Developing Internet Security Policy for Organizations

Sharman Lichtenstein
Department of Information Systems
Monash University
Melbourne, Australia
email: sharman.lichtenstein@is.monash.edu.au

Abstract

This paper describes a general framework for developing an organization's Internet security policy. A model of Internet security risks for an Internet user organization is proposed; the framework utilizes this model, as well as considering important holistic issues, in order to develop the user organization's Internet security policy. A hierarchy of subpolicies for the Internet security policy is also suggested. This paper presents the results of one phase of a wider investigation into Internet security policy.

1. Introduction

Usage of the Internet is growing exponentially. Although the Internet may not be the ultimate model or technology for future national or global infrastructures, it is nevertheless an important landmark in the evolution of any future infrastructures. Therefore, any major problem areas associated with Internet use need to be addressed.

Since its inception in the 1970's, the Internet has both threatened and displayed a variety of vulnerabilities, existing in the underlying communications network and its nodes, in the Internet protocols, in network administration, and in the host systems. Vulnerabilities have often been located in the security mechanisms of the various host systems [7], examples being the ability to obtain unauthorised privileged access, and the ability to gain unauthorised access to passwords. Hackers, competitors, disgruntled employees and ex-employees have been exploiting these and other vulnerabilities [7], highlighting the changed nature of the Internet environment from collegial and trustworthy to competitive and hostile. There are also increasing concerns about threats emanating from trusted employees; for example, an employee may send out information over the Internet to a global audience, innocently yet falsely presenting as a spokesperson for an entire organization. Commercial usage of the Internet has brought a host of new threats, for example, interception of data in transit by competitors or criminals. The current vulnerabilities, together with an increasingly unfriendly environment, plus heavy and rapidly growing usage of the Internet by technically sophisticated users globally, combine to signal information security as a major Internet problem area.

Internet security policies and procedures should be the media by which Internet security guidance and rules are provided to Internet participants, each of whom has their own peculiar security interests. Inside a user organization, participants include: owners, administrative managers, system managers, third parties (for example, clients) and employees. External to user organizations, participants include: government bodies, security system vendors and developers, and site and network service providers. Some participants have already established policies: The Internet organizational structure is a loosely coupled coalition of organizations and activities without any central management structure, possessing rules which must be followed in order to connect to its backbone communication system, and possessing protocols which must be followed in order to communicate via the network. However, for the remainder of the Internet community, there is a notable shortage of policy.

To date, very little guidance for the development of Internet security policies has been available; early work included Pethia et al. [28] and IETF [14]. Recent work includes the USA's National Performance Review report on information technology [22], which commissioned the development of a Federal framework for Internet security [8]. This led in turn to the development of a Federal Information Security Plan (FISP) [9]. Particular actions in the plan address the need for guidelines for developing Internet security policy, and follow-up work is currently in progress [10].

One major thrust of the FISP plan is the recommendation for a holistic approach to Internet security, in which physical, human and technical issues are taken into account. Recent research has similarly supported holistic perspectives of information security [for example, 11,13,16,23,24,32]. Thus it is appropriate that the development of Internet security policies be carried out within a holistic framework.

The FISP policy-related actions firstly recommend the development of broad Internet security policies to be

Proceedings of The Thirtieth Annual Hawwaii International Conference
on System Sciences ISBN 0-8186-7862-3/97 $17.00 © 1997 IEEE

1060-3425/97 $10.00 (c) 1997 IEEE

issued through established channels such as Federal Information Processing Standards (FIPS), to be followed by the development of community-specific policies, which would be carried out by the various participants in the Internet community. Key participants are the user organizations, who are not only vulnerable to threats emanating from the Internet, but also represent sources of threats to other Internet participants. These organizations have thus far largely ignored the need for Internet security policy. Pethia et al. [28] wrote "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."

Currently, within user organizations there is an urgent need for Internet security policies. Very little rational selection of Internet security mechanisms as implementations of any formal policy takes place. Instead, user organizations have been typically implementing security mechanisms such as firewalls as a knee-jerk reaction to the Internet security problem (Beker [4] pointed out that there is a need to develop a model of those information security requirements which are actually enforced via a firewall!). Thus, there is an important need for each user organization to specify an Internet security policy describing the requirements for Internet security within the organization. These requirements should address Internet-related risks for the organization. Mechanisms which implement these particular requirements can then be selected. The Internet security policy should be a key component of an overall Internet security program in the organization.

