The Various Dimensions of IT Security Awareness

Mikko T. Siponen Jorma Kajava

Department of Information Processing
Science,University of Oulu,
FINLAND
E-mail:{Mikko.T.Siponen, Jorma.Kajava}@oulu.fi

ABSTRACT

Until recently, information technology (IT) security was mainly an area of concern for corporations whose line of business demanded a high degree of security. However, the growing use of IT is affecting the status of IT security such that it is gradually becoming an area that plays an important role in our everyday lives. As a result, IT security issues are now on a par with other security issues. In this paper, we discuss and outline the different dimensions of IT security awareness.

KEYWORDS: IT Security, Information Security Awareness, Social Aspects of Computing, Security Threats

1. BACKGROUND

A number of papers presented at recent IT security seminars have championed IT security awareness as the best preventive measure against the biggest weakness in all systems: the human factor [1]. Industrial life, however, seems to have a different view of the value of awareness: IT security awareness is only too often interpreted either as a trivial function or – at best - a necessary evil. Perhaps this attitude can be traced back to the non-technical nature of the function: the value of awareness is not recognized because awareness falls outside the scope of the engineering sciences[1]. But things are changing, and awareness is no longer an irrelevant issue. In fact, the awareness factor should form the basis of the security strategy of any organization [1;6;7;14;16] and it should also constitute an integral part of the general knowledge of the citizens of the modern information society. Sometimes the role of security awareness is not internalized properly, and it is regarded merely as a matter of security or health. Consequently, nothing is done as long as everything is all right. The problem is that when something undesirable happens, it often requires a huge effort to recover from the situation.

[1] It is a common misconception that the foundation of computer (or IT) science is mathematical analysis [2], because computer science is often interpreted as a technical discipline. It has been said [3] that although the mathematical approach is inappropriate in many cases, there is no alternative education either, focusing on the non-mathematical aspects computing [2].

Moreover, it has been said that we are under the spell of IT technology. Somehow people seem to think that everything that is somehow connected to IT is good a thing. Therefore, many companies, individuals and educational institutes think that it is important to develop IT skills, to use IT for every conceivable purpose and to advance the computerization[2] of society in general. Catch phrases such as 'information revolution' or the names of particular programs[3] have strong positive metaphorical associations, redolent of paradise [2]. In addition, IT technology is already embedded in our everyday lives to the extent that we often fail to notice it. All these factors pave the way for misusers.

1.1 Motivation

Even though the significance of the awareness factor has finally been recognised by IT security researchers, its various perspectives are not. The Internet is still largely a lawless zone, a playground for a wide variety of undesirable criminal activities, a paradise for all sorts of criminals from drug dealers to terrorists and child abusers. It is also a place where intellectual property rights are consistently ignored [11]. Many terrorist groups finance their activities through extortion, blackmail (personal and international) and other crimes [15] like hacking and "faking". Some terrorist activities target advanced industrial nations [15]. Criminal 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 transportable. Because the general public commonly browses the Internet for different kinds of services, a host of security issues have surfaced along with ethical (even moral) problems. As a consequence, increasing organisational awareness does not suffice as a security measure. Many companies deem the current situation unsafe and refrain from doing business on the Internet [11], while the lack of control and global Internet laws encourages less scrupulous companies and a wide variety of criminals to practice their business on the net. According to [15], we also have to deal with organized governmental penetration (including data destruction and gathering). Moreover, IT security issues are more complex in terms of risks than other aspects of security, because, in addition to loss of money, assets or even life, IT security also includes a host of problems centring on privacy. As a result, even occasional net surfers have to be aware of basic security issues.

1.2 Research questions and the scope of the paper

In this paper, we shall outline the different dimensions of IT security awareness and explore some key issues around these dimensions. We shall also discuss target groups in each dimension. In other words, the scope of this paper is limited to setting up IT security dimensions in terms of form and target group. Our main purpose is to formulate a framework for different awareness perspectives in order to raise certain issues and produce practical examples in the hope of inspiring further research around the topic. Although we shall provide a number of practical examples, the objective of this paper is not to put forward a state of the art collection of security flaws; rather, the examples are

[2] We do not claim that this happens universally. Moreover, we do not wish to take a stand on the ultimate strength or weakness of this attitude.
[3] Word Perfect is a case in point.

used to provide justification for each dimension. Other, equally important, issues such as the content of security issues in each dimension, fall outside the scope of the present paper.

