Five Dimensions of Information Security Awareness

Mikko T. Siponen
University of Oulu, Department of Information Processing Science,
Linnanmaa, 900014 Oulu University, FINLAND.
e-mail: Mikko.T.Siponen@oulu.fi, Telephone: +358 8 553 1984

Abstract

Until the era of the information society, information security was a concern mainly for organizations whose line of business demanded a high degree of security. However, the growing use of information technology is affecting the status of information security so that it is gradually becoming an area that plays an important role in our everyday lives. As a result, information security issues should now be regarded on a par with other security issues. Using this assertion as the point of departure, this paper outlines the dimensions of information security awareness, namely its organizational, general public, socio-political, computer ethical and institutional education dimensions, along with the categories (or target groups) within each dimension.

1. INTRODUCTION

The relevance of information security awareness is widely agreed upon among information security researchers (e.g. McLean, 1992; Spurling, 1995; Thompson & von Solms, 1997; 1998; Spurling, 1995; Straub & Welke, 1998). The concept of information security awareness is taken in the literature to mean that users should be made aware of security objectives (and further committed to them). Although information security awareness is commonly recognized, there are only a few scientific studies that consider it in any depth; see Siponen (2000) for more on these. Perhaps this situation can be traced back to the non-technical nature of security awareness and related areas. The concept of awareness may have been not considered in greater depth because it falls outside the scope of the traditional engineering and "hard" computer sciences (cf. (Dunlop & Kling, 1993; Ehn, 1989).

Even though researchers interested in information security have recognized the significance of the awareness factor at the organizational level (organizational dimensions in the terminology of this paper), it is curious that they have failed to see its other dimensions. The information society has a powerful need to extend this organizational viewpoint, however. This paper is based on a belief that the concept of information security awareness, in addition to the organizational viewpoint, should also constitute an integral part of the general knowledge of citizens in the information society. In other words, anyone who regards information in any form as an important asset (e.g. starting from information that is regarded as private) should be aware of the possible threats related to it.

Particularly due to the Internet, the concern of widening the scope of security awareness is not made up out of the whole cloth. The Internet is currently largely a lawless zone, a playground for a wide variety of undesirable activities, a paradise for all sorts of criminals from drug dealers to terrorists and child abusers (Quirchmayr, 1997). Even some terrorist groups finance their activities through extortion and blackmail (Strassman, 1997; Warren, 1998)–all these with the help of the Internet.

Furthermore, the undesirable activities seem to be on the increase, at least partly because the current technological tendencies favour misusers: costs are at a minimum, the necessary technology is available, the number of potential targets is increasing and the relevant know-how is easily transferable. As the general public commonly browses the Internet for different kinds of services (e.g. shopping), a host of security issues have surfaced along with ethical problems (e.g. the use of cookies has raised informational privacy concerns). Some companies deem the current situation insecure and refrain from doing business on the Internet (Quirchmayr, 1997), while other organizations follow the trend of electronic commerce with or without knowledge of the possible risks involved. On the other hand, the lack of control and global Internet laws encourages less scrupulous companies and a wide variety of criminals/abusers to practice their business on the net. According to Strassman (1997), we also have to deal with organized governmental penetration (including personal data destruction and gathering). Moreover, information security issues are no less significant in terms of risks than other aspects of normal/physical security, because of the role of information: A loss of information may imply other kinds of losses, from the loss of money and "loss of" informational privacy even to loss of life (consider, for example, a hospital environment where all patient records are kept in electronic form). As we have seen, the Internet seems to make "the fundamental dilemma of computer security" even more acute. This dilemma arises from the fact that security-unaware users have a need for security but no expertise in such matters (Gollman, 1999 p. 9-10).

Finally, for different reasons, a lot of people see issues and aspects connected with information technology (IT) through rose-coloured spectacles, often blindly ignoring potential complications. For example, it seems that many companies, individuals and educational institutions think that it is important to increase technical IT skills, to use IT for almost every conceivable purpose and to advance the computerization of society in general. And often the main limits they see for such development are financial restrictions or lack of technical knowledge (which should therefore be increased)! Moreover, catch phrases such as "information revolution" or the names of particular programs (such as WordPerfect) have strong positive metaphorical associations, redolent of paradise (Dunlop & Kling, 1992). In addition, IT is already embedded in our everyday lives to the extent that we often fail to notice it (let alone realize the encapsulated security flaws). All these factors pave the way for misusers. As a result, even occasional net surfers should be aware of basic security issues. Organizational informational security awareness is not sufficient to satisfy the concerns of security–additional dimensions are needed and a proposal is outlined in this paper.

