Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2006 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2006

Managerial Information Security Awareness' Impact on an Organization's Information Security Performance

Namjoo Choi
Michigan State University

Dan Kim
Michigan State University

Jahyun Goo
Florida Atlantic University

Managerial Information Security Awareness' Impact on an Organization's Information Security Performance

Namjoo Choi
Michigan State University
choinamj@msu.edu

Dan J. Kim
Michigan State University
dankim@msu.edu

Jayhun Goo
Florida Atlantic University
jgoo@fau.edu

ABSTRACT

The primary goal of this study is to examine the relationship between managerial information security awareness and managerial actions toward information security for the purpose of putting stress on the significant roles of managerial information security awareness in an organization's total information security performance. Under the assumption that managerial actions toward information security has a positive impact on changes in the content of strategies and organizational outcomes in turn, the research supports the following: higher managerial information security awareness leads to more managerial actions toward information security and ultimately more efficient organization performance regarding information security.

Keywords

Information security awareness (ISA), Managerial information security awareness (MISA), Managerial actions toward information security (MATIS)

INTRODUCTION

The term "information security awareness (ISA)" is mostly defined in the literature as a state in which employees in an organization are aware of information security objectives (Thomson and von Solms, 1997; 1998, Hawkins et al., 2000; Siponen, 2000; 2001, Furnell et al., 2002). Researchers interested in information security have recognized ISA as a significant factor in an organization's total information security performance. However, there are not many scientific studies that consider ISA in any depth (Siponen, 2001), and those few studies about ISA have focused mostly on employees' ISA: how to raise their ISA through more effective and efficient educational programs.

Surprisingly, although it is obvious that managerial information security awareness (MISA) has a powerful impact on an organization's total ISA and its implementation, the research from the managerial perspective is almost nonexistent or still in the infancy stage. In order to implement appropriate information security strategies, to effectively raise employees' ISA, and ultimately to produce better information security performance, the concerns about MISA should be addressed first.

The primary goal of this study is to examine the relationship between MISA and Managerial actions toward information security (MATIS) for the purpose of putting stress on the significant roles of MISA in an organization's total information security performance. Under the assumption that more MATIS have a positive impact on changes in the content of strategies and organizational outcomes in turn (Figure 1), by utilizing the data which were collected by the Korean Information Management Institute for Small and Medium Enterprises in 2003, this research explores the following research question: whether higher MISA leads to more MATIS, which were manipulated with executed MATIS by each organization.

RELEVANT LITERATURE

Loch et al (1992) predicted that the growth of connectivity and dispersion of technology within or between organizations would continuously increase information systems security risk. To reduce the risk, they suggest that information system management teams need to become more informed of the potential for security breaches and increase their ISA. A comparative qualitative case study conducted by Straub and Welke (1998) supports their two propositions: 1) managers are aware of only a fraction of the full spectrum of actions that could be taken to reduce systems risk; 2) managers exposed to theory-grounded security planning techniques are inclined to employ these in their planning processes. Some recent research has begun to take into account the managerial elements of information security. For example, by conducting interviews with information security executives who hold the title of either Vice President or President and who are directly responsible for the information security strategies of their firm, a recent study revealed that interviewees consider executive management cognition of information security as a major issue (Cline and Jensen, 2004). In other words, they all put stress on the importance of a decision maker's information security awareness for successful information security implementation and performance. Other recent research reports by the Henley Management College (2003; 2004) also suggested that for an effective information security strategy, even board members should be aware of information security objectives and should see information security as not a financial cost but as an opportunity. Regarding budgetary concerns, security practitioners often stress that senior management involvement in information security is very critical. For instance, investments in information security require budgetary approvals, which require senior management awareness in the information security problems.

Straub (1990) showed that increased security actions in general result in significantly less damage from computer abuse, which supports the assumption in the current study that more MATIS have a positive impact on organizational information security performance.