1.3 IT Security Awareness

By studying actual end-user practices we have come to the conclusion that there are three stages in how people respond to awareness[4] issues. We maintain that people progress upwards or regress downwards as a measure of the success or failure of IT security awareness. The stages of IT security awareness are [6]:

1. drawing people's attention to security issues,
2. getting user acceptance,
3. getting users to learn and internalize the necessary information security activities.

The first stage includes drawing people's attention to information security-related issues and trying to catch their interest. The second stage involves user acceptance. In the case of organizational awareness, for example, having got the end-users' attention, it is important to get them to accept the IT security policy of their organization. Finally, at the third stage[5], the end-users should have internalized the instructions they have received during their security education, and they should take corrective measures in accordance with the security policy of their organization. As mentioned earlier, these stages are derived from empirical research by [6] and have proved most relevant in the case of organisational awareness. However, we argue that other dimensions of awareness can be related to the same stages, even though their emphasis is on stages 1 and 2[6]. Thus, we may talk about prescriptive or descriptive awareness, depending on the dimension we are referring to (see next chapter). Prescriptiveness is the main goal of any organizational awareness program, while descriptiveness suffices to satisfy the requirements of the other dimensions of awareness.

2. DIMENSIONS OF IT SECURITY AWARENESS

We argue that awareness is an aspect whose dimensions are not perceived holistically enough. As mentioned earlier, information security awareness is an issue that everyone using any form of information technology services, either directly or indirectly, should bear in mind. Of course, a wider knowledge of these awareness dimensions may have negative consequences if the knowledge is used to commit IT crimes or other kinds of malpractice. That is one reason why information is not shared equally among the parties mentioned below. Informally, the dimensions of awareness could be classified as follows:

- organizational dimension;
  - top management,
  - IT/IS management;
  - IT security staff;

[4] For a further discussion on IT security awareness and its history, see [6;7]
[5] In the case of organizational awareness.
[6] Because, e.g., in the case of the general public dimension, it may not be relevant to waste resources on trying to reach stage 3, particularly as it would involve a consideration of ethical aspects, etc.

- ADP-professionals;
- end-users (e.g., casual end-users, parametric end-users, sophisticated end-users and stand-alone users)
- third parties,

- general public dimension;
- socio-political dimension (lawyers, public relations people, politicians, etc.);
- computer ethical dimension (co-operation among computer ethics scholars);
- institutional education dimension.

We maintain that there are no 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.

2.1 The organizational dimension

The awareness factor plays a significant role in the overall security level of any organisation. Without an adequate level of awareness, all security techniques are liable to be misused or misinterpreted by users, thereby losing their real usefulness. The time-honoured approach of "giving guidelines" or of arranging training sessions or sending circulars in the hope that the members of the organisation would then strictly follow the given instructions, is by no means sufficient. What is required is a more holistic view of the organizational dimension of awareness.

The tools and methods of any awareness package (including training, education, campaigning and IT security management) should be directed consistently and effectively at increasing security awareness. Moreover, measuring is needed to ascertain that the results of the awareness programme are indeed the intended ones and that the awareness development programme is on the right track.

