A Framework for the management of human issues in information security

Jorma Kajava[1], Jussipekka Leiwo[2] and Mikko T. Siponen[1]

[1] University of Oulu, Department of Information Processing Science, Linnanmaa, 90570 Oulu, Finland, {Jorma.Kajava, Mikko.T.Siponen}@oulu.fi

[2] Monash University, PSCIT, McMahons Road, Frankston, Vic 3199, Australia, Jussipekka.Leiwo@fcit.monash.edu.au

Abstract

There is no doubt consideration of human issues is an essential success factor in the management of information security. Several models have been proposed for dealing with complex human issues related to information security and different frameworks and sets of guidelines have been established to guide in the management of end users of systems to achieve adequate security of information systems. Many of these proposals remain on a high level of abstraction, hence making direct applications difficult. This leads easily to unsatisfactory high level descriptions of problems being tackled instead of comprehensive, environment specific solutions. In this paper a systematic approach towards human issues in the security of information systems shall be proposed to clearly identify areas that need to be considered when dealing with human issues of information security.

Keywords: Information Security, Security Management, End-User Security

1 Introduction

Information security is a state of affairs reached when data and information, systems and services, are adequately protected against all threats both in normal times and in times of crisis. Protection methods can be roughly divided into administrative, technical, and other methods. Technical methods comprise of specification and enforcement of technical security services and mechanisms, such as access control, encryption, authentication, integrity and non-repudiation. Administrative methods can be divided into technical administration, usually related to the coordination and maintenance of the above mechanism, and people administration, herein called leadership. Other measures include security enforcement not directly related to any specific technology, such as requirements of trusted implementation of enforcement mechanisms. The major contribution of this paper is to propose a systematic framework for leadership, to be applied in concert with various methods to provide a systematic approach towards human issues in the security of information systems.

An important observation is that information security permeates the whole organisation. The direction is top down, from managers to end-users. The highest level of management must endorse the idea of information security, and the end-users of systems, those to implement the security procedures in daily work, must understand the security principles, and act accordingly. In practice, the management must define the organizational information security policy and enforce it among users of systems and information. End-users must follow the given instructions and information security guidelines. One of the main concerns of managerial information security personnel is to make sure that every user is aware of the importance of information security. Certainty should be reached on the understanding of guidelines and other advisory documents. Education is needed to convince users from the importance of guidelines, and to make the users aware of the consequences of intentional violations of information security [1, 21]. Awareness can be descriptive or prescriptive [20]. Descriptive awareness is the general understanding of underlying protection measures and prescriptive awareness the agreement upon the importance of secure routines for information processing and the commitment into acting accordingly. User awareness is a state to be reached when each individual user understands the principles, functionality and importance of security enforcement technologies, as well as is aware of the specific organisational security policy, and is committed into acting accordingly.

There are several models on the management of information security and the value of non-technical issues has been widely acknowledged [9]. An example is the ISSI model (Information Systems Secure Interconnection) [12], where various non-technical layers are added on OSI communication protocols. The difficulty is that high level issues do not offer enough basis for concrete end user-oriented development of information security. Also, research on information security as specification of structures of responsibility [2] remains on a high level of abstraction. Additionally, many sets of guidelines, such as [8, 11], have been proposed towards information security and end users. Guidelines are effective in practise but, from a scientific point of view, a reasonable primitive mechanism to enforce information security and strongly dependant on the application context. The attempt in this paper is to provide a context independent framework for dealing with human issues in information security by identifying major components and their role in the provision of user-centered information security. The paper starts by a survey of related research to motivate this work in section 2. Section 3 then provides a detailed discussion of specific tasks within the adopted security management framework. Conclusions shall be drawn and directions highlighted for future research in section 4.

2 Background and motivation

The management architecture for information security shall first be summarised in section 2.1. Section 2.2 then summarises the major changes in the 'nformation processing that make it essential to study human issues in information security. Section 2.3 deepens this analysis by studying the role of end users in the provision of comprehensive information security.

2.1 A framework for the management of information security

From a wide point of view, information security can be seen as a provision of layers of protection measures up to ecological and social protection of information systems [9]. Within this paper, the scope is slightly reduced and management of information security is seen as a specification and enforcement of information security meta policies that coordinate actual information security policies [14]. A similar management architecture as in [16] shall be adopted for specifying boundaries of the management of information security. Upper boundary is the formulation of information security requirements based on information security objectives set by the top management. Information security objectives are informal statements regarding desired security of systems and operations and are usually based on different national and international laws, agreements, standards and organisational business objectives. Formulation refers to the presentation of these objectives formally in an unambiguous way. Lower boundary is in the specification of technical security policies based on upper layer security requirements. From a managerial point of view, it can be assumed that once identified and specified, security enforcement mechanisms can be implemented in a secure manner by technical personnel.