The main contribution and objective of this paper is to outline the various dimensions of information security awareness and to explore certain key issues around these dimensions. Additionally, the categories (or target groups) in each dimension are distinguished. In other words, the scope of this paper is limited to setting up information security dimensions in terms of form and target groups by proposing a framework for awareness perspectives in order to raise certain issues and produce practical examples in the hope of inspiring further research and practical activities around the topic. Conceptual analysis, in the terms of Järvinen (1997), is used as the research approach. In order to justify the dimensions and categories proposed in this paper in the light of this conceptual analysis, a number of practical examples will be provided. The objective of this paper is not to put forward a state of the art collection of security flaws, however, but rather to use the examples to provide a justification for each dimension. Other equally important issues, such as the content of security issues in each dimension (e.g. a list of particular actions that one should take or should not take), fall outside the scope of the present paper. An early version of this paper was presented in International Conference on Information Security (IFIP/Sec'98).

This paper is divided into four sections as follows. At the beginning of the second section the proposed information security dimensions are outlined and each dimension of information security awareness is considered. The discussion on the 'organizational dimension' mainly summarises briefly what has been contributed already in the field. In the third section, selected implementation issues are considered. Finally, the summary section highlights the key issues of the paper.

2. DIMENSIONS OF INFORMATION SECURITY AWARENESS

As mentioned earlier, the dimensions of security awareness are based on the belief that awareness is an issue that everyone using any form of IT services, either directly or indirectly, particularly in an Internet environment, should bear in mind. It is possible that a wider knowledge of these awareness dimensions may have negative consequences if it is used to commit abuses (this may be true of all kinds of knowledge, of course), and this may be one reason why information is not shared equally among the parties mentioned below. In an attempt to formalize an essentially informal issue with various aspects into an understandable pattern, the dimensions of awareness may be classified as follows:

Because of the informal nature of information security awareness, there may not be any exact and clear borders between these dimensions. Within the organizational dimension, for instance, we have to take into account issues that belong to the general public dimension.

Two very different characteristics of information security awareness have to be considered. The first relates to the division between descriptive and prescriptive, as modified and simplified from the theory of universal prescriptivism by R.M. Hare (1952). The term prescriptive denotes here (only) intrinsic, action-guiding commitment to the objectives of awareness (e.g. security guidelines), while descriptive, albeit including some level of knowledge of information security, may not include such an action-guiding commitment to objectives. Ideally, the objective of the organizational dimension of informational security awareness, at least from the organizational point of view, is to achieve the stage of prescriptiveness, i.e. that users should be intrinsically committed to the security objectives of the organization (Siponen, 2000). Other dimensions of information security awareness are classified as descriptive, as commitment to certain security norms may not be necessary (see the Discussion section).

As a second characteristic, it seems to be that security awareness may be difficult to internalize properly in the sense that it may often be regarded in the same way as a matter of health; nothing is done as long as nothing goes wrong. And when things do go wrong, people are suddenly very keen on the issue. The problem is that when something undesirable happens, it often requires a huge effort to recover from the situation, if recovery is possible at all any longer.

2.1 The organizational dimension

There seems to be common agreement that security awareness (like education) plays a significant role in the overall security level of any organisation (e.g. Ceraolo, 1996; Thompson & von Solms, 1997; 1998; Spurling, 1995; SSE-CMM, 1999a; 1999b; Straub & Welke, 1998). Without an adequate level of awareness, many security techniques are liable to be misused or misinterpreted by their users, the possible result being that even an adequate security mechanism may become inadequate. Several approaches to increasing user commitment to organizational security guidelines have been presented (McLean, 1992; Thompson & von Solms, 1997; 1998; Spurling, 1995; Siponen, 2000). But most of these fail to pay enough attention to behavioural theories, and the empirical studies based on behavioural theories are especially urgently needed (Siponen, 2000). Moreover, measurements of the adequacy of awareness approaches (e.g. whether the motivation of end-users towards security missions or end-user guidelines has increased) are far and few between and this is still an open issue.

