessitating the controversial monitoring of net use, in order to detect the abuse. This trend was also reflected in the cases studied for the project, with increasing action being taken for detected employee abuses in similar areas (nonbusiness use and confidentiality). The trend highlights the seriousness with which companies now regard these breaches, and the progression of e-business security past its early wait-and-see stage.

We found other human issues to be of concern, in particular:

- censorship—filtering of sites from employee access via firewalls and other mechanisms, was not
- popular with employees at the companies studied;
- the right to be kept informed—employees were suffering from a lack of awareness of security risks, needs and policy;
- accountability—employees were not being held accountable enough for their Internet actions, due to a lack of policy, policy implementation technology, and monitoring resources; and
- trust—employees were concerned about the lack of trust shown in them by their employers through various policy decisions (for example, the decision to monitor net use).

(d) As we reported above, high levels of non-business usage were occurring in all the companies studied, a natural consequence of the immaturity of Internet diffusion in the workplace (employees are highly tempted to use the Internet for personal purposes while at work). This suggests that:

- Firstly, employees and managers alike are uncertain as to the nature of genuine business uses of the Internet. A business should develop an e-business strategy to include planned, value-adding or otherwise valid uses of the Internet. It was very evident from the studies that companies are not always certain of what constitutes valid, or value-adding, Internet use. 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 permit.
- Secondly, it was clear from the cases studied that employees, for the most part, are aware of the extent of their non-business usage, and are simply taking advantage of ("rorting") the system. In order to halt this trend, companies must set and enforce more stringent policies, and also utilise powerful Internet security management technological tools for filtering out selected undesirable sites, and for 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 some evidence that

companies have begun to tighten the reins, in line with these conclusions (for example, Xerox dismissed 40 employees in the US in October, 1999, and Centrelink dismissed six call centre employees in Australia in 2000, for email misuse).

- Thirdly, companies must establish a level of non-business use which both they and their employees find acceptable. For example, is two hours a day of Internet use sufficient to get the employee's work done? If so, then such a restriction will force the employee to restrict their business use. More and more policies are being developed along the lines of: "Limited personal use of the Internet is permitted," or "Personal use of the Internet should be limited to essential use," which seems to be a grass roots policy rooted in necessity.

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 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, rather than a right.

(e) All cases studied showed considerable employee misuse of the Internet. The companies remarked many times on the serious shortage of human resources (authorised people with the time available) for the purpose of checking Internet access logs, and for human surveillance of Internet screen activity (any hopeful reliance on business unit managers for surveillance of employees did not appear to work).

Senior managers must be informed of the growing e-business security problem and the need for additional resourcing, in the form of purchasing the necessary Internet security management technology for monitoring purposes, as well as securing the necessary human resources to check resulting reports and take action if necessary. Business unit managers must also be educated with respect to taking action when Internet misuse or abuse is apparent. However, we recognize that it is no longer realistic to rely on "sufficient" human resources, in the type of downsized, stressed-employee world which we now inhabit, 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.

(f) The research highlighted the fact that some employees are always going to "behave badly"—as it were—no matter what kind of policy, awareness, monitoring, and sanctions, are employed. For example, employees who want to engage in joke-sending, personal email to friends, etc, will find a way, no matter what the policy and technology to prevent or detect it. 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. We address this need further, below.

(g) Some employees committing e-business security breaches are not "behaving badly", but rather are making innocent mistakes—due to ignorance, carelessness, or oversight. For example, in the cases studied, employees accidentally: misdirected important emails, sent out confidential emails, downloaded viruses as email attachments (in one of the case studies, it took three weeks for the company's email system to recover fully from the Love bug virus in May, 2000), and so forth.

As mentioned before, a reliance on the employee following policy, or behaving securely, is a fruitless and frustrating security strategy. Technology companies have, fortunately, been responding to a newly perceived demand by developing Internet security management tools which prevent these types of accidents. For example, customisable email text filters, which 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. We recommend that a company investigate the technical options available, as an important part of their e-business security policy – hence minimising, yet again, reliance on the employee.

(h) Most companies lack a coordinated e-business security management programme, taking instead a piecemeal approach to managing e-business security. Our research shows the need for a well-resourced, formal organisational e-business security infrastructure, featuring a comprehensive, holistic e-business security management programme containing a range of coordinated elements, including: an e-business 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 e-business security situation.

Dynamic and ongoing Internet training and awareness was noticeably missing in each company:

- Firstly, there should be mandatory e-business/Internet security training, with testing, for each employee, prior to the employee being granted Internet access privileges.
- Secondly, in today's rapidly 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 can continue).
- Thirdly, awareness of e-business/Internet security issues must be provided for senior managers, in order to secure their commitment to e-business security matters—beginning with their resourcing of the organisational infrastructure, through to their setting a good example via exemplary, personal Internet behaviour.