CONCEPTUAL DEVELOPMENT AND RESEARCH MODEL

The research employs a conceptual model (Rajagopalan and Spreitzer, 1997) that synthesizes recent organizational change literature and adapts it into a new model (see Figure 1) to focus on the relationship between MISA and MATIS. The idea came from a recent study (Cline and Jensen, 2004) that adopted this conceptual model. By conducting a qualitative content analysis and interviews, Cline and Jensen (2004) collected all the possible information security issues in an organization, separated them into relevant constructs (environmental conditions and changes, organizational conditions and changes, managerial cognition, managerial actions toward information security, changes in the content of strategy, and organizational outcomes) in the conceptual model to examine changing information security requirements and the strategies that organizations are developing to meet the related challenges. Finally, they investigated how an organization can develop the strategies in response to new information security requirements.

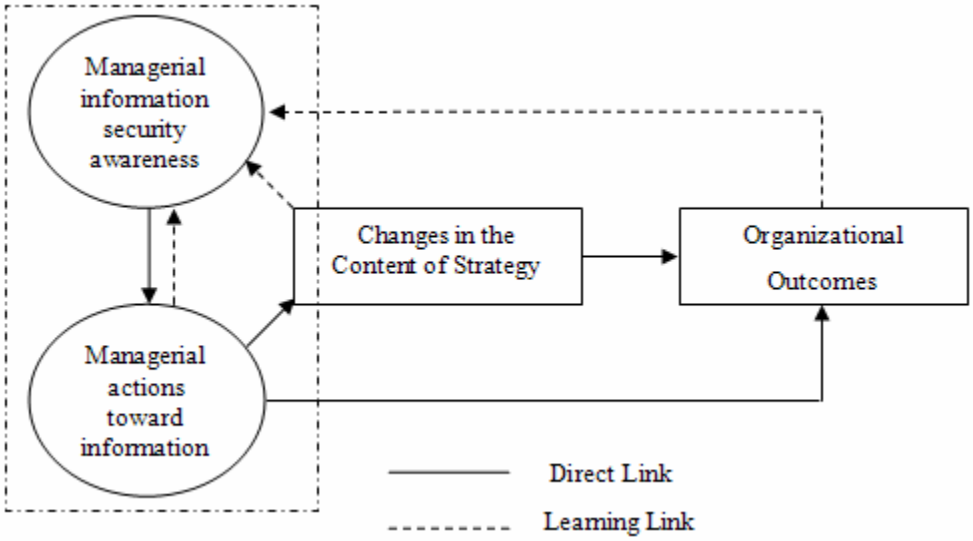

Figure 1. Conceptual Research Model[1]

[1] The model was adapted from Cline and Jensen, 2004

Under the assumption that more MATIS have a positive impact on changes in the content of strategies and organizational outcomes in turn, the current research mainly focuses on examining the relationship between MISA and MATIS.

While ISA is mostly defined as a state where employees in an organization are aware of information security objectives, MISA in the current study particularly focuses on how managerial or higher levels regard the significance of information security. Since awareness is defined as recognition or understanding and significance is defined as the importance or worth, it is controvertible to mix up those two relevant concepts. For instance, managerial or higher levels can be aware of security and not view it as significant (maybe not significant to their own job or maybe not significant in relationship to other issues). They may also believe security is significant, but may not be aware of how to go about attaining it.

The current study, however, assumes that if those decision makers regard information security as significant, they will take into account information security issues more seriously, and ultimately they will be aware of them and take more MATIS. Therefore, under this assumption, the term "MISA" in the current study starts from being aware of the significance of information security.

MATIS would embrace all the possible activities regarding information security: setting, maintaining, and implementing security policies, procedures, and standards, increased hiring of certified security professionals, increased training, installations of security hardware and software, acquisition of security services, and so on.

Although there are hosts of other actions involved in information security, the current study confines these actions to information security priorities perceived by the managerial level based on a survey conducted by InformationWeek (2003). According to the survey report, information security priorities perceived by the managerial level are "raise user awareness of policy and procedures, train/retrain staff, security review and assessment, security policies and standards, data ownership and classification standards, qualified staff, and incident response teams."

Consequently, the current study utilizes these priorities to manipulate variables for MATIS from the original questionnaire (KIMI, 2003). Finally, they were manipulated into the following five variables: 1) information security policies and procedures, 2) information security training and education, 3) information access control, 4) information security systems and programs updates, and 5) information security teams.

Since the variables are drawn from the MISA perspective and are found as the most common practices in the field, and the purpose of the study solely focuses on the relationship between MISA and MATIS to stress on the significant roles of MISA in an organization's total information security performance, it is considered that excluding other factors related to information security barely biases the purpose of the study.