The categories of the organizational dimension of awareness discussed here refer to different target groups for security awareness at an organizational level. Examples of these categories may include the following: top management, IT/IS management, information security staff, computing/IS professionals, end-users of various kinds (e.g., casual end-users, parametric end-users, sophisticated end-users and stand-alone users) and third parties.

From the organizational point of view, the five target groups mentioned above (referred to as categories within this dimension) need different kinds of information on security.

With respect to the top management category, awareness is most closely related to the gap between top management and information security concerns. In this respect, the main objectives of awareness are A) getting the commitment of the top management (Perry, 1985; Parker, 1998); B) reaching an exact understanding and consensus within the top management as to what components of the organization require protection (along with the nature of that protection). With regard to the latter, it is essential that security resources are not used in an irrelevant way owing to a misunderstanding of the mission strategy and business environment of the organization in question, for example.

The other possible categories starting from IT/IS management and going on to normal end-users are largely about sealing the gap between information security and the various target groups of the awareness programme (such as those mentioned). Necessary information concerning information security issues must be shared, and this information must be clarified to all the target groups to enable them to reach a state of commitment (the ideal state from an information security point of view).

Finally, the third party category of the organizational dimension of awareness consists of factors by which the company ensures that third parties are aware of the required information security level.

2.2 The general public dimension

The general public dimension can be divided into two target groups: IT/computer/IS professionals and other end-users. The professional skills of IT/computer professionals should include certain knowledge related to security. Consequently, professional qualifications should be established that harmonize and develop these skills alongside others. Furthermore, the professional associations should co-operate with educational institutions to manage this procedure and to determine the content of the relevant knowledge and skills.

The main objective in terms of the other target group of the general public dimension is to increase public awareness of relevant security issues. The main idea of this dimension is based on the argument that there are some central information security issues that every citizen using IT should be aware of. These issues are no less relevant than "normal" security issues[1], which are often regarded as a part of general knowledge these days. This knowledge should now include information security issues as well. Although the Internet is one of the main causes behind this concern, there are many other information security threats not related to it, such as cash and smart cards (as used by ATM machines, mobile phones, etc) (see Anderson, 1993; Anderson & Kuhn, 1996; Gollman, 1996). As far as the Internet is concerned, there are possible dangers for occasional net surfers. To give an example[2] of such a threat, consider a form of impersonation (in the WWW-environment) in which someone pretends to represent a bank or store, for example, in order to obtain money or critical information. Malicious impersonation can also include free upgrades, cyber friends[3], or customer support (Strassman, 1997). The use of cookies has also raised concerns regarding informational privacy (e.g. Rubin & Geer, 1998) and debates on whether cookies are morally acceptable (e.g. Lin & Loui, 1998). The collection of "user information" (e.g. log information) by electronic marts (e.g. to provide customised services) has also raised concerns over informational privacy (e.g. Clarke, 1999), and the Java problems (see Dean *et al.*, 1996) and bugs related to web browsers are questions which also concern home end-users. Moving from these examples to a hypothetical one, we must first remember that the Internet is a complex and rather disordered source of information. As a consequence, so-called WWW agents/robots have been developed to solve the problem of searching for specific information amid this immense collection of data. However, when an agent filters all the information that a person accesses, there is a risk that the person's view of the topic will narrow. This may be a threat, since it could be assumed that only a small number of people understand agent technology and possess the relevant technical knowledge, with the result that they are the only ones capable of studying agent activities in a critical, objective way. This offers the designers of such agents an opportunity to manipulate people's minds by producing agent technology that filters away information that is not in accordance with a certain ideology. Additionally, in shopping via electronic markets, such agents, programmed to behave maliciously, could disclose financial information such as credit card status to unauthorized parties.

There are many other common practices that, if not carried out carefully, could constitute a security threat[4]. Perhaps the most common ones include the failure to observe adequate password procedures etc. (e.g. Gong *et al.*, 1993) and careless use of the Common Gateway Interface (CGI) or Application Programmer Interface (Garfinkel & Spafford, 1997). These practices, if neglected or undertaken carelessly, offer an easy way for misusers and criminals to violate the system and the users' (account holders) informational privacy and assets.