Apart from the need to formulate a formal holistic approach based on the necessary pre-conditions of awareness (such as getting the commitment of the top management), there is another perspective that must be taken into consideration here; namely, the content of the programme. Content is, indeed, the primary factor, correlating in the final analysis with the extent to which people reach the target level (3) of awareness. It is the content of any awareness programme that ultimately determines its success or failure. Consequently, both the form (the framework) and the content of the awareness programme must be taken into account and they must both reach an adequate level. The five different target groups mentioned above need different kinds of security-related information. In the organizational dimension, the effectiveness of awareness is most closely related to the gap between the top management and IT security concerns. There must exist 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). It is essential that security resources are not used in an irrelevant way owing, for example, to a misunderstanding of the mission strategy and business environment of the organization[7] in question. Additionally, there is often a gap between IT security and the various target

[7] We are looking at the situation from the awareness point of view. Of course, other perspectives may necessitate the estimation of IT security threats.

groups of the awareness programme. Necessary information about IT security issues must be shared, and this information must be clarified to all the target groups to enable them to reach the third stage of awareness. Finally, third party awareness consists of factors whereby the company ensures that third parties are aware of the required IT security level. One level of awareness includes the knowledge that security problems are unavoidable – and that recovery plans and different crisis management plans are a necessity [5].

2.2 The general public dimension

The main objective of the general public dimension is to increase public awareness of relevant security issues. We argue that there are some central IT security issues that every citizen should be aware of. These issues are no less relevant than "normal" security issues[8] which are often regarded as a part of general world knowledge these days. In our view, this knowledge should also include IT security issues. To give an example[9], some UK banks discontinued their WWW services, because they were not secure enough. Other banks using the same services with the same platform and software should inform their customers of the potential IT security risks[10] of the service in question. Another example is "faking", a form of impersonation (in the WWW environment) in which someone pretends to represent a bank or a store to obtain money or critical information. Criminal impersonation also includes free upgrades, cyber friends[11], customer support and insiders [15] (insiders are in fact more of an organizational threat). Moving from these case studies to a hypothetical case, we must first remember the obvious fact that the Internet is a complex, disordered source of information. As a consequence, WWW agents or robots have been designed to solve the problem of searching for specific information amid this immense collection of data [10]. However, when an agent filters all the information that a person accesses, there is a risk that the person's view of the topic narrows [10]. Moreover, 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 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 virtual shopping, agents could disclose financial information such as credit card information to unauthorized parties.

There are additional common practices that constitutive a security threat[12]. For example, the first of these is the failure to observe adequate password procedures, and the second is the use of the CGI standard in homepages. Both practices offer an easy way for misusers and criminals to violate the system and the owner's privacy and assets.

---

[8] By 'normal' we refer to such security concerns as not using electrical appliances when the shower is on, and so on.

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

[10] Naturally, this raises the ethical question of whether these banks should provide the service at all? However, the ethical perspective falls outside the scope of this paper.

[11] It is ironic, but it seems that "chat sites" and other public communication sites on the net sometimes even foster personal trust and intimacy [2].

[12] Of course there are many other unsecure practices, however as mentioned, listing of such flaws is not the aim of this doctrine.

Moreover, the Internet is also home to 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) [11]. In addition to "standard" ways of committing crimes, it is reasonable to expect criminals to use social engineering methods, because they tend to be very effective not just owing to the frailties of human nature, but also due to an inadequate level of IT security awareness [7]. Organisations and individuals alike should consider very carefully what they put on their WWW server, voice mail, e-mail, speak mail, etc. People should keep information about their personal lives and their organisation at a minimum. Critical information encompasses home addresses, phone numbers, pictures, dates of birth, and other similar information. It is particularly ill-advised to publish information about holidays and days-off, or send non-crypted information concerning credit cards on the Internet.

2.3 The socio-political dimension

The socio-political dimension involves increasing the IT security awareness of lawyers, public relations people and politicians. This is an important concern within the socio-political dimension and an important factor in terms of the overall well-being of society. Laws are a case in point in this respect. As we know, legislation usually lags behind the current state of affairs in the real world. For that reason, politicians have to be aware of IT security issues because, directly or indirectly, they make legislative decisions. Hence they – along with lawyers – must understand the basic principles of IT security. At present, legislative decisions are sometimes dictated by economic or political perspectives (or even pressures), and politicians may fail to recognize the underlying moral conceptions of their decisions even though their objectives may be good. We postulate that if the moral foundations of IT are neglected, a moral/legislative gap may emerge implicating conceptualist laws, which is not good for human well-being[13]. Many IT legislation experts are convinced that the world needs global legislation, and different pressure groups such as the G7, EU, OECD and the UN are starting a push in this direction [11]. The fact remains, however, that too few people in these circles have an adequate knowledge of security issues. Moreover, different countries are adopting different approaches to the development of e-mail and other services (such as smart cards) for official communications or for trading. Last but not least, public relations people are also key players in the security game because they are in a position to inform people of various IT security issues. IT security people should ensure the co-operation of this group to be able to influence the general public dimension through their help.