A method is required to develop an Internet security policy. The method should incorporate holistic issues, should address Internet-related risks, and should result in a well-structured, comprehensive and effective Internet security policy. This paper addresses the question:

- Can a framework for developing a user organization's Internet security policy be specified, which ensures that holistic information security issues are accommodated?

The paper begins by describing a high-level Internet risks model for an Internet user organization. A discussion of holistic issues in Internet security follows. A framework is then presented for developing a user organization's Internet security policy. The paper also suggests a hierarchy of subpolicies for the Internet security policy. Finally, the research is evaluated, and plans for further work outlined. This paper presents the results of one phase of a wider investigation into Internet information security.

2. Internet risks for user organizations

In the development of an Internet security policy for a user organization, it is imperative that the risks to the organization arising from the Internet connection be addressed. This requires identification of the relevant risks, followed by a prioritisation of the risks via risk assessment. Much has been written about the risks for organizations using the Internet [for example, 6,8,21]. It is beyond the task of this paper to identify or discuss in detail the many and varied risks, however the above sources as well as others should be consulted in order to add richness to the Internet risks model illustrated in Fig. 1.

In the model, risks are categorized into risk groups, in order to enable the identification of relevant Internet risks for the user organization. The effects of the risk groups are typically loss of confidentiality, integrity or availability to either the user organization's information resources or to other Internet participants' information resources. The model also includes Internet risks which infringe employee privacy rights (for example, the sending or receipt of junk email by employees). The central circle denotes a user organization with Internet connection. The outer ring labelled 'Other Internet Participants' denotes other members of the Internet community with whom the user organization communicates via the Internet. The two-way arrows portray Internet risks which can emanate from within the organization and affect other Internet participants, or which can emanate from other Internet participants and affect the organization. Each arrow represents a different type of Internet risk, as briefly described below.

Accidental erroneous business transactions

User organizations or employees may accidentally issue transactions incorrectly, for example, by sending a transaction to the wrong application at another user organization.

Low quality data

The quality of data being exchanged via the Internet is questionable, in that it may be inaccurate, untimely, inconsistent, or merely opinion rather than fact [17]. Organizations or employees may accidentally issue transactions which contain incorrect data (for example, by inclusion of an inaccurate data field). Another manifestation of the problem is that initially correct information, in the form of business transaction data or communications, may become altered in transit, either deliberately, via eavesdropping (also known as sniffing or snooping), or accidentally [17]. Outdated (i.e. untimely) information may remain on old Web sites. Conflicting versions of data may exist, for example, two versions of a database. Subjective opinion, rather than fact, may be transmitted by organizations or individuals, via postings.

Non-business activities

Employees may be using the Internet for a variety of nonbusiness activities, including surfing the Internet, Internet relay chatting, downloading games and images, personal use of email, personal use of other tools (for example, videoconferencing), netphones and newsgroups.

Accidental/deliberate disclosure

Employees may be incautious in their use of the Internet when communicating possibly confidential business matters. An example of accidental disclosure is the inclusion of confidential information within email, a Web site, or another posting mechanism. Deliberate disclosure may occur. For example, 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.

Junk email

User organizations or employees may send unwanted email to one another, representing an infringement of privacy rights. Spamming of individuals or sites may occur, this being the sending of excess flame mail, sometimes referred to as mail-bombing, indicative of a decline in civility between Internet participants [12].

Inaccurate advertising

A user organization or employee may 'advertise' within email, Web sites, or other posting mechanisms, in such a way as to appear to represent an official view. The content of this information may be inaccurate, in an organizational context.

Hacking

An employee may gain unauthorised access to an organization's systems or data either out of curiosity or for a more harmful reason, and may subsequently cause damage. The well-known risk of impersonation is included in this risk type, two pertinent examples being the forging of electronic mail ("Email is usually easy to forge, being the electronic equivalent to a postcard written in pencil") and the existence of undependable Internet identifications [21].

Internet-transferred threats

Other Internet participants may act as a source or conduit for harmful threats to attack an organization. For example, a flaw in an Internet component may be exploited in order to transfer threats from outside into the organization.