The Internet is also home to various forms of organized crime (including drug-related crimes, crimes against minors, technology transfer, product privacy) and local crime with a global impact (such as economic crimes, violations of human rights, transitional gang activities) (Quirchmayr, 1997). Social engineering methods are also widely employed, and they tend to be very effective (e.g. Dowd & McHenry, 1998), not just owing to the frailties of human nature, but also due to an inadequate level of information security awareness–people are not aware of such dangers. In addition to the possible problem areas briefly discussed here, Internet users, (organizations and individuals alike) should also consider carefully what information they put on their homepage, plan file (which is accessible via a finger command), voice mail, e-mail, speak mail, etc. Many people may not yet be aware of the insecurity of the Internet per se (as the TCP/IP protocol family is insecure without the use of additional cryptographic techniques, see Atkins *et al.* (1997); Bishop *et al.* (1997); Al-Salqan (1997); Gollman (1999) and may send "classified" information by it (e.g. credit card numbers).

2.3 The socio-political dimension

The socio-political dimension involves increasing people's information security awareness with respect to the socio-political nature of IT. This dimension includes the following categories (target groups): lawyers, public relations people, politicians and the government. Information security awareness is an important concern within the socio-political dimension and an important factor in terms of the overall well-being of society. The examples already given in the introduction and section 2.2 attempted to provide an indication of this. In addition to these, many countries are developing electronic services for official communications and trading. Failures to see the importance of security issues related to such solutions may lead to serious complications in terms of the well-being of the society in question.

Laws are another case in point. As we know, legislation is often said to be lagging behind current technological development (e.g. Quirchmayr, 1997). Nevertheless, in order to be successful, it should reflect the moral view of society in question. For that reason, politicians should be aware of information security issues in high-level and ethical principles, because, at least in democratic societies, they are directly or indirectly responsible for making legislative decisions. Hence–along with lawyers–they should understand information security issues at a high-level. Unfortunately, legislative decisions are sometimes, if not always, dictated at present by economic or political perspectives (or even pressures), and politicians may fail to recognize the moral conceptions underlying their decisions even though their objectives may be good–e.g. to promote justice. If the moral perspective of IT is neglected, a moral/legislative gap may emerge, implying conceptualist laws (laws for which the moral background has not been explored), which may be detrimental to human well-being[5]. Many juridical experts on IT legislation are convinced that the Internet will force the introduction of some form of global legislation, and various pressure groups such as the EU and the UN are already starting to push in this direction (Quirchmayr, 1997). One weakness, however, may be that too few people in these circles have an adequate knowledge of security issues[6], for many of these issues require thorough contemplation with the help of ethical theories and facts (including security issues).

Finally, public relations people are also key players in the security game, because they are in a position to inform people of various information security issues. Information security practitioners should ensure the co-operation of this group in order to be able to influence the general public dimension through them.

2.4 The computer ethical dimension

The objective of the computer ethical dimension is first of all to provide relevant (e.g. technical) information for (computer) ethics scholars, and secondly to learn from and make use of their conclusions. These scholars study, among other things, ethical dilemmas and problems, and there is a strong demand to produce continuously updated issues (e.g. technical facts) that covers the whole area of IT. Information security researchers are likely to be helpful in providing information concerning security issues which computer ethics scholars can use when studying its moral dimensions. Co-operation and sharing of information between information security people and computer ethics scholars have so far been ineffective, in spite of the fact that many such issues offer possibilities for synergism (they might share some of the same goals, for example). Computer ethics can perhaps be defined as an approach for finding the best solution to the problem of enabling harmonious human life in the information technology domain. Although information security is not ethics (nor vice-versa), information security (or security generally) may have a certain special connection with the field of ethics. This does not mean that security activities are more right *per se* than any other activities, whether scientific or practical (and as a result we should analyse all activities equally from a moral point of view). Instead, this special connection means that security activities, whether in terms of science or practice, are mainly stimulated by a concern to prevent certain activities that are interpreted as abuses. Moreover, demands have been raised by computer ethics scholars to develop (more specific) professional norms (McFarland, 1990; Walsham, 1996), the creation of which may benefit technical facts on information security–even though not purely based on these[7].