Changes in the content of strategy are defined as a relatively long term of changes in information strategy as a consequence of MATIS. Organizational outcomes are defined as realized organizational information security performance through MISA, MATIS, and changes in the content of strategy in turn. Finally, the learning links describe continuous managerial learning as a reshaping of MISA.

Based on the above conceptual backgrounds and the assumption that MATIS have a positive impact on changes in the content of strategies and organizational outcomes in turn (Figure 1), the research formally hypothesizes:

Proposition: higher managerial information security awareness leads to more managerial actions toward information security.

Information Security Policies and Procedures

The development of information security policies and procedures is generally considered as the beginning of an effective information security program. If there is no process in place to make sure that the employees are made aware of their responsibilities regarding information security issues, the implementation of a strong information security system will be less effective (Peltier, 2005).

Management establishes its goals and objectives for protecting the assets by implementing policies. Policies are used to introduce the concepts of what is expected of all employees when using enterprise assets. In other words, information security policies establish the behavior expected of all personnel granted access to the information system.

Information security procedures provide users with the information needed to complete a task and ensure management that the tasks are being completed in a uniform and approved manner. Procedures improve efficiencies in employee workflow and assist in the prevention of misuse and fraud.

H1: higher managerial information security awareness leads an organization to establish information security policies and procedures.

Information Security Training and Education

Information security policies and procedures can only be effective if employees understand the necessary safety measures and always keep those in mind when executing whatever tasks are given to them. In other words, the establishment of perfect policies and procedures does not directly guarantee the successful implant of them among employees unless employees are made aware of those policies and procedures (Fowler, 1996).

In addition, the process that educates these skills required for using information security tools could be also included in these training and education activities. After providing at least proper training and education on how to use the organization's information system, an organization can proceed to focus on educating its information security policies and procedures.

As mentioned in the first section of the study, there are not many studies about ISA, and those few studies about ISA have focused mostly on employees' ISA with topics such as how to raise their ISA through more effective and efficient education programs. In this context, it is meaningful that the *H2* examines whether higher managerial information security awareness leads an organization to execute information security training and education programs because it is obvious that without approval or support from the managerial level, it is impossible to execute those training and education programs for employees.

H2: higher managerial information security awareness leads an organization to execute information security training and education programs.

Information Access Control

Since information access control is popularly known and the most heavily used information security technique from the managerial perspective, it can be assumed that it represents other similar variables excluded in the current study.

Information access control allows the user to access only authorized data so that different users can be restricted to different modes of access and also assures that communication is authentic (Farahmand et al, 2005). It can vary from virus protection systems to ESM (Enterprise Security Management). Also, it can provide policy-based control of who can access specific systems, what they can do within them, and when they are allowed access. Policies can be created, managed, and distributed on an enterprise-wide basis, or they can be customized to meet the security requirements of specific applications.

H3: higher managerial information security awareness leads an organization to implement information access control.

Information Security Systems and Programs Updates

Updating of information security systems and programs includes all applications and operating systems. It is obvious that without proper updates, well-developed information security systems and programs can become useless at any time. This makes it important to keep all systems and programs updated to prevent security incidents.

As it can be assumed, to maintain properly updated information security systems and programs, it is also very critical that managerial levels set up the proper policies and procedures with higher MISA. Beyond that, the constant supervision by managerial levels needs to be practiced.

H4: higher managerial information security awareness leads an organization to update information security systems and programs more frequently.

Information Security Teams

Many experiences show that prevention is by far less expensive than mitigation after a loss has taken place. In that, to provide accelerated problem detection, damage control and problem correction services, the establishment of information security specialized teams is considered essential to most organizations. However, management, especially in small and medium sized organizations, has yet to allocate sufficient resources necessary to establish an information security teams. This may be due to budgetary limitations or simply ignorance of its significance.

However, if it is caused by neglecting its significance and not from budgetary limitations or other factors, it should be questioned not only for the present but also for the future loss. The form of retaining information security teams can vary by an organization's circumstances. It can be outsourced to information security specialized firms, processed by related departments (mostly found in small and medium sized organizations), or solely processed by a specialized information security team.