Management architecture for information security refers to a generic description of major parties involved in the management of information security, different tasks, and inputs and outputs of these tasks. The architecture assumed in this paper is illustrated in figure 1. The technical track from security objectives and organisational security criteria to specification of technical criteria has been studied in detail in [16]. That discussion covers many aspects of the technical track but only mention the human track. The human track is mostly concerned with delegation of authorities and resources to refined duties and authorisations and non-technical policies and guidelines. Top management of the organisation has duty and authorisation to set organisation wide policies concerning information security. These duties and authorisations are then delegated throughout the organisation, and harmonised to assure from consistency, correctness and optimisation. Managerial information security personnel then comes out with duties and authorisations delegated to specific end users or roles they act in, and different non-technical protection criteria to be followed by end users.

Technical security requirements are processed by formal information security harmonisation functions. These functions assume a formal notation for expressing requirements and are therefore not applicable in human issues. Various factors are needed for enforcing appropriate harmonisation of non-technical security requirements, such as leadership through communication, inspiration and motivation. Number of research suggests that deterrence and other "negative" procedures are effective in preventing violations of security [21, 26] but the value of positive encouragement is not as much studied.

Information security can be seen as specification of structures of responsibilities within an organisation [2]. Therefore the importance of delegation of duties and authorities should not be underestimated. The top management is in charge of secure business operations, and has an authority to set policies that govern entire organisation. This authority and responsibility is then delegated to the information security personnel that further designs security enforcement technologies, structures of responsibilities and other non-technical security enforcement functions, such as user education and statements governing rights, duties and responsibilities of users. Even though studying human issues, it should be noted that non-technical solutions are strongly dependent on underlying security enforcement technology. As most security eduction and awareness development must be tied into underlying technologies, they can be specified only after actual technical protection measures have been identified and implemented. Otherwise, there is a risk of having awareness without skills of enforcement. Highly abstract and conceptual user awareness is only of limited importance.

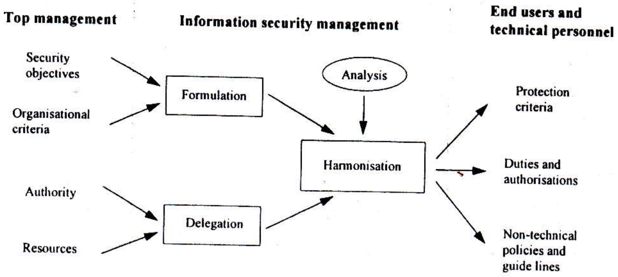

Figure 1 An architecture for the management of information security

2.2 The changing information processing environment

Throughout 1990’s, organisations have been moving from big centralised mainframe computers and specific operating systems to smaller distributed computers and universal operating systems or operating system independent program execution platforms, such as Java Virtual Machine. This trend has caused the emergence of client/server architecture and global information access protocols such as HTTP. Considerable performance gains of small computers, improved networking features, along with the rapidly developing information networks, are the basic elements of computing in the 1990's leading way to 2000’s. In a modern organisation "the big computer" is no longer a single physical device, rather, it consists of several different computers, nodes, a covered computer network and a number of input/output devices. Nodes can be geographically far removed from each other and load can be shared between nodes. It is self evident that in such a situation the end-user has more possibilities and more freedom, the network and the computer systems are more "open" to him/her. But the price they pay for this openness is increased responsibility [13, 24]. From the security point of view, the shift from centralised to distributed computing has lead to the need for confidentiality, authenticity, integrity of data and non-repudiation of transactions, usually enforced by cryptographic protocols and techniques. Authorisation is strongly directed towards role based access control models [19, 23] instead of physical security of computer centers and traditional access control models derived from the military community.