In addition, issues related to (computer) ethics are intimately connected with legislative issues: behind successful legislation there is a moral dimension. Without a moral consensus, laws tend to be ignored, regardless whether the law is considered important–a lesson that the information age needs to learn (Severson, 1997). As Kohlberg recognized, arguments appealing purely to legislation (e.g. "because this is the law or rule"), are not sufficient *per se* to qualify peoples actions (Kohlberg, 1981). Therefore, a one possible mission of this dimension, from an information security point of view, should include the provision of persuasive arguments for legislation (presuming, of course, that the legislation would stand up to closer moral scrutiny–and therefore perhaps avoiding indoctrination). As a result, the computer ethical dimension is important for information security. If people were to regard particular security breaches, misuses or abuses (e.g. distribution of viruses) as immoral, they might avoid them. Security people (or those concerned about security) would likely to be beneficiaries of a strengthening in moral thinking in the area of computing.

2.5 The institutional education dimension

Institutional education refers to a society-driven process of education that is aimed at making individuals proper members of society. In this way, society–ideally–will develop and renew its culture in a desirable way (and hopefully in a way that is not based on indoctrination). However, the amount of technical education provided with respect to computers is increasing, and organizations are increasingly using computers and global computer networks such as the Internet. Unfortunately, as a result of this (and without any information security awareness), the sheer number of people who constitute a potential target for criminals and misusers is increasing (selected high-level technical examples of such activities were given in section 2.2).

Consequently, certain relevant information security concerns should be included in the educational programmes, which is seldom the case at present. The Council of European Professional Informatics Societies (CEPIS), for instance, has established the European computer driving licence (ECDL), which is intended to serve as a multinational standard testifying to a certain competence. Alas, the CEPIS seems to be concentrating only on technical skills, while ignoring the relevant social, ethical and security aspects encapsulated in IT.

Moreover, the increasing number of home Internet users and organizational end-users with little knowledge may cause damage through careless use (virus distribution and creation are cases in point). From the point of view of educational institutes, the former case raises the need for providing relevant computer ethical education. Educational institutes play an important role in this, for in addition to imparting technical knowledge, they also teach ethics and bring up ethical topics for discussion. To summarise, the mission within this dimension is to share relevant information with various educational institutes (referred to as categories within this dimension), bearing in mind the fact that they have different educational needs.

3. DISCUSSION

It is argued above that the organizational dimension of information security has prescriptiveness as its goal, as mentioned at the beginning of the second section. The other dimensions are regarded as descriptive, mainly for two reasons. First, the stage of prescriptiveness may be difficult to put into practice in the case of the other dimensions (this may even be so within the organizational dimension), and secondly, prescriptiveness (or commitment) as an objective may raise an ethical concern, namely the danger of indoctrination.

This paper started off with the problem of what information should be given to the different target groups, because, as shown earlier, this information can be used to commit computer crimes or other kinds of malpractice. The conclusion was that target groups should receive only information that is relevant to their needs. As a result, there should be a classification of what is relevant/irrelevant information for each target group. One problem in this approach is deciding on the classification scheme to be followed, and another is that, due to the dynamic nature of IT, the exact scope of information is difficult to pin down. One possible solution could be a multinational organization offering regularly maintained standards in that respect.

Efforts should be made to avoid indoctrination. Security matters, since they are factual, may not entail a problem of indoctrination and therefore can be approached through international standards, for instance. Moral education (e.g. concerning the morally right use of computing) and education in legislation (e.g. issues such as what legislation should cover and why one should follow it) are more vulnerable to indoctrination, and the use of multinational organizations, even the UN, may not be a panacea in these cases, for there is a possibility that the decisions of such organizations could be driven by political pressures in a negative sense, perhaps ignoring questions of right and wrong. It cannot be taken for granted that all decisions made by the UN, for example, are truly based on concern for what is morally right or wrong, As they may be (in some respects) biased towards the interests of particular countries or people (which the UN represents). It is suggested by R.M. Hare that, to avoid indoctrination, "*what has to be passed on is not any specific moral principle* [nor a list of acceptable or unacceptable acts], *but an understanding of what morality is and a readiness to think in a moral way and act accordingly*" (Hare, 1964). In other words, he sees that the teacher's task is the same in moral questions as in mathematics, for example: it is not to give the right answers but to help the students to learn the means to perform the decisions or calculations for themselves (Hare, 1975) and to give them an eager desire to find the answers (Hare, 1976). Hare (1964) maintains that since it may be difficult to start education with abstract concepts (or meta-analysis), we need to use concrete examples, and the principles that we hold in best regard should be used for that purpose. In that case indoctrination can be avoided if we are ready to accept that students have the same liberty to choose their principles.