H5: higher managerial information security awareness leads an organization to retain information security teamsTitle and Authors

DATA COLLECTION AND RESEARCH METHOD

The hypotheses were evaluated by means of a secondary data analysis. The research utilizes the data that were collected by the Korean Information Management Institute for Small and Medium Enterprises (KIMI) in 2003. Since 2001, the KIMI has been annually conducting a study called "the small and medium-sized enterprises' informationalization level evaluation" to council relevant policy makers in Korea.

Even though the study might seem to focus on small and medium-sized enterprises from its title, the population of the sample (KIMI, 2003) was all of the enterprises in Korea. By executing the random stratification sampling method considering the area, type, and size, 1,773 enterprises were selected. The data collection was requested of a specialized research firm that visited each selected enterprise and conducted the survey and interview with information system related managerial or higher level personnel. In the current study, the items selectively chosen from the original questionnaire were used to measure the hypotheses.

Measurements

Managerial information security awareness (MISA) was measured by adding the values of three related items that asked subjects: how they regard the significance of information security, how they regard their concerns about information security and willingness to support it, and how they regard their participation in information security investment strategies.

As briefly mentioned in section II, the research from the managerial perspective is still in the infancy stage. Part of the difficulty in conducting the research may be a lack of data, and it is common knowledge that organizations are reluctant to share their data. By utilizing the secondary data, and beginning by asking how they regard the significance of information security to appreciate MISA, the current study, however, offset the above limitations.

The study expects that by adding the values of related items (basically, all the items can be considered to be asking the same question: how they regard the significance of information security), it can minimize possible bias from the incomplete set of measurements not solely dedicated to test MISA.

Information security policies and procedures were measured by employing an item that asked subjects whether their enterprises established information security policies and procedures.

Information security training and educating was measured by employing an item that asked subjects whether their enterprises executed information security training and education programs.

Information access control was measured by employing an item that asked subjects whether their enterprises implemented access control for the network and information systems.

Information security systems and programs updates were measured by employing an item that asked subjects how often their enterprises updated information security systems and programs.

Information security teams were measured by employing an item that asked subjects whether their enterprises retained information security teams.

Finally, *managerial actions toward information security* were manipulated by adding the scores of information access control, information security systems and programs updates, information security teams, information security training and education, and information security policies and procedures.

ANALYSIS AND RESULTS

All the hypotheses were tested using simple correlations first, and then ANOVA was used for more accurate results. ANOVA tests were facilitated by dividing the scores of managerial information security awareness into three groups (group 1: low, group 2: medium, group 3: high). Table 1 shows the simple correlations among all the variables:

	(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*
Managerial information security awareness (1)	1						
Information security policies and procedures (2)	.310(**)	1					
Information security training and education (3)	.357(**)	.476(**)	1				
Information access control (4)	.371(**)	.344(**)	.306(**)	1			
Information security systems and programs updates (5)	.346(**)	.274(**)	.281(**)	.399(**)	1		
Information security teams (6)	.334(**)	.380(**)	.440(**)	.377(**)	.480(**)	1	
Managerial actions toward information security (7)	.496(**)	.713(**)	.719(**)	.722(**)	.641(**)	.698(**)	1

*** Correlation is significant at the 0.01 level (2-tailed)*

Table 1. Simple Correlations

Table 2 shows F-test, mean, and standard deviation (sd) score of each construct (information access control, information security systems and programs updates, information security teams, information security training and education, and information security policies and procedures) by the scores of managerial information security awareness (group 1: low, group 2: medium, group 3: high) in each ANOVA test.

Managerial information security awareness		*Low*		*Medium*		*High*	
	F-test	*Mean*	*Sd*	*Mean*	*Sd*	*Mean*	*Sd*
Information security policies and procedures	F (2, 1742) = 52.01, P < .001	.03	.18	.14	.35	.32	.47
Information security training and education	F (2, 1745) = 64.37, P < .001	.05	.21	.17	.37	.37	.48
Information access control	F (2, 1742) = 128.47, P < .001	.12	.33	.36	.48	.66	.47
Information security systems and programs updates	F (2, 1689) = 109.88, P < .001	.37	.39	.58	.42	.80	.35
Information security teams	F (2, 1746) = 69.29, P < .001	.05	.21	.19	.34	.36	.39
Managerial actions toward information security	F (2, 1665) = 182.62, P < .001	.61	.73	1.44	1.27	2.53	1.49

Table 2. ANOVA Results

First of all, the proposition of the study "*higher managerial information security awareness leads to more managerial actions toward information security,"* was supported according to the simple correlations above. The ANOVA test (Table 1) shows that there is also a significant difference between three different groups by the scores of MISA (F (2, 1665) = 182.62, P < .001).