2.4 The computer ethical dimension

The aim of the computer ethical dimension is, first of all, to provide information to computer ethics scholars and, secondly, to learn from their conclusions. These scholars study ethical dilemmas and problems, and there is a strong demand to produce continuously updated material that covers the whole area [11]. IT security concerns are helpful in providing information about security issues which computer ethics scholars can

[13] Because people use their moral judgment in their decision-making.

use when researching 'gaps' in moral and ethical dimensions. Co-operation and sharing of information between IT security people and computer ethics scholars have been highly ineffective so far, in spite of the fact that a lot of issues offer possibilities for synergism (we all share partly the same goals, for example). Computer ethics can be defined as an approach to finding the best solution to the problem of enabling harmonious human life in the information technology domain. [12]. It is obvious that the aforementioned definition is based on the so-called CIA[14] criterion, meaning that the aims of IT security are factors that enable harmonious human life in general. More specifically, computer ethics scholars are developing (more specific) professional norms, which are indirectly correlated to certain security factors. In addition, computer ethics related issues are intimately connected with legislative issues and, generally speaking, the mission of computer ethics should include the provision of persuasive arguments for global legislation. Nevertheless, as current research shows [8;4], laws are not sufficient per se to satisfy people. To fill up this gap, we need ethical discussion, persuasion and reasons for instituting some form of global legislation. This is the mission of computer ethics [11]. As Kohlberg first recognized, pure legal arguments, such as "because this is the law or rule", are not sufficient per se to qualify peoples actions. As a result, the computer ethical dimension is extremely important for IT security. If people intuitively identify particular security breaches, misuses or abuses as immoral, they will avoid them.

2.5 The institutional education dimension

By institutional education we mean a society–driven process of education that is aimed at making individuals members of the society. In this way, society will develop and renew its culture. Needless to say, the amount of technical (IT) education is increasing in different educational institutes, making WWW and e-mail services available to more and more people. This naturally increases the sheer number of people who constitute a potential target for different kinds of criminals and misusers. Hence, we argue that certain relevant IT security concerns should be included in the educational programmes of these institutes. The examples given in chapter 2.2 indicate why this is necessary. Moreover, the increasing number of net users and individual end-users with little knowledge may cause serious damage through misuse (virus creation, hacking, etc.) or a misinterpretation of the use of IT. From the point of view of educational institutes, the former case raises the need of 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 to discussion. To sum up, the mission within this dimension is to share relevant information with various educational institutes, bearing in mind the fact that they have different educational needs.

3. SOME ISSUES CONCERNING THE IMPLEMENTATION OF THE DIMENSIONS OF AWARENESS

We started off with the problem of what information to give to the different target groups, because, as shown earlier, this information can be used to commit IT crimes or other kinds of malpractice. The conclusion was that different target groups should only get information relevant to their needs, and nothing more. As a result, we suggest that

[14] The so-called CIA-model comprises confidentiality, integrity and availability [9].

there should be a classification of what is relevant/irrelevant information for each target group. The problem in this approach is deciding on the classification scheme to be followed, along with the problem that, due to the dynamic nature of IT, the exact scope of information is difficult to pin down. One solution could be a multinational organization offering regularly maintained standards. In addition, certain didactic issues should also be explored, and we would like to challenge different institutions to own up to their responsibility in this matter. Each group should have their own specific goals. These goals should be based on a careful contemplation of the most relevant issues that the target group needs to know.