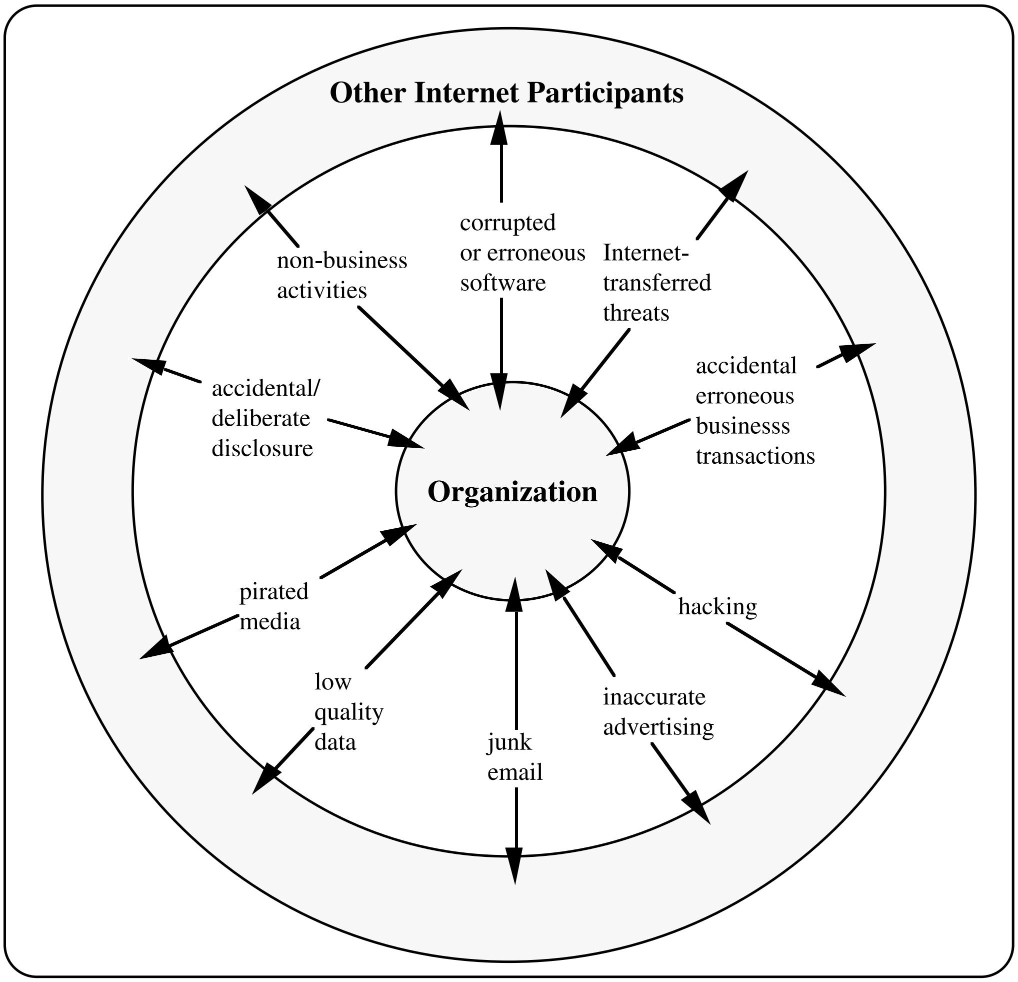
Other Internet Participants
corrupted or erroneous software
non-business activities
Internet-transferred threats
accidental/ deliberate disclosure
accidental erroneous businesss transactions
Organization
pirated media
hacking
low quality data
inaccurate advertising
junk email

Figure 1: Internet risks for a user organization

Pirated media

An employee may download software or data in breach of copyright or licensing laws.

Corrupted or erroneous software

An employee may download software containing bugs, or malicious software such as viruses and trojan horse programs. Web browsers are particularly dangerous, in their provision of access to untrustworthy systems and in their invocation of unproven applications.

Signicant Internet risks identified via use of the model in conjunction with a risk assessment, should be considered in the development of the Internet security policy. However, this policy also needs to be developed in the holistic context which was introduced earlier in the paper.

3. Holistic perspectives of Internet security

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 [30]. Holism is defined as "the tendency in nature to produce wholes from the ordered grouping of units" [25]. 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.