H1, "*higher managerial information security awareness leads to an organization to establish information security policies and procedures,"* was supported according to the simple correlations above. The ANOVA test for H1e (Table 1) shows that there is also a significant difference between three different groups by the scores of MISA (F (2, 1742) = 52.01, P < .001).

H2, "*higher managerial information security awareness leads an organization to execute information security training and education program,*" was supported according to the simple correlations above. The ANOVA test for H1d (Table 1) shows that there is a significant difference between three different groups by the scores of MISA ($F (2, 1745) = 64.37$, $P < .001$).

H3, "*higher managerial information security awareness leads an organization to implement information access control,*" was supported according to the simple correlations above. The ANOVA test for H1a (Table 1) shows that there is also a significant difference between three different groups by the scores of MISA ($F (2, 1742) = 128.47$, $P < .001$).

H4, "*higher managerial information security awareness leads an organization to update information security systems and programs more frequently,*" was supported according to the simple correlations above. The ANOVA test for H1b (Table 1) shows that there is also a significant difference between three different groups by the scores of MISA ($F (2, 1689) = 109.88$, $P < .001$).

H5, "*higher managerial information security awareness leads an organization to retain information security teams,*" was supported according to the simple correlations above. The ANOVA test for H1c (Table 1) shows that there is also a significant difference between the three different groups by the scores of MISA ($F (2, 1746) = 69.29$, $P < .001$).

H	Variables Independent à Dependent	Simple Correlations	ANOVA F-test	Results
P	Managerial information security awareness à Managerial actions toward information security	.496(**)	F (2, 1645) = 182.50 (***)	Accepted
H1	Managerial information security awareness à Information security policies and procedures	.310(**)	F (2, 1742) = 52.01 (***)	Accepted
H2	Managerial information security awareness à Information security training and education program	.357(**)	F (2, 1745) = 64.37 (***)	Accepted
H3	Managerial information security awareness à Information access control	.371(**)	F (2, 1742) = 128.47 (***)	Accepted
H4	Managerial information security awareness à Information security systems and programs update	.346(**)	F (2, 1689) = 109.88 (***)	Accepted
H5	Managerial information security awareness à Information security teams	.334(**)	F (2, 1746) = 69.29 (***)	Accepted

* Significant at the 0.05, ** significant at the 0.01 level, *** significant at the 0.001 level, ns – not significant

Table 3. Summary of the Results

DISCUSSION AND CONCLUSIONS

As mentioned from the beginning, although it should be obvious higher MISA would lead to more MATIS, the research from the managerial perspective is almost nonexistent or still in the infancy stage. Therefore, the primary contribution of the study is that it empirically confirms the seemingly explicit fact that higher MISA would lead to more MATIS.

Under the assumption that MATIS has a positive impact on changes in the content of strategies and organizational outcomes in turn, the results show that higher MISA leads to more MATIS. As its subcategories, it is also found that MISA has a positive impact on each variable: information security policies and procedures, information security training and education, information access control, information security systems and programs updates, and information security teams. Therefore, the current study in its proposed model (Figure 1) can reach the conclusion that higher MISA can ultimately lead to better information security performance in an organization.

Another interesting finding from the study's results is that if an organization has higher MISA, it actually practices more variables examined in the study: information security policies and procedures, information security training and education, information access control, information security systems and programs updates, and information security teams. It can be

intuitively perceived that with higher MISA, an organization can be expected to perform more information security related activities (supposedly, under the circumstances in accordance with budget and purpose).

From the findings above, it is argued that the concerns about MISA should precede the concerns about employees' information security awareness. As emphasized throughout the study, an organization should set up strategies to raise its MISA and consider it as a first priority. After that, an organization can take into account the other issues related to information security. Therefore, it can be suggested that if an organization is concerned about its information security performance, then it should be necessary for managerial levels to participate in the issue more actively, and to do so their MISA must be raised. Without their perception of information security objects and its fundamental significance, in most organizations, it is hard to expect better information security performance.

