Human, Organizational and Technological Challenges of Implementing Information Security in Organizations

R. Werlinger, K. Hawkey and K. Beznosov

University of British Columbia
e-mail:{rodrigow, hawkey, beznosov}@ece.ubc.ca

Abstract

Our qualitative research provides a comprehensive list of challenges to the practice of IT security within organizations, including the interplay between human, organizational, and technical factors. We validate and extend prior work through an integration of these challenges into a framework that organizations can use to identify their limitations with respect to IT security. Furthermore, we suggest research opportunities for the improvement of IT security technologies from a holistic point of view.

Keywords

Security challenges, Organizational security, Qualitative analysis.

1. Introduction

Recent research has recognized that technological factors are not the only key to the effectiveness of information security controls; there is also a need to understand the impact of human and organizational factors (Beznosov & Beznosova, 2007; Botta et al., 2007; Vaughn & Fox, 2001). A better understanding of how different human, organizational, and technological elements interplay could explain how different factors lead to sources of security breaches and vulnerabilities within organizations (Kraemer & Carayon, 2007).

This paper reports on the challenges that security practitioners face within their organizations. We used qualitative methods to understand factors that affect the adoption of best security practices within organizations. Our data consisted of 34 questionnaires and 27 interviews with security practitioners from different organizations (18 from academia and 9 from private organizations). Our results not only validate and extend other studies that address challenges that security practitioners face, but also provide an integrated framework that classifies these challenges. This framework can help organizations identify their limitations with respect to implementing security standards as well as determine if they are spending their security resources effectively. It also provides a way to understand how different factors interplay, for example, how the culture of the organization's people and decentralization of IT security trigger security issues that make security management more difficult. We also elaborate on several opportunities for researchers and developers to improve technology and processes that are used to support the adoption of security policies or standards within organizations. To illustrate, we found that security processes should consider that security practitioners have to effectively communicate security issues to other stakeholders who have different perceptions of risks and do not have security as a first priority within the organization.

We first present related work (section 2) on IT security challenges. We then describe our methodology (section 3), including our research questions and participant profiles. We present results (section 4) as an integrated framework of human, organizational, and technological challenges. We perform a cross-analysis of the findings and discuss the interplay between the challenges (section 5). We end this section by grounding our findings in prior research and discussing opportunities for future research before providing final conclusions (section 6).

2. Background

Our results build upon prior work that addresses a subset of the human, organizational, and technological elements that challenge the adoption of security within organizations. We define human aspects as those related to cognition at the individual level, as well as culture and interaction with other people. Organizational aspects are those related to the structure of the organization, including size and managerial decisions around IT security. Technological aspects involve technical solutions such as applications and protocols.

2.1. Human factors

From the human point of view, adoption of security practices poses several challenges for security practitioners. For example, effective interactions and communications are required to reach a mutual understanding about security risks among different stakeholders. Koskosas & Paul (2004) study how security risks are communicated in financial organizations. They conclude that risk communication “plays a significant role at the macro-goal level of security management,” and affects the setting of banking security goals. Tsohou, et al. (2006) recognize that risk management is basically a human activity and propose the use of cultural theory to classify the different perceptions of security risks that stakeholders might have. Depending on the classification, security professionals should adopt different strategies to communicate and reach common risk perceptions with other stakeholders. Garigue & Stefaniu (2003) elaborate on the importance of reporting in order to communicate security concerns within organizations. They conclude that reporting on security issues is both a science and an art, with much human judgement necessary to interpret the reports from security tools.

Human errors represent another threat for best security practices. Kraemer & Carayon (2007) identify and characterize elements related to human errors in the field of information security. They populated a conceptual framework with qualitative data from 16 interviews with network administrators and security specialists. Their analysis shows that organizational factors such as communication, security culture, and policy are frequent causes of errors in the context of information security and that communication breakdowns cause security vulnerabilities.