4. SUMMARY

The increased use of IT stresses the importance of IT security, particularly IT security awareness. This awareness can be divided into five dimensions; namely, organizational, general public, socio-political, computer ethical and institutional education. As to the last dimension, educational institutes should develop computer ethical education in parallel with technical education, in addition to discussing issues related to IT security awareness. Within this dimension, we maintained that the different target groups need different kinds of information. Relevant issues and goals should be deliberated, partly for security reasons and ethical reasons, and partly to maximize resources. Different kinds of global organizations should have a liability for keeping the whole process on the right track.

REFERENCES

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

[2] Dunlop, Charles & Kling, Rop, (1992): Social Relationships in Electronic Commerce - Introduction. In Computerization and Controversy - Value Conflicts and Social change, edited by Charles Dunlop and Rop Kling. Academic Press, New York, USA.

[3] Ehn, Pelle, (1989): Work-Oriented Desing of Computer Artifacts, Arbetslivecentrum, Stockholm. U.S Edition: Lawrence Erlbaum, New Jersey, 1989.

[4] Helkama, Klaus, (1993): Nuoren kehittyvä etiikka (The developed ethics of young). Hyvän opetus (Education of the good), Edited by Timo Airaksinen, Pekka Elo, Klaus Helkama and Bertel Wahlström, painatuskeskus Oy, Helsinki, Finland. In Finnish.

[5] Kajava, J., Siponen, M.T. (1996): Security Management in Organizations - Bottom-Up or Top-Down Approach?" NORDSEC '96 - Nordic Workshop on Secure Computer Systems (ed. Erland Jonsson), SIG Security and Chalmers University of Technology, Department of Computer Engineering, 7 - 8th November 1996, Gothenburg, Sweden.

[6] Kajava, J., Siponen, M.T., (1997 a): Effectively Implemented Information Security Awareness - An Example from University Environment. Proceedings of IFIP-TC 11 (Sec'97/WG 11.1). 13th International Conference on Information Security:

Information Security Management - The Future. 13th May 1997, Copenhagen, Denmark.

[7] Kajava, J., Siponen, M.T., (1997 b): Social Engineering - IT security threat of Informatics. In Kristin Braa & Eric Monteiro (eds.): Proceedings of IRIS 20th, "Social informatics". University of Oslo, Department of Informatics, Conf. Proc. Nr. 1, Part 2, June, Oslo, Norway.

[8] Kohlberg, Lawrence, (1981): The Philosophy of Moral Development. San Francisco, USA.

[9] Parker, Donn, B., (1981): Computer Security Management. Prentice Hall, Reston, USA, 1981.

[10] Pedersen, Christian H., (1996): Agents Searching Information in a Network (Agentit seulovat tietoa verkosta). *Tieteen Kuvalehti* (*Magazine of Science*), No. 6. (in Finnish).

[11] Quirchmayr, Gerald, (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.

[12] Siponen, M.T. & Kajava, J., (1997 a): Computer Ethics - the Most Vital Social Aspect of Computing: Some Themes and Issues concerning Moral and Ethical Problems of IT. In Kristin Braa & Eric Monteiro (eds.): Proceedings of IRIS 20th, "Social informatics". University of Oslo, Department of Informatics, Conf. Proc. Nr. 1, Part 2, June, Oslo, Norway.

[13] Siponen, M.T. & Kajava, J., (1997 b): The Applicability of Ethical Theories in Computer Ethics - Selected Issues. Research Paper Series A 28. Department of Information Processing Science, University Of Oulu. Oulu University Press, Finland.

[14] Solms von, R., (1997): WG11.1 chairman's Foreword. Proceedings of IFIP-TC 11 (Sec'97/WG 11.1). 13th International Conference on Information Security: Information Security Management - The Future. 13th May 1997, Copenhagen, Denmark.

[15] Strassman, Paul 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.

[16] Thompson, T.E & Von Solms, R., (1997): An effective information security awareness program for industry. Proceedings of IFIP-TC 11 (Sec'97/WG 11.1). 13th International Conference on Information Security: Information Security Management - The Future. 13th May 1997, Copenhagen, Denmark.