Earlier, every computer had its specific operating system, whereas now we are transferring to more open, standard operating systems, in many cases UNIX, OS/2, Win95 or Windows NT. Openness means, firstly, computer independence. Computers built by different manufacturers are interconnected, which is made possible by the fact that we have standard computer networks at our disposal. To put the networks to good use, the programs and data must be used in concert. Reaching this goal, openness, seems to bring new problems, which appear difficult to solve. The idea was that by increasing openness we would encourage the positive use of computers, and thus make human work easier. But the situation is not as simple as that. Earlier, information security problems were in control, and in many cases, when we were faced with a problem, we could find a solution. Openness has, together with public global networks being employed, in fact, made misuse of information more common during the past two decades, and the negative inventive power of people seems to be increasing, too. Several examples of misuse of computer networks, such as TCP SYN flooding [5] and TCP/IP Ping attacks [6] show that explorations of weaknesses in underlying protocol suites can cause significant harm on businesses employing new technologies. The major problem in these attacks is that they exploit weaknesses on protocol design, not flaws in individual software components such as previously common attacks to gain unauthorised access by misusing common system software, such as UNIX finger and sendmail. Due to the heterogeneity of users among global networks, commonly adopted ethical and moral norms are also most likely to fail [15]. Due to the heterogenicity of cultural backgrounds, social control as a means to prevent misuse of computers and information becomes weak. Therefore, organisations need to put more emphasis on technical protection, starting from seeing security as a major requirement in system analysis and design, but also on education on users and other human issues related to information security. Ignorant or unaware users provide a great threat for the entire security of information systems.

2.3 The human factor - the end users

When we talk about computer end-users in this paper, we are refer to people, who use either microcomputers or workstations to implement their work duties. If talking about end-user computing instead of people, we can use the definition offered by Beatson [3]: *end-user computing is the functionality associated with allowing users to manipulate information and applications at their discretion, and can maintain their information.* Information security is not in any way limited to computerised information, information in all its forms must be taken into consideration. End-user computing refers principally to the discretionary functionality given to the user, as compared with transaction based applications, where the users' actions are constrained by predetermined procedural steps.

When people work a long time under pressure, their ethical principles are put to the test. Even if acts are considered immoral, pressure and stress may reduce the barrier of committing into such acts, such as misuse of information or processing devices. With continuing education the organisation should improve the end-users' knowledge concerning the information system and its security. Descriptive awareness should lead to prescriptive awareness, commitment into secure processing of information. This is important since many computer abuse is caused by insiders. Distinguishing the degree of risks posed by insiders and outsiders is vulnerable to an oversimplifying of complex relationships between victims and perpetrators, and may lead the information security manager and his management team to allocate their limited and precious security resources inappropriately. The only valid conclusion, based on limited knowledge of loss experience, is that the majority of loss is caused by authorised persons engaged in unauthorised activity [18, 26].

The question concerning information security and people is one of the most difficult in the world of computing. There is a clear demand for increasing the number of people who work in professions related to information security. Since information security is becoming one of the key factors in successful information processing policy, the responsibilities and rights of the different groups of users, administrators and managers should be clearly defined. Education should be implemented at every level in the organisation, with the occupational role of each employee determining which facets of information security are his/her main concerns [24, 25].

3 Tasks related to human issues in information security

This section identifies major components of the human track of information security framework illustrated in figure 1, and discusses each of them in detail. First one is specification of duties and responsibilities, to be studied in section 3.1. Second issue is delegation of authorities to the members of organisation, to be studied in section 3.2. As illustrated in figure 1, there are two major outputs of human issues: different protection guide lines for end users of information systems and non-technical policies governing protection of sensitive information. Structure and content of these guide lines and statements shall be discussed in section 3.3.

3.1 Specification of duties and responsibilities

It is commonly agreed that managerial commitment is a key success factor in information security. Briefly, they have a responsibility of secure operations in the organisation and authority to set and implement organisation wide policies, guidelines and criteria. Clear specification of information security related duties and authorisations becomes then essential in the provision of secure operations. Typically, these activities can be seen as specification of high level roles different employees act in within the organisation. Once roles are adopted, they come with a set of authorisations needed to carry out those duties. Therefore, the problem can be divided into two: specification of duties and authorisations and assignment of employees into roles. A user then adopts a role, if so authorized, when executing specific tasks within the system. This is a fundamental assumption of role based access control systems and work flow analysis. Roles are seen as representations of duties carried out within the businesses and are expected to be stable. Also, each role is expected to have a specific set of authorisations required to carry out tasks of the role.

The set of roles is constant over considerably long periods of time, whereas adoption of roles by users varies within each session. This is a significant improvement in the management of information security compared to application of traditional access control models. As user-role assignment is a simple task compared to specification of roles and their authorisations, the major focus shall be on provision of trusted assignment of users into roles, and assurance that no roles can be adopted by users that violate these assignments. An additional advantage of role based approach is, that several commercial network operating systems, such as Microsoft Windows NT and Novell NetWare, support the paradigm [19].

