Received 4 October 2008
Revised 31 October 2008
Accepted 1 November 2008

An integrated view of human, organizational, and technological challenges of IT security management

Rodrigo Werlinger, Kirstie Hawkey and Konstantin Beznosov
Electrical and Computer Engineering, University of British Columbia, Vancouver, Canada

Abstract

Purpose – The purpose of this study is to determine the main challenges that IT security practitioners face in their organizations, including the interplay among human, organizational, and technological factors.

Design/methodology/approach – The data set consisted of 36 semi-structured interviews with IT security practitioners from 17 organizations (academic, government, and private). The interviews were analyzed using qualitative description with constant comparison and inductive analysis of the data to identify the challenges that security practitioners face.

Findings – A total of 18 challenges that can affect IT security management within organizations are indentified and described. This analysis is grounded in related work to build an integrated framework of security challenges. The framework illustrates the interplay among human, organizational, and technological factors.

Practical implications – The framework can help organizations identify potential challenges when implementing security standards, and determine if they are using their security resources effectively to address the challenges. It also provides a way to understand the interplay of the different factors, for example, how the culture of the organization and decentralization of IT security trigger security issues that make security management more difficult. Several opportunities for researchers and developers to improve the technology and processes used to support adoption of security policies and standards within organizations are provided.

Originality/value – A comprehensive list of human, organizational, and technological challenges that security experts have to face within their organizations is presented. In addition, these challenges within a framework that illustrates the interplay between factors and the consequences of this interplay for organizations are integrated.

Keywords Data security, Communication technologies

Paper type Research paper

The authors thank the anonymous HAISA reviewers who provided constructive and helpful comments on the conference version of this paper. Members of the HOT Admin project and the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) gave periodic feedback on the research reported in current and early drafts of this paper; special thanks to David Botta and Kasia Muldner for their detailed comments. Members of Werlinger's Masters examination committee, Sidney Fels and Philippe Kruchten, provided feedback that ultimately further improved this paper. Craig Wilson helped to improve its readability. This research was supported by the Canadian NSERC Strategic Partnership Program, Grant STPGP 322192-05.

Information Management & Computer Security
Vol. 17 No. 1, 2009
pp. 4-19

0968-5227
DOI 10.1108/09685220910944722

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 hubman and organizational factors (Beznosov and Beznosova, 2007; Botta *et al.*, 2007; Rayford *et al.*, 2001). While there have been studies of specific challenges of IT security management (Koskosas and Paul, 2004; Knapp *et al.*, 2006; Audestad, 2005) or sets of challenges along one of the factors (Kankanhalli *et al.*, 2003; Chang and Ho, 2006), none have provided a comprehensive integrated overview of the challenges faced by security practitioners. 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 and 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 final data set consisted of 36 interviews with security practitioners from 17 different organizations, both academic and non-academic (private, government). Our results not only validate and extend other studies that address challenges facing security practitioners, but also provide an integrated framework that classifies these challenges. This framework can help organizations identify their limitations with respect to implementing security standards and 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 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 the technology and processes used to support the adoption of security policies or standards within organizations. To illustrate, we found that security processes should consider that IT 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. This paper is an extension of a earlier version based on the first 27 interviews (Werlinger *et al.*, 2008a).

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 discuss the interplay between the challenges, ground our findings in prior research, and discuss opportunities to address the challenges through improvements to tool design and processes (Section 5). We end Section 5 by discussing limitations of our approach and opportunities for future research on challenges and provide final conclusions in 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 IT 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. Our definitions of human, organizational,

and technological aspects were adapted from Beznosov and Beznosova (2007) who define technical, human, and social aspects of IT security.

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 and 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 and 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 to best security practices. Kraemer and Carayon (2007) define human error as a human but non-deliberate accidental cause of poor computer and information security (e.g., an accidental programming error that causes a computer to crash under certain circumstances). Kraemer and 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 concluded 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 concluded that factors such as top management support, size, and organization type are related to the implementation of security controls