There has been much discussion of holistic perspectives of information security. 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 [23], 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 [3].

There is a common theme to all holistic perspectives: the non technical issues should be considered equally important to the technical issues.

Other examples of holistic information security perspectives include:

- The OECD's information security guidelines [24], which relate to many diverse aspects: people, their rights and their responsibilities; viewpoints (multidisciplinary, interorganizational, and intraorganizational); technical, administrative, organizational, operational, commercial, educational and legal aspects; the cooperation of parties; the integration of the parts to form a coherent information security system.
- Organizational information security policies, which should take into account the organisation's information security philosophy, national policy, international standards, political issues, relevant organizational policies, implementation platform limitations, and relevant ethical, legal and privacy issues [27].

While many holistic views of information security currently exist, holistic approaches are still required for developing, evaluating, and managing information security [11,15,29,32]. Holistic perspectives are also being recommended for specific domains of information security, with this paper advocating a holistic perspective for the domain of Internet security.

A brief discussion of holistic Internet security issues which impact on policy follows, using Yngstrom's [32] classification scheme for holistic information security issues:
legal; ethical, social and cultural; managerial; administrative and operational; and technical.

Legal issues

The organization will need to be aware of relevant international, national and state laws, and relevant standards, before setting its policy.

Ethical, social and cultural issues

There are many such issues to consider. Employees will demand certain rights, and accept certain responsibilities and a certain degree of accountability, depending on the ethical, social and cultural climate of the organization and country. For example, in many organizations, employees may feel unduly restricted, and may revolt, if prohibited entirely from utilising the Internet for personal reasons. They may feel that they have the right to send personal email, for example. Employees in many environments may refuse to accept accountability without adequate Internet awareness programs in place, including provision of written policy which clearly defines both their responsibilities and the acceptable employee usages of the Internet. Employees will need to have policy concepts explained clearly via security awareness sessions, for example, what are "reasonable and prudent precautions" [5]? Employee sanctions for breaching policy should be clearly defined, and acceptable. Employee privacy issues must also be addressed. For example, individual employes may not wish personal information about them to be published and available on the Internet. Other ethical concerns include Rannenberg's [29] multilateral security concerns: unobservability, anonymity, unlinkability, pseudonymity and non-repudiation.

Managerial issues

Management must ensure that Internet security policies form part of a comprehensive Internet security program, which is in turn part of an organization's information security program. The Internet security program should include risk assessment, policy determination, training, readily available and accessible policy documentation, monitoring, and regular security briefings.

Administrative and Operational issues

Many administrative and operational tasks need to be considered and defined, for example "applying, monitoring and auditing the security procedures" [5].

Technical issues

Technical mechanisms must be installed and then monitored, in order to implement the security requirements specified by the policies. Procedures must be specified for ensuring that the mechanisms (for example, firewalls) are selected, installed, and monitored.

4. Framework for developing a user organization's Internet security policy

An information security program for an organization consists of various policies and procedures, security education, security management, and a range of security mechanisms [7]. A typical strategy for the engineering of information security comprises four phases [2]: 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; a certification or accreditation phase, which results in a certificate of accreditation being produced, if relevant.

Many methods to develop specific types of security policies have been described [for example, 26], and many structures devised for policies and their subpolicies [for example, 1,20,27]. This paper only considers the development of the Corporate Information Security Policy and its subpolicies to the extent necessary to show the role they play in the development of the Internet security policy.