If assigning authorisations to users, there is a risk of violating the need-to-know principle, since users may not each time need all their authorisations to carry out a specific task. Role based approach reduces the risk by assigning a user to a different role each time carrying out a different task within the information system. Reliable adoption of roles by users is a more simple administrative task than specification of roles and authorizations, and therefore it can be executed dynamically within each access request to a system. User executes identification, authentication and system level access control procedure in form of a username password pair, biometric mechanism or a cryptographic protocol. Once assurance is provided from the authenticity of a user and eligibility of entering the requested role, user is authorised to enter the role and is given specified authorisations within which the user may act.

3.2 Delegation of authorisations

Managerial personnel is in charge of fair and efficient allocation of duties within the organisation. Therefore, authorisations to carry out different tasks are delegated to employees of the organisation. To be on align with organisational procedures, it is essential to set the authorisations in a way that no sensitive information can leak to unauthorised parties. Issue can be studied as a set of delegation paths by which authorisations propagate from top management throughout the organisation. Each delegation path should only consist of employees in roles that are authorised to handle that information. These authorisations should be specified in the specification of duties and authorisations, and actual delegation of authorisation is then enforcement of the top level policy regarding these duties and authorisations.

3.3 Structure and content of policies

There are two major outputs of the process: end user guidelines and non-technical policies to be enforced by managerial control. This is the most studied area of human issues in information security. Mostly, the focus has been on the specification of application-dependent guidelines for secure operation of systems and processing of information. Also, generic guidelines are widely available for proper application of security mechanisms and services, such as selection of passwords and phrases, how to prevent viral infections, and how to deal with sensitive information when being transmitted over an insecure public network, such as the Internet. The best known generic guidelines are those provided by U.S. National Institute of Standards in Technology (NIST). These divide responsibilities of secure operations into executive, managerial and operational guidelines and provide with common objectives of duties at each level. This is an important division, since much of research focuses on the provision of security guidelines for end users but similar sets of guidelines should be made available to different organisational layers. Managerial duties must be attached with a set of guidelines, too.

When studied from a wide point of view, information security covers many areas of computerized and manual lprocessing of information. Therefore, covering of all security sensitive processes becomes a complicated task. Various non-technical covert channels must be eliminated and each document must be considered from the security point of view. Therefore, organizing these policies into meaningful collections of rules and guide-lines can be very complicated. Various quality methodologies, such as ISO 9000, has been applied to information security to include security documentation in each process. This is a promising approach due to it's integration into general business process descriptions. Due to the lack of space, the issue shall not be further studied herein.

4 Evaluation, conclusions and future work

The major contribution of this paper has been in to identification of a systematic approach into the management of human issues in information security. We have analysed a systematic management framework for information security and identified a number of areas for further research. As security enforcement technologies advance, two major issues become essential. Control of those technologies to provide secure and cost-efficient systems from secure building blocks and expansion of organisational policies to govern also human issues of information security. This is an essential area of research in security, and should not be ignored. End users need to be aware of inherent security risks of information and be skilled to operate systems in a secure manner. Much of existing research has focused on the provision of either generic or implementation specific guidelines and rules of operation, but has contributed only little to the establishment of a systematic approach towards human issues.

The focus of this paper has rather been on the provision of an overview of a broad area of research than in the detailed analysis of specific issues involved. Therefore, the detailed application of different logics for coding information security statements is left for future work. Deontic logic provides a promising framework for future work in the coding of non-technical information security requirements. Deontic logic, basically, is the study of obligation and permission. Therefore, this is a logical approach, since we are mostly concerned with obligations and permissions regarding use of systems and services. Also, similar approaches have been previously used for coding access control requirements and cryptographic requirements. Early work of Minsky and Lockman [17] highlighted the need for deontic operators when specifying authorisations in databases and operating systems. Later, deontic and epistemic logics have been applied in the specification of security policies for access control and cryptographic protocols [4, 7, 22]. Also, Jones and Sergot

[10] have proposed a mechanism to apply formal theory of normative positions in the specification of access control requirements. The major difference in coding authorisation rules and rules for human actions is, that in the latter case, requirements must remain as descriptive statements, full semantics can not be specified. Also, enforcement must be through leadership, not through security enforcement software or hardware. This research is, anyhow, left for future work.

This work is concluded by looking at the big picture provided by the proposed approach. Several components have been identified regarding human issues in information security. More detailed research is required at each of these areas to identify processes and their dependencies to provide with concrete and practical tools for the management of information security from a holistic and systematic point of view.

References

[1] Angerfelt, B. Computer Crimes. A Study of Different Types of Offences and Offenders. Proc IFIP TC11 8th International Conference of Information Systems Security. Singapore, May, 1992.

[2] Backhouse, J. and Dhillon G. Structures of Responsibility and Security of Information Systems. *European Journal of Information Systems*, 5(1):2-9, 1996.