Furthermore, each target group should have its own specific goals, which should be based on careful consideration of the most relevant issues that it needs to know. This is something that can be left for future research.

4. CONCLUSIONS

The continually increasing use of IT and computerization stresses the importance of information security, and particularly individual awareness of this. Thus other dimensions are needed in addition to organizational ones. To address this need, awareness can be divided into five dimensions; namely, organizational, general public, socio-political, computer ethical and institutional education. The general public dimension is needed to inform ordinary computer users about the risks related to use of the Internet, for example. As for the last dimension, educational institutions should develop education in computer ethics in parallel with technical education, in addition to discussing issues related to information security awareness. Within each dimension the different target groups need different kinds of information. Relevant issues and goals should be considered, partly for security reasons and ethical reasons, and partly in order to maximize resources. Organizations such as professional bodies and education institutes should take the reins in order to keep such a process on the right track.

REFERENCES

Al-Salqan, Y.Y., (1997), Future Trends in Internet Security. *Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing.*

Anderson, R., (1993), Why Cryptosystems Fail. *Communication of the ACM*, November, vol. 37, no.11, pp. 32-44.

Anderson, R., & Kuhn, M., (1996), Tamper Resistance--a Cautionary Note. The *Second USENIX Workshop on Electronic Commerce Proceedings*, Oakland, California, November 18-21.

Atkins, D., Buis, P., Hare, C., Kelley, R., Nachenberg, C., Nelson, A.B., Phillips, P., Ritchey, T., Sheldon, T., Snyder, J., (1997), *Internet Security: Professionals Reference*. Second edition, New Riders Publishing, Indianapolis, USA.

Bishop, M., Cheung, S, Wee, C., (1997), The threat from the net [Internet security]. *IEEE Spectrum*, vol. 34, issue 8.

Ceraolo, J.P., (1996), Penetration Testing Through Social Engineering. *Information Systems Security.* Vol 4, No 4. Winter.

Clarke, R., (1999), Internet privacy concerns confirms the case for intervention. *Communications of the ACM.* Vol. 42, issue 2, pp. 60-67.

Dean, D., Felten, E.W., Wallach, D.S., (1996), Java security: from HotJava to Netscape and beyond. *Proceedings of the 1996 IEEE Symposium on Security and Privacy.*

Dowd, P.W. & McHenry, J.T., (1998), Network Security: It's Time to Take It Seriously. *IEEE Computers.* Vol. 31, Issue 9, September, pp. 24-28.

Dunlop, C. & Kling, R., (1992), Social Relationships in Electronic Commerce– Introduction. In *Computerization and Controversy - Value Conflicts and Social change*, (ed. C. Dunlop and R. Kling). Academic Press, New York, USA.

Ehn, P., (1989), Work-Oriented Desing of Computer Artifacts, *Arbetslivecentrum*, Stockholm. U.S Edition: Lawrence Erlbaum, New Jersey, 1989.

Garfinkel, S. & Spafford, G., (1997), *Web Security & Commerce.* O'Reilly & Associates.

Gollman, D., (1999), *Computer Security.* John Wiley & Sons, UK.

Gong, L., Lomas, M.A., Needham, R.M., & Saltzer, J.H., (1993), Protecting poorly chosen secrets from guessing attacks. *IEEE Journal on Selected Areas in Communication*. Vol. 11, Issue 5, pp. 648-656.

Hare, R. M., (1952), *The Language of Morals.* Oxford University Press, Oxford, UK.

Hare, R.M., (1964), Adolescents into Adults. In: *Aims in Education* (eds): T.C.B. Hollins, Manchester. Reprinted in *Essays on Religion and Education* (eds): R.M. Harc. Oxford University Press, 1992.

Hare, R.M., (1975), Autonomy as an Educational Idea. In: *Philosophers Discuss Education* (eds): S.C. Brown. Macmillan.

Hare, R.M., (1976), Value Education in a Pluralist Society: A Philosophical glance at the Humanities Curriculum Project. *Proceedings of the Education Society of Great Britain*. Reprinted in *Essays on Religion and Education* (eds): R.M. Harc. Oxford University Press, 1992.

Hare, R.M., (1981), *Moral Thinking: Its levels, method and point.* Oxford University Press, UK.