From an academic perspective, information security researchers need to determine why, what and how managerial or higher level decision makers in an organization should be educated about information security while most research focuses mostly on how to raise employees' ISA through more effective and efficient education programs. Again, in order to implement appropriate information security strategies, to effectively raise employees' information security awareness and to produce better information security performance, the concerns about MISA should be addressed first.

Furthermore, the idea found in the current study could be applied to ISA's different dimensions: general public dimension, socio-political dimension, computer ethical dimension, and institutional dimension (Siponen, 2001). In other words, as MISA's important role in an organizational dimension was examined in the study, ISA researchers first look for key role subjects who have the most powerful impact on others. After that, to raise total ISA and finally produce better information security performance in a whole society, the close interactions between each dimension can be viewed.

A first limitation of the research is that it utilized the secondary data. The items from the original questionnaire were selectively collected. Therefore, measures need to be more elaborate, and more items should be added for purposes of the current research. However, since the research subjects were randomly selected from all the enterprises in Korea by a specialized research firm, and the sample size is large enough to ensure accuracy (1,773), it is assumed that the weaknesses of the secondary data in the current study were offset somehow. Secondly, the other concern is that since the data were collected in one specific country, Korea, the findings of the study should be applied to other countries with caution. Further, a comparison study with the data from other countries dealing with the same topics as the current research can help generalize the results.

REFERENCES

1. Cline, M. and Jensen, B. K. (2004) Information Security: An Organizational Change Perspective, *Proceedings of the Tenth Americas Conference on Information Systems,* August 5-8, New York, New York, USA, 4514-4520
2. Farahmand, F., Navathe, S. B., Sharp, G. P. and Enslow, P. H. (2005) A Management perspective on risk or security threats to information systems, *Information Technology and Management*, 6, 2-3, 203-225.
3. Fowler, J. (1996) Developing the security culture at the SEISMED reference centers, in Barber, B., Treacher, A. and Louwerse, K. (Eds.) *Towards Security in Medical Telematics: Legal and Technical Aspects*, IOS Press, Amsterdam, 156-161.
4. Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002) A prototype tool for information security awareness and training, *Logistics Information Management*, 15, 5/6, 352-357.
5. Hawkins, S., Yen, D. C. and Chou, D. C. (2000) Awareness and challenges of Internet security, *Information Management and Computer Security*, 8, 3, 131-143.
6. Henley Management College (2003) Information Security: Setting the boardroom agenda, from http:// www.henleymc.ac.uk/.
7. Henley Management College (2004) Information Assurance: Strategic alignment and competitive advantage, from http:// www.henleymc.ac.uk/.
8. InformationWeek (2003) What's to Come, November 10, 116.
9. Korean Information Management Institute for Small and Medium Enterprises (KIMI) (2003) The annual survey 2003: The small and medium-sized enterprises' informationalization level evaluation, from http://www.kimi.or.kr/.
10. Loch, K. D., Carr H. H. and Warkentin, M. E. (1992) Threats to Information Systems: Today' Reality, Yesterday's Understanding, *MIS Quarterly*, 17, 2, 173-186.

11. Peltier R. (2005) Implementing an information security awareness program, *EDPACS*, 33, 1, 1-18.
12. Rajagopalan, N. and Spreitzer, G. (1997) Toward a Theory of Strategic Change: A Multi-lens Perspective and Integrative Framework, *The Academy of Management Review*, 22, 1, 48-79.
13. Siponen, M. T. (2000) A Conceptual Foundation for Organizational Information Security Awareness, *Information Management and Computer Security*, 8, 1, 31-41
14. Siponen, M. T. (2001) Five Dimensions of Information Security Awareness, *Computers and Society*, 31, 2, 24-29.
15. Straub, D. W. (1990) Effective IS Security: An Empirical Study, *Information Systems Research*, 1, 3, 255-276.
16. Straub D. W. and Welke, R. J. (1998) Coping with Systems Risks: Security Planning Models for Management Decision making, *MIS Quarterly*, 22, 4, 441-469
17. Thomson, M. E. and 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.*
18 Thomson, M. E. and von Solms, R. (1998) Information security awareness: educating our users effectively, *Information Management and Computer Security*, 6, 4, 167-173.