[3] Beatson, J. G. Information Security: The Impact of End User Computing. *Proc. IFIP TC11 8th International Conference of Information Systems Security*. Singapore, May, 1992.

[4] Bieber, P. and Cuppens, F. Computer Security Policies and Deontic Logic. *Proc. 1st International Workshop on Denotic Logic in Computer Science*. Amsterdam, the Netherlands, 1996.

[5] CERT Advisory CA-96.21. *TCP SYN Flooding and IP Spoofing Attacks*. Sep. 1996. ftp://info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding.

[6] CERT Advisory CA-96-26. Denial of service attack via ping. Dec. 1996. ftp://info.cert.org/pub/cert_advisories/CA-96.26.ping.

[7] Glasgow, J., MacEwen, G. and Panangaden, P. A Logic for Reasoning About Security. *ACM Transactions on Computer Systems*. 10(3): 226-264, 1992.

[8] Hale, R. End-User Computing Security Guidelines. *Information Systems Security*, 4(4): 49-64, 1996.

[9] Hartman, A. Comprehensive Information Technology Security: A New Approach to Respond Ethical and Social Issues Surrounding Information Security in the 21st Century. *Proc. IFIP TC11 11th International Conference of Information Security*. Cape Town, South Africa, May, 1995.

[10] Jones, A. I. J. and Sergot, M.. Formal Specification of Security Requirements using the Theory of Normative Positions. In *Computer Security - ESORICS'92*. Springer-Verlag LNCS 648, 1992.

[11] Kajava J. and Leiwo J. Information Security for Workstations: Implications for End-Users. *Proc. WG11.1 Workshop on Information Security Management*. Cape Town, South Africa, May, 1995.

[12] Kowalski, S. Computer Ethics and Computer Abuse: A Longitudinal Study of Swedish University Students. *Proc. IFIP TC11 6th International Conference on Information Systems Security*. Espoo, Finland, May, 1990.

[13] Lawrence, L. G. Security in a Client Server Environment. *Network Security*, July 1994. Elsevier Science LTD, 1994.

[14] Leiwo, J. and Heikkuri S. Clarifying Concepts of Information Security. *Proc. 2nd Baltic Confecence on DB and IS.* Tallin, Estonia, June, 1996.

[15] Leiwo J. and Heikkuri S. An Analysis of Ethics as a Foundation of Information Security in Distributed Systems. *Proc. 31st Hawaiian International Conferenсe on Systems Sciences*. Hawaii, USA, Jan. 1998.

[16] Leiwo J. and Zheng, Y. A Framework for the Management of Information Security. *Proc. 1997 Information Security Workshop.* Ishikawa, Japan, Sep. 1997.

[17] Minsky, N. H. and Lockman, A. Ensuring Integrity by Adding Obligations to Privileges. *Proc. 8th International Conference on Software Engineering.* Aug. 1985.

[18] Parker, D. B. Seventeen Information Security Myths Debunked. *Proc. 6th International Conference on Information Systems Security*. Espoo, Finland, May, 1990.

[19] Sandhu, R. S., Coyne, E.J., Feinstein, H.L. and Youman, C.E. Role-Based Access Control Models. *IEEE Computer*. pp. 38-47, Feb. 1996.

[20] Siponen, M.T. and Kajava, J. The Various Dimensions of IT Security Awareness. *Proc. 3rd International Baltic Workshop on DB and IS*, Riga, Latvia, Apr. 1998.

[21] Straub, D. W., Carlson, P. J. and Jones, E. H. Deterring Highly Motivated Computer Abusers: A Field Experiment in Computer Security. *Proc. IFIP TC11 8th International Conference of Information Systems Security*. Singapore, May, 1992.

[22] Syversen, P. Formal Semantics for Logics of Cryptographic Protocols. *Proc. Computer Security Foundations Workshop,* 1990.

[23] Tari, Z. and Chan, S-W. A Role-Based Access Control for Intranet Security. *IEEE Internet Computing*, 1(5): 24-34, Nov.-Oct. 1997.

[24] Wolfe, A. D. Jr. Securing the Distributed Environment: A Question of Trust. *Network Monitor*. 7(1), 1992.

[25] Wood, Charles C. *How Many Information Security Staff People Should You Have* ? Information Integrity Investments, Sausalito, CA, USA, 1989.

[26] Young, L. F. Utopians, Cyberpunks, Players and Other Computer Criminals: Deterrence and Law. *Proc. of the IFIP WG9.6 Working Conference on Society and Control of Information Technology in Society*. St. Petersburg, Russia, Aug. 1993.