Hare, R.M., (1985), Ontology in Ethics. In *Morality and Objectivity: Essays in Memory of John Mackie* (eds): T. Honderich. Routledge.

Järvinen, P., (1997), The new classification of research approaches. *The IFIP Pink Summary–36 years of IFIP.* Edited by H. Zemanek, Laxenburg, IFIP.

Kohlberg, L., (1981), *The Philosophy of Moral Development.* San Francisco, USA.

Lin, D. & Loui, M.C., (1998), Taking the byte out of cookies: privacy, consent, and the Web. *ACM Computers & Society.* Vol. 28., No. 2. June.

McFarland, M. C., (1990), Urgency of ethical standards intensifies in the computer community. *IEEE Computer*, Vol. 23, No. 3, March.

McLean, K., (1992), Information Security Awareness - Selling the Cause. *Proceedings of the IFIP TC11 /Sec'92*, Singapore, 27-29 May.

Parker, D. B., (1981), *Computer Security Management.* Prentice Hall, Reston, USA.

Parker, D. B., (1998), *Fighting Computer Crime–A New Framework for Protecting Information.* Wiley Computer Publishing. USA.

Perry, W. E., (1985), *Management Strategies for Computer Security.* Butterworth Publisher, Boston.

Quirchmayr, G., (1997), Selected Legal Issues Related to Internet Use. *3rd International Conference on Reliability, Quality & Safety of Software-Intensive Systems (ENCRESS'97)*, 29-30 May, Athens.

Rogerson, S., (1996), The Ethics of Computing: the First and Second Generation. *The Business Ethics Network News*, Issue 6.

Rubin, A.D., & Geer, D.E., (1998), A Survey of Web Security. *IEEE Computer*, Vol. 31, Issue 9, September, pp. 34-41.

Severson, R. J., (1997), *The Principles of Information Ethics.* Armonk (N.Y.) M. E. Sharpe Co. (tai mitä "cop" tarkoittaa?) USA.

Siponen, M.T., (2000), A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security.* Volume 8, Issue 1.

Spurling, P., (1995), Promoting Security awareness and commitment. *Information Management and Computer Security*, Vol. 3 No. 2., pp. 20-26.

SSE-CMM, (1998a), *The Model.* v2.0. http://www.sse-cmm.org.

SSE-CMM, (1998b), *The Appraisal Method.* v2.0. http://www.sse-cmm.org.

Strassman, P.A., (1997), Auditing the Reliability of the Information Infrastructure. Keynote Presentation in *25th Annual International Conference, Information Systems Audit and Control Association*, Washington, DC area, 20-23 July. USA.

Straub, D.W. & Welke, R.J., (1998), Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, Vol. 22, No. 4, p. 441-464.

Thompson, M.E. & von Solms, R., (1997), An effective information security awareness program for industry. Proceedings of WG11.2 and WG11.1 of TC11 (IFIP): *Information Security -from small systems to Management of Security Infrastructure.*

Thomson, M.E. & von Solms, R., (1998), Information security awareness: educating our users effectively. *Information Management & Computer Security*. Vol. 6, no. 4, pp. 167-173.

Walsham, G., (1996), Ethical theory, Codes of ethics and IS practice. *Information System Journal*, Volume 6, Number 1, January.

Warren M.J., (1998), Cyber Terrorism. *Proceedings of the 14th Conference on Information Systems Security (SEC'98, TC11).*

Notes:

[1] Normal security refers to such security concerns as not using electrical appliances while taking a shower, etc.

[2] There are countless appropriate real life examples, but they fall outside the scope of this paper.

[3] Ironically, it seems that "chat sites" and other public communication sites on the net sometimes even foster personal trust and intimacy (Dunlop & Kling, 1993).

[4] Of course, there are many other insecure practices as well, but as mentioned before, listing such flaws is not within the scope of this paper.

[5] Because people use their moral judgement in their decision making and are therefore more likely to base their lives on values than on unreasonable rules (e.g. Hare, 1981; Kohlberg, 1981) these are referred to here as conceptualist laws.

[6] Not to mention the fact that they would be capable of weighing up the moral reasons undermining legislation (that have some relevance to well-being, considering the legislation/moral gap that complicates conceptualist laws).

[7] We believe that right and wrong (what one "ought" to do) cannot be deduced from facts (what "is"). Consider Hume's law "no ought from is" in this regard.