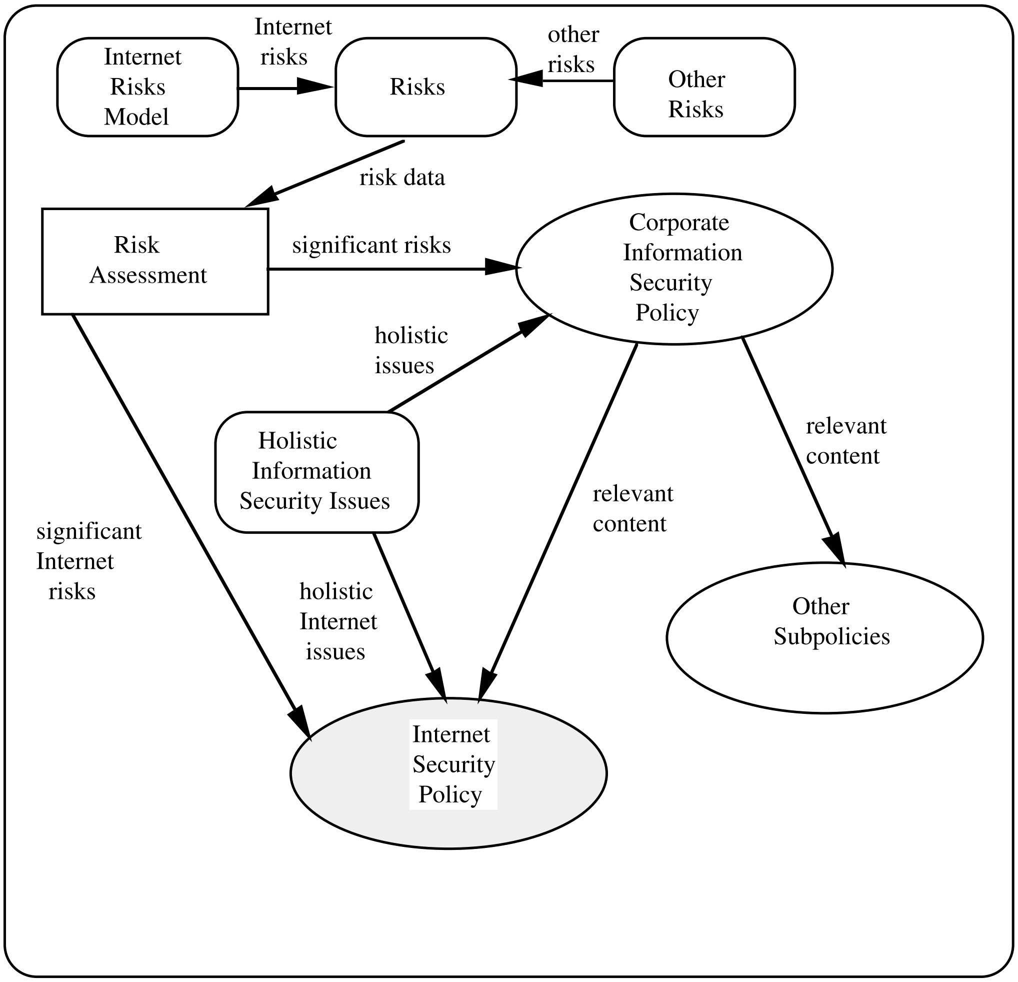

Figure 2. Framework for developing a user organization's Internet security policy

Proceedings of The Thirtieth Annual Hawaii International Conference
on System Sciences ISBN 0-8186-7862-3/97 $17.00 © 1997 IEEE

The Corporate Information Security Policy document is of critical importance to an organisation's information security program. It contains the complete information security requirements for the organization, in the form of layers of policies representing progressively more refined and progressively more rule-like policies, addressing different audiences and different aspects of information security. The creation of appropriate policies involves many choices and decisions, from high-level decisions concerning organisational objectives down to lower-level decisions regarding hardware. The Internet security policy is a subpolicy of the Corporate Information Security Policy, and is therefore determined during the requirements definition phase.

A framework in which to develop a user organization's Internet security policy is illustrated by Fig. 2. A brief explanation of the framework follow: Initially, a risk assessment is carried out to determine and prioritise significant risks for the user organization [31]. The risk assessment uses the Internet risks model in Fig. 1, described earlier, to provide a reference for determining Internet-related risks, which are then added to the other risks which the organization faces. The total set of risk data is then analysed within the risk assessment process, and the results used together with a consideration of holistic information security issues, to determine the Corporate Information Security Policy. Relevant higher-level policies from the corporate document are refined, by considering both the holistic Internet security issues discussed earlier, and the Internet risks, to create the policies which make up the Internet security policy.

5. User organization Internet security policy content

Early work carried out on Internet security policy includes Pethia et al. [28], who discussed policy for the entire Internet community. They recommended that user organizations 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.

The Internet Engineering Task Force 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
- seek technical improvements.