2.2. Organizational factors

Kankanhalli, et al. (2003) propose a model that relates organizational factors such as organization size, top management support, and type of industry with the effectiveness of information security controls within organizations. From 63 surveys, they conclude that management support is positively related to the implementation of preventive security efforts. They found that financial organizations invest more resources in controls to deter bad security practices than other organizations and that larger organizations invest more in deterrent measures than smaller ones. Similarly, Chang and Ho (2006) study the factors that influenced the adoption of the IT security standard BS7799 in various organizations in Taiwan. From 59 surveys, they also conclude that factors such as top management support, size, and organization type are related to the implementation of security controls. Additionally, they find that the uncertainty of environmental elements, including high-speed change of technology, competitors' behaviors, customers' security requirements, and changes in legislation affect security management.

Knapp, et al. (2006) surveyed 936 security professionals about the importance of top management support in predicting policy enforcement and security culture within organizations. They conclude that this factor is critical for implementing security controls within organizations. Similarly, Straub & Welke (1998) study the impact of management training on the implementation of security plans in two tech services organizations. They conclude that managers are not aware of the full spectrum of actions that can be taken to reduce risks, but they will employ security planning techniques if they receive training about these techniques.

2.3. Technological factors

Technological complexity is another challenge for security practitioners. Audestad (2005) suggests that one of the reasons for not reaching 100% security is because of the complexity of technology. This complexity makes it extremely difficult for the decision makers to manage the big picture and design security policies that cover all the possible configurations of the systems. Welch (2003) studies the complexity of wireless networks and the challenges they pose to security practitioners. Jiwnani 2002 describes security testing of systems as a lengthy, complex, and costly process. He proposes a taxonomy to classify vulnerabilities and assist security practitioners in the prioritization of resources to patch them.

3. Methodology

A better understanding of real world conditions and constraints during the adoption of security practices would help developers and designers make secure systems more usable (Flechais & Sasse, 2007). None of the studies described in the related work provide a comprehensive, integrated overview of the challenges faced by security practitioners. The goal of our study is to help fill that gap. Our analysis of security challenges is part of an ongoing project whose long term goal is to construct a set of guidelines for evaluating and developing tools used for managing IT security (Hawkey et al. (to appear)). For the analysis reported here, our primary research questions were: (1) What are the main challenges that security practitioners face in their organizations? (2) How do these challenges interplay? and (3) What are the implications of the challenges on future research?

To answer these questions, we collected empirical data from interviews with security practitioners working in real environments. The strategies we used to address the difficulties of collecting data on how organizations manage IT security are described elsewhere (Botta et al., 2007). For this study, we obtained 34 completed questionnaires that led to 27 interviews with IT professionals with security responsibilities. The questionnaire provided demographic information, while the semi-structured interviews covered various aspects of IT security. Participants answered questions about their tasks, the tools they use, and the challenges of implementing security controls. To reduce interviewer bias, two researchers conducted each interview. This approach ensured coverage of interview questions and allowed the interviewers to probe for details from different perspectives. It is important to note that, due to the nature of semi-structured interviews, not all topics were discussed at the same level of detail with all participants; 23 of our participants explicitly discussed challenges (see Table 1 for their profiles).

Type of organization	Interviews	Job description
Financial services 1	I4	IT security specialist
Financial services 2	I25	IT security specialist
Insurance services	I5	IT security specialist
Security consulting services 1	I23	IT security specialist
Security consulting services 1	I27	IT security specialist
Non-profit medical services	I19	IT systems specialist
Manufacturing	I16	IT Manager
	I21	IT security specialist
Research institution	I12	IT systems specialist
Academic 1	I1	IT Manager
	I3	IT security specialist
	I14	IT systems specialists
Academic 2	I2, I15, I17, I18	IT Managers
	I9, I11, I24	IT security specialists
	I7, I10, I20	IT systems specialists
Academic 3	I22	IT systems specialist