(j) Non-technical managers responsible for e-business/Internet security issues (as well as for general information security issues) appear to have very little knowledge of, or interest in, the existing implementation and state of Internet security, at a detailed level. The managers interviewed in the case studies continually redirected questions about such issues to the technical system administrator present, and there was obviously an awkward professional relationship between the two parties on such occasions, most probably due to the inappropriateness of the power and knowledge being vested in the systems administrator. There was a block in knowledge of e-business/Internet security matters in the company, at this point in the managerial chain to the top, with the result that senior managers have little chance of receiving accurate information about the 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 e-business/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 e-business/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 relevant security issues, and hence be able to plan and make important decisions, as well as 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.

(k) Clearly, companies are fighting an uphill battle with an inherently insecure global Internet infrastructure. Hence, external parties (other than individual businesses) must also take some responsibility for improving Internet security levels. We 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 e-business/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 rebuilt more securely.

5. Summary and Conclusions

We have shown in this paper, which reported the major findings from a four year research project, that there are significant Internet risks for organisations conducting e-business, and that there are many other diverse and sensitive issues to be considered in the management of these risks, suggesting an holistic approach is needed for e-business security management and policy. We presented a framework for e-business security policy (Figure 1), featuring a model of the factors in e-business security (Figure 2) and a structure for the content of the e-business security policy (Table 1). We highlighted the sensitivity and special significance of the human issues involved when setting policy, and demonstrated the need for effective, holistically developed, e-business security management and policy. Finally, we articulated a number of recommendations to assist companies with their endeavours to this end. We now draw conclusions for business.

Clearly, Australian companies and, indeed, companies globally must heed these research findings by recognising the seriousness of the e-business security problem they are confronting. Businesses must invest resources—time, skilled people, energy and money—to address those recommendations which are particularly relevant to their own situation. Furthermore, they will find that they need to lobby third parties to fulfil their roles in supporting these recommendations:

- educational institutes—to educate the public as future e-business consumers and employees; to provide the necessary e-business training courses for existing employees; to educate managers in valid e-business uses of the Internet; and to develop courses for e-business security professionals;
- the media—to inform members of the public of existing and new Internet risks, as well as educate them in e-business security issues in general;

- technology creators—to develop and supply the required Internet security management software;
- regulatory bodies such as governments—to develop supporting regulations;
- industry support bodies—to form conglomerates who will rally together as needed, to devise protection against new risks and outbreaks of attacks;
- commercial organisations to sponsor the development of research guidelines into professional documents which can be used by companies and security specialists; and
- e-business security professionals—to acquire necessary skills and expertise for developing the required policies and management programmes, for companies.

Finally, in order to gain the maximum benefit possible, industry should support research being conducted on this important topic, so that recommendations may be made to companies regarding:

- personal use of the Internet in the workplace; and
- the resolution of conflicts for e-business security policy in sensitive human issues such as privacy: for example, is it ethical for a company to rule that its managers may read employee email?

Clearly, in an era where a single Internet incident—whether an external attack or mere employee misuse—can severely impact any Internet-connected company, businesses engaged in e-business need to become proactive in this important area.

References

Bernstein, T., Bhimani, A. B., Schultz, E. and Siegel, C. A. (1996), *Internet Security for Business*, John Wiley & Sons, Inc.

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.

Cavazos, E.A. and Morin, G. (1994) *Cyberspace and the Law: Your Rights and Duties in the On-Line World*, MIT Press.

CSI (Computer Security Institute) (2000*) Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey*, CSI, San Francisco, USA.

D'Alotto, L.J. (1996) Internet firewalls policy development and technology choices. *Proceedings of 19th National Information Systems Security Conference*, Baltimore, MD, U.S.

Gaskin, J.E. (1998) Internet acceptable usage policies. *Information Systems Management*, 15(2).

Guttman, B. and Bagwill, R. (1997) *Internet Security Policy: a Technical Guide*, NIST, Special Publication 800-XXX, http://csrc.nist.gov/isptg/html/ (accessed October 31 2000).

Heard, F.T. (1996) Internet security policies and Internet appropriate use policies. *Proceedings of EDPAC 96 Conference*, Perth, Australia.

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.

Lichtenstein, S. (1996a) Internet acceptable usage policy. *Computer Audit Update*, Elsevier Advanced Technology, UK, December.

Lichtenstein, S. (1996b) *Internet acceptable usage policy: human issue.* Working Paper 10/96, School of Information Management and Systems, Monash University, Melbourne, Australia.

Lichtenstein, S. (1997), Developing Internet security policy for organisations. 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, CA.

Lichtenstein, S. (2000) *Internet security policy for organisations*, PhD thesis (public version), School of Information Management and Systems, Monash University, Melbourne, Australia.

Lichtenstein, S. and Swatman, P.M.C. (1997) Effective Internet acceptable usage policy for organisations. *Tenth International Bled Electronic Commerce Conference* (Vogel, D.R., Gricar, J. and Novak, J., eds), Bled, Slovenia.

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.

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 October 31 2000).

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).

Saunders Thomas, D., Forcht, K. A. and Counts, P. (1998) Legal considerations of Internet use - issues to be addressed. *Internet Research*, 8(1).

Smith, G.J.H. (1996) Setting up a Web site - managing the legal risks. *Internet Research*, (6/2/3).

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.