These guidelinelines agree with several important holistic Interent security issues discussed earlier. Branstad et al.'s [5] sample Internet security policy for the NREN (National Research and Education Network) adheres to the IETF guidelines, and includes sections briefly defining objectives, scope, applicability, threats and vulnerabilities, principles, and allocation of responsibilities, for the NREN Internet participant user organizations.

Various types of Internet security policies for user organizations exist, for example the NASA Internet Acceptable Usage Policy [19]. Current organizational Internet security policies appear to be largely Internet acceptable usage policies or Internet information protection policies.

The Internet risk model described in Fig. 1 would suggest that at least the following six subpolicies form part of a user organization's Internet security policy:

Enterprise Internet acceptable usage policy

This policy should contain guidelines for the user organization indicating acceptable and unacceptable uses of their Internet connection.

Employee Internet acceptable usage policy

This policy should contain the security responsibilities for individual employees, and the acceptable and unacceptable purposes for which the employees may use the user organization's Internet connection.

Internet information protection policy

This policy should contain guidelines for the protection of the user organization's information resources from risks emanating from other Internet participants.

Internet information publication policy

This policy should contain guidelines for the division, allocation, electronic publication and dissemination of information via the Internet.

Internet information access policy

This policy should contain guidelines for allowing and disallowing access to a user organization's information resources via the Internet.

Internet employee privacy protection policy

This policy should contain guidelines for providing a user organization's employees with privacy protection from other Internet participants.

6. Research evaluation and conclusion

This section discusses the research results embodied by the framework for developing an Internet security policy which has been described in this paper. The framework in its current form may prove to be a useful tool in the development of a user organization's Internet security policy. It also offers a number of opportunities for further research.

The Internet risks model is a high-level description of Internet risks. It would be useful to identify specific Internet risks, and then classify each risk within the risk groups used by the model. This would improve the usefulness of the model.

Holistic Internet issues are of great importance, and deserve a more thorough investigation than was possible in this work. In particular, the ethical, social and cultural issues are intriguing and complex, but have an important effect on the effectiveness of any implemented Internet security policy.

A rigorous method, to improve on the framework presented here, is required for the developing of the Internet security policy. The content and the structuring of content are also as yet ill-defined. The exact relationship between various types of security policies, and the Internet security policy, needs to be defined. Guidance in these areas may be forthcoming [for example, 10], however investigations should be continued independently.

Empirical work to explore this area would be worthwhile. For example, case studies of user organizations in order to determine their current and planned views, policies and procedures, would contribute useful data.

Current and planned research activities include:

- identification and classification of Internet risks;
- investigation of holistic Internet security issues;
- refinement of the framework for developing a user organization's Internet security policy;
- investigation of content and structure of a user organization's Internet security policy

Given the early stage of research into the development of all kinds of Internet security policy, there is much work ahead. Several avenues of investigation have been suggested above, and no doubt others are awaiting identification.

7. Acknowledgments

The author would like to thank Associate Professor Paula Swatman for her helpful comments.

8. References

[1] Abrams, M.D. and Bailey, D. (1995a) "Abstraction and Refinement of Layered Security Policy", in *Information Security - an Integrated Collection of Essays* (Abrams, M.D., Jajodia, S. and Podell, H.J., eds.), IEEE Computer Society Press, Los Alamitos, California.

[2] Abrams, M.D., Podell, H.J. and Gambel, D.W.(1995b) "Security Engineering", in *Information Security - an Integrated Collection of Essays* (Abrams, M.D., Jajodia, S. and Podell, H.J., eds.), IEEE Computer Society Press, Los Alamitos, California.

[3] Baskerville, R. (1988)*Designing Information Systems Security*, John Wiley.

[4] Beker, H. (1994) *Security Research for the Financial Sector*, in *Proceedings Third European Symposium on Research in Computer Security*, Brighton, UK.

[5] Branstad, D., Oldehoff, A., Aiken, R. and others (1995) *Security Policy for Use of the National Research and Education Network*, in Federal Networking Council (1995a), Appendix 4.

[6] Cheswick, W. and Bellovin, S. (1994) *Firewalls and Internet Security*, Massachusetts, USA: Addison-Wesley Publishing Company.

[7] Doddrell, G. R. (1995) "Information Security and the Internet", *Information Management & Computer Security*, 3(4).