Table 1: Profile of our participants and their organizations

The interviews were analyzed using qualitative description (Sandelowski, 2000) with constant comparison and inductive analysis of the data. We first identified instances in the interviews when participants described the challenges they faced when implementing security controls within their organizations. These situations were coded iteratively, starting with open coding and continuing with axial and theoretical coding. Results were then organized by the types of challenges (e.g., lack of resources to implement security controls). Posterior analysis was based on further elaboration of “memos” (Charmaz, 2006) written during the coding process. Following a selective coding approach, interview questions were adjusted three times (before interviews 15, 22, and 27), in order to validate emerging theories. For the overall project, four researchers performed the analysis, each focusing their analysis on different themes. The challenges theme had a considerable degree of overlap with other themes (e.g., sources of errors for security practitioners); this made triangulation of analysis possible at the researcher level.

4. Building an Integrated Framework of Challenges

Our participants described a variety of factors that made it difficult for them to implement security controls in their organizations and face the perceived security risks. Table 2 provides a summary of the challenges. We next describe in more detail the human, organizational, and technological challenges identified by our participants.

Type	**Challenge**	**Participants**	
		Academia	**Private**
Human	Lack of training or experience	I14, I18	I19, I27
	Culture within the organization	I22	I5, I16, I19
	Communicate security issues	I7, I9, I12	I25
Organizational	Risk estimation	I20	I4, I25
	Open environments and academic freedom	I1, I3, I11, I15, I20 I15, I20	NA
	Lack of budget	I2, I3, I18	I16
	Security as secondary priority	I24	I18, I23, I25, I27
	Tight schedules	I7	I25
	Business relationships with other organizations	I17	I4, I5, I25
	Distribution of IT responsibilities	I2, I11, I17	I16, I21
	Access control to sensitive data	I9, I17, I20	I4, I5, I25
Technological	Complexity of systems	I11	I23
	Vulnerabilities (systems/applications)	I11, I20, I22	I25
	Mobility and distributed access	I14	None

Table 2: Challenges participants described for implementing security controls

4.1. Human factors

We classified three challenges as human factors: (1) culture; (2) lack of security training; and (3) communication of security issues. These were particularly challenging for participants who had to actively interact with other people across the organization to implement security controls. Lack of a security culture within organizations made it difficult to change practices, such as several employees using the same account to access one system (I16). In other cases, employees considered their privileges to access data as a status symbol and resisted the loss of privileges as a result of organizational changes (I5). Lack of security training was another issue. It is difficult to implement security controls when people do not have enough orientation or education about best IT security practices (I19). Both lack of security culture and training influenced the perception of risks that stakeholders have within the organization. When there was not a common view of risks between stakeholders, communication of security issues was particularly difficult. For example, two participants (I5 and I14) describe how they tried to avoid communication breakdowns with other stakeholders (e.g., business people) who did not share the same perception of security risks. In these circumstances, the participants assumed the role of "risk evaluators" to explain the risks associated with different business decisions.

4.2. Organizational factors

Our participants discussed several challenges linked to the characteristics of their organizations. These included: (1) risk estimation; (2) open environments and academic freedom; (3) lack of budget; (4) security as a secondary priority; (5) tight schedules; (6) business relationships with other organizations; (7) distribution of IT responsibilities; and (8) access control to sensitive data.

Risk estimation, the consequences if the risks were not mitigated, and the success of mitigation controls, were all elements our participants found difficult to assess (I20, I25). Stakeholders need security training and experience before they can estimate risks (I14), which made it necessary for security practitioners to try to effectively communicate potential losses for the organization (I25).

An open academic environment proved challenging for some participants (I1, I3, I9, I11, I15, I20) who had to adapt their solutions to expectations of academic freedom by faculty members and students: "...that's an interesting trade off all the time. You're constantly trading access versus risk"(I1). This made it difficult to enforce security and implement technical solutions to mitigate risks that could compromise security. For example, one participant (I3) mentioned how difficult it was to monitor and control attacks that could be initiated using the organization's IT systems.

Budget restrictions for security programs was also a challenge discussed by participants. The implementation of security technologies can be costly (I19). It is also difficult to obtain resources for security controls when people do not understand the importance of security (I18).

Security may be a relatively low priority for some businesses: "I come from an outsourcing background where security had very tight processes...What I've learned through this company is we can't always go there...This is not an IT company, it's a manufacturing company" (I16). Participants from the private sector discussed the trade-off between security and the business processes. This trade-off was reflected in specific situations where our participants had to either relax security policies or justify the application of security controls. One participant described how the application of security patches that decreased the performance of certain applications triggered a conflict between IT security people and internal users (I5). A lack of priority for security may also make organizations overlook the need for enforcing security controls when they hire services externally. If security is not part of the big picture, external workers might not be made aware or trained about the security controls in the organization (I17).

Tight schedules as a result of business priorities are a related challenge and may result in human errors that might make the organization more vulnerable (I7). Tight schedules may also result in security controls not being implemented in the systems unless the implementation of security controls is integrated with the development process (I25).

Business relationships with other organizations posed a challenge when the organizations involved did not have similar standards in their security levels. This may also occur when organizations merge or acquire other organizations, resulting in internal silos with different needs and practices in terms of IT security. This problem can be more difficult to solve when IT security is not a main priority of the business (I16). For example, one participant (I4) explained how they had to sacrifice the application of security policies when her organization started to interact with other organizations with different security requirements.

Distribution of IT responsibilities across organizational units was an issue for our participants, particularly for those from academic settings. In the academic organizations we studied, various administrative departments shared the IT networks and systems; within each academic department, at least one employee was responsible for the local IT infrastructure. Some participants believed this distribution diminished the capability of the organization to apply IT security controls: "the decentralized nature does not help." (I2). This challenge of decentralization is similar to interactions with other organizations, as in both cases the decisions on IT security involves distributed entities.

Controlling access to data was an important challenge for our participants (I4, I5, I9, I17, I20, I25). They were concerned about sensitive data distributed in different areas of the organization; this data needed to be accessed by stakeholders from different networks and systems. The problem arose as they did not have a system to control access to data in a centralized fashion.

4.3. Technological factors

Our participants were also concerned with technological factors as they tried to implement security policies. The factors we found in our analysis were: (1) complexity of systems; (2) mobile and distributed access; and (3) vulnerabilities in systems and applications. We focus our findings on the first two factors, as they were more related with other organizational factors.

The complexity of academic systems and the need for having open and secure networks had an influence on the interactions with security vendors and providers. One participant (I15) mentioned how difficult it was for vendors to understand the architecture of the network and offer products that suit his organization's needs. Onother participant (I23) also mentioned the complexity of the networks and systems as a challenge to implement security controls in organizations. For example, a typical network could have firewalls, DMZs, proxies, switches behind the firewall, routers in front of the firewalls, mail servers and not enough people to look after the overall security of these interconnected devices. Other organizational factors such as decentralization of IT management, interaction with other organizations, and distributed sensitive data increased the complexity of technical solutions. These technical solutions needed to restrict access from different users with different needs and security requirements.

Mobility and distribution of user access made it difficult to control access to internal resources. Mobility of laptops that can be taken to different places and accessed by people who do not have enough technical expertise was a big problem for one participant (I14). He mentioned how Mondays were particularly bad days as users often came back to work with their laptops infected with malicious software from home usage.

5. Discussion

We discuss our results from three different perspectives. First, we perform a cross analysis of the challenges described by participants, considering their organizations and positions. Second, we describe how different challenges interplay. Third, we ground our results in prior research and discuss research opportunities to improve security tools and processes. Where possible, we propose characteristics that these tools and processes should have to support security practitioners in real contexts.

5.1. Cross analysis

Our analysis showed no contradictions between the challenges described by managers and other participants; managers discussed factors that either confirmed or complemented the challenges mentioned by other security practitioners. Patterns did emerge from the cross-analysis of participants from different sectors. First, academic institutions face challenges related to academic freedom and the need for an open environment. Second, challenges related to the distribution of IT management were similar for academic and private organizations; in academic organizations there were several independent departments with their own IT infrastructure, whereas in private organizations there was a need for interacting with IT departments from other organizations or from different branches within the same organization. We also found that the need for controlling access to sensitive data was a common concern.

These findings validate and extend prior research as our sample of participants contrasts in quantity and type with those ones used in similar studies (e.g., Koskosas & Paul (2004) performed 15 interviews in three organizations; Kraemer & Carayon (2007) performed 16 interviews in two academic laboratories). However, more data are necessary in order to empirically test these emerging theories. Continued research in this area is important as these factors might be used to predict how effectively security policies are adopted within a given organization.

5.2. A holistic view of challenges and their interrelationships

Kankanhalli et al. (2003), Knapp et al. (2006) and Chang et al. (2006) relate organizational variables such as size, type of business, environmental elements (e.g., customers security requirements), and top management support with security effectiveness, security culture, and enforcement of security policies within organizations. Our framework identifies other organizational variables that make it more complex to perform IT security within organizations. Furthermore, we found human, organizational and technological factors that interplay with each other and directly impact the work of security practitioners (Figure 1 illustrates this interplay). For example, communication of security issues is affected negatively by both human (perception of risks) and organizational factors (risk estimation, business relationships with other organizations, and distribution of IT management). Lack of security training negatively impacted the risk estimation and the priority given to security. Organizational factors such as an open academic environment, distribution of IT management, interaction with other organizations, and controlled access to data distributed in different departments increased technical complexity.

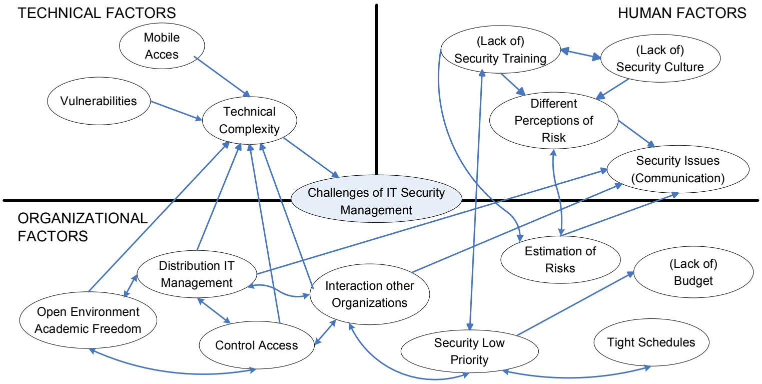
TECHNICAL FACTORS
HUMAN FACTORS
ORGANIZATIONAL FACTORS
Mobile Acces
Vulnerabilities
Technical Complexity
Challenges of IT Security Management
(Lack of) Security Training
(Lack of) Security Culture
Different Perceptions of Risk
Security Issues (Communication)
Estimation of Risks
(Lack of) Budget
Distribution IT Management
Interaction other Organizations
Open Environment Academic Freedom
Control Access
Security Low Priority
Tight Schedules

Figure 1: A holistic view of challenges and their interrelationships. Two-edged arrows indicate association between factors. Single-edged arrows indicate that one factor affects the other factor.

5.3. Opportunities for future research

The challenges we described not only illustrate the complexity of the environment where security practitioners work, but also show the limitations that organizations face when implementing security policies. These challenges also represent opportunities for future research. For example, our analysis showed that effective communication was a challenge for our participants, who needed to explain to other stakeholders security risks and the need for security controls. Pattinson & Anderson (2007) highlight the importance of risk perceptions for end-users and how important it is to communicate these risks to them. Koskosas & Paul (2004) study how risks are communicated in financial organizations. They concluded that risk communication "plays a significant role at the macro-goal level of security management." Our study extends this result by showing that the implementation of security processes should consider the organizational culture and the view that different stakeholders (not only end-users) have about security risks. A good starting point for addressing communication issues may be to apply Tsohou et al. (2006)'s proposal of using culture theory to communicate security risks, but focusing only on a subgroup of stakeholders (e.g., managers).

We found that distribution of IT management and the lack of security training of other stakeholders are also factors that negatively impact the effectiveness of communications performed by security practitioners. To address these challenges, security tools might consider the use of flexible reporting (Botta et al., 2007) to communicate security issues (i.e., reports customizable depending on the knowledge or level of the recipient). Our analysis, that included 13 more interviews than the one performed by Botta et al. (2007), also showed that a better integration between security and communication tools is necessary (e.g., integration of firewall administration tools with e-mail or chat).

Tight schedules for delivering services that include security requirements was another challenge for some participants. Kraemer & Carayon (2007) relate the lack of time, resources, and inconsistent communication among the staff with errors that are introduced into the systems. This implies a direct relationship between tight schedules and the security level of the organization. We propose that security processes and technologies should provide more support on how security practitioners should prioritize their tasks. For example, in the context of security incident reporting, Sveen, et al. (2007) propose that organizations should save resources and time by reporting only high priority security incidents. Another potential avenue for improvement is the development of tools that not only show security vulnerabilities, but also give better support to determine how security practitioners should prioritize their tasks considering the level of security risks of the different systems.

Distribution in the context of controlled access to data had two facets: first, to control access from users that are distributed and use different access technologies; and second, to control access to data distributed across the organization and managed by different stakeholders. It seems difficult for those organizations that are highly distributed in nature (e.g., academic ones) to implement centralized, strong security controls able to restrict every access and action. We propose that security processes and technologies must be developed assuming distributed environments. They should be flexible enough to both provide controlled access to highly distributed data and improve communication channels among the different stakeholders that access those data.

Training and education may improve security awareness in organizations (Sveen et al., 2007; Kankanhalli et al., 2003). We argue that the process of designing security policies can be used to train and educate other stakeholders within organizations. When designing security policies, security practitioners have to share their experiences about security incidents, vulnerabilities and culture with other stakeholders. For example, Gonzalez, et al. (2005) developed mental models that integrated the fragmented knowledge from different experts. These models identified risks in the transition to integrated operations in the Norwegian oil and gas industry. In the same vein, security policies should not be seen only as artefacts to enforce best IT practices (Thomson & von Solms, 2005), but also as a way to share the tacit knowledge that security practitioners have by explaining the "why" of the controls to other stakeholders. At this point, techniques such as the use of scenarios and anecdotes (Flechais & Sasse, 2007) look appropriate to spread the tacit knowledge used to build the policies.

We found that, within organizational factors, security as a low priority and lack of resources to implement security controls are related to what Kankanhalli et al. (2003) and Chang and Ho (2006) call organization security effectiveness. They find that the greater the top management support, the more effective security is in organizations, as organizations spend more resources in preventive measures to avoid security incidents. Kankanhalli et al. (2003) propose that penetration testing, security vulnerability, and risk analysis reports can be used to convince top management about the importance of security. They also propose making explicit the tangible business benefits of implementing security controls (e.g., raising customer confidence). However, this is not always possible when the organization does not have security experts with the knowledge to convince other stakeholders. Karyda, et al. (2006) propose outsourcing IT security services as a solution for those organizations that do not have resources or the required knowledge to implement security controls or develop security projects. However, outsourcing security seems infeasible when organizations do not perceive security as a priority from the beginning. We argue that more research is needed to both determine the rationale behind the decisions that organizations make in the context of IT security, and the trade-offs between the priority given to resources devoted to IT security and the core business of the organization.

6. Conclusion

We used empirical data and prior work to provide an integrated framework of the different human, organizational, and technological challenges that security experts have to face within their organizations. As far as we know, this is the first empirical study that provides a comprehensive list of these challenges in the context of information security. This framework is intended to provide guidance for those organizations and security practitioners that need to identify their limitations to implementing security policies, and determine what is relevant in their decisions in the context of IT security. We discussed how the different challenges interplay and suggested various research opportunities to improve security processes and technologies, considering human and organizational factors in the development of security processes and technologies.

More research is needed to understand how security challenges interplay, as this interaction affects the improvements that organizations can make in terms of their security levels. In this vein, we are currently developing a survey to administer to security practitioners, in order to refine and generalize the results we presented in this paper.

References

Audestad, J. (2005). 'Four reasons why 100 % security cannot be achieved'. Telektronikk 1.2005.

Beznosov, K. and Beznosova, O. (2007). 'On the Imbalance of the Security Problem Space and its Expected Consequences'. Information Management & Computer Security 15(5):420–431(12).

Botta, D., et al. (2007). 'Towards Understanding IT Security Professionals and Their Tools'. In SOUPS Proceedings, pp. 100–111, Pittsburgh, Pennsylvania.

Chang, S. and Ho, C. (2006). 'Organisational factors to the effectiveness of implementing information security management'. Information Management & Computer Security, vol.106, pp.345-361.

Charmaz, K. (2006). Constructing Grounded Theory. SAGE publications.

Flechais, I. and Sasse, M. (2007). 'Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science'. I. J. Human-Computer Studies .

Hawkey, K., Botta, D., Werlinger, R., Muldner, K., Gagne, A., and Beznosov. K. (2008) 'Human, organizational, and technological factors of it security'. Accepted at CHI 2008 (Research Landscapes), (to appear).

Garigue, R. and Stefaniu, M. (2003). 'Information Security Governance Reporting'. EDPACS 31(6):11–17.

Gonzalez, J., et al. (2005). 'Helping prevent information security risks in the transition to integrated operations'.

Jiwnani, M. and Zelkowitz, K. (2002). 'Maintaining software with a security perspective'. Software Maintenance, 2002. Proceedings. International Conference on pp. 194–203.

Kankanhalli, A., et al. (2003). 'An integrative study of information systems security effectiveness'. International Journal of Information Management 23.

Karyda, M., et al. (2006). 'A framework for outsourcing IS/IT security services'. Information Management & Computer Security 14:403–416.

Knapp, K., et al. (2006). 'Information security: management's effect on culture and policy'. Information Management & Computer Security 14(1):24–36.

Koskosas, I. and Paul, R. (2004). 'The interrelationship and effect of culture and risk communication in setting internet banking security goals'. In ICEC '04, pp. 341–350, New York, NY, USA. ACM Press.

Kraemer, S. and Carayon, P. (2007). 'Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists'. Applied Ergonomics 38:143–154.

Pattinson, M. and Anderson, G. (2007). 'How well are information risks being communicated to your computer end-users?'. Information Management & Computer Security 15.

Rayford, R., Vaughn, B. and Fox, K. (2001). 'An empirical study of industrial securityengineering practices'. The Journal of Systems and Software 61:225–232.

Sandelowski, M. (2000). 'Whatever Happened to Qualitative Description?'. Research in Nursing & Health 23(4):334–340.

Straub, D. and Welke, R. (1998). 'Coping with systems risk: security planning models for management decision making'. MIS Q. 22(4):441–469.

Sveen, F., et al. (2007). 'Toward Viable Information Security Reporting Systems'. Information Management & Computer Security 15(5):408–419(12).

Thomson, K. and von Solms, R. (2005). 'Information security obedience: a definition'. Computers & Security 24(1):69–75.

Tsohou, A., et al. (2006). 'Formulating information systems risk management strategies through cultural theory'. Information Management & Computer Security 14(3):198–217.

Welch, S. and Lathrop, D. (2003). 'Wireless security threat taxonomy'. Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society pp. 76–83.