[8] FNC (Federal Networking Council) (1995a) *FEDERAL INTERNET SECURITY - A Framework for Action - Draft*, Federal Networking Council, Security Working Group.

[9] FNC (Federal Networking Council) (1995b) *Federal Internet Security Plan (FISP)*. Federal Networking Council, Security Working Group.

[10] FNC (Federal Networking Council) (1996) Proceedings Internet Privacy and Security Workshop, Mass.

[11] Hartmann, A. (1995) "Comprehensive Information Technology Security": A New Approach to Respond Ethical and Social Issues Surrounding Information Security in the 21st Century, in *Information Security - the Next Decade, IFIP/Sec '95*, *Proc. of the IFIP TC11 Eleventh International Conference on Information Security,* Chapman and Hall.

[12] Highland, H.H. (1996) "Random Bits and Bytes", *Computers & Security*, 15(1).

[13] Hitchings, J. (1995) "Achieving an Integrated Design: The Way Forward for Information Security", in J.H.P. Eloff and H.S. Von Solms (eds.), *Information Security - the Next Decade, IFIP/Sec '95*, *Proc. of the IFIP TC11 Eleventh International Conference on Information Security,* Chapman and Hall.

[14] IETF (1991) *Site Security Handbook*, Holbrook, P. and Reynolds, J. (eds.)

[15] Kaspersen, H. (1992) "Security measures, standardisation and the law", in R. Aiken (ed.), *INFORMATION PROCESSING 92 - Proceedings of the IFIP 12th World Computer Congress.*

[16] Lichtenstein, S. (1996) *Information Security Principles: a Holistic View*, Working Paper 3/96, Department of Information Systems, Monash University, Melbourne, Australia.

[17] Mathieu, R. G. and Woodard, R. L. (1995) "Data Integrity and the Internet: implications for management", *Information Management & Computer Security*, 3(2).

[18] McGuire, R. (1995) *Dealing With Insecurity: Progress Towards a Secure Internet*, NEIUC, 1(4),Wilnet Internet Services.

[19] NASA (1996*) NASA Internet Acceptable Usage Policy*, NASA.

[20] NIST (1994) *Computer Security Policy*, Computer Systems Laboratory Bulletin.

[21] NIST (1996) *The World Wide Web: Managing Security Risks*, Computer Systems Laboratory Bulletin.

[22] 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.

[23] 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.

[24] OECD (1992) *Guidelines for the Security of Information Systems*, OECD/GD(92)190, Paris.

[25] OED (1992) *The Shorter Oxford English Dictionary of Historical Principle,* Clarendon Press, Oxford.

[26] Olnes, J. (1994) "Development of security policies", *Computers & Security*, 13(8).

[27] Olson, I.M. and Abrams, M.D. (1995) "Information Security Policy", in M.D. Abrams, S. Jajodia and H.J. Podell (eds.), *Information Security - an Integrated Collection of Essays*, IEEE Computer Society Press, Los Alamitos, California.

[28] Pethia, R., Crocker, S. and Fraser, B. (1991) *Guidelines for the Secure Operation of the Internet*, IETF RFC1281.

[29] Rannenberg, K. (1994) "Recent Development in Information Technology Security Evaluation - The Need for Evaluation Criteria for Multilateral Security", in R. Sizer, L. Yngstrom, H. Kaspersen and S. Fischer-Hubner (eds.), *Proc. Security and Control of Information Technology in Society,* IFIP Transactions A43, Elsevier Science B.V. (North-Holland).

[30] Von Bertalanffy, L. (1956) "Main Currents in Modern Thought", in *Yearbook of the Society for General Systems Research,* 1.

[31] Wood, C. C. (1995) "Writing InfoSec Policies", *Computers & Security*, 14.

[32] Yngstrom, L. (1995) "A Holistic Approach to IT Security", in J.H.P. Eloff and H.S. Von Solms (eds.), *Information Security - the Next Decade, IFIP/Sec '95*, *Proc. of the IFIP TC11 Eleventh International Conference on Information Security*, Chapman and Hall.

Proceedings of The Thirtieth Annual Hawwaii International Conference
on System Sciences ISBN 0-8186-7862-3/97 $17.00 © 1997 IEEE

IEEE COMPUTER SOCIETY

1060-3425/97 $10.00 (c) 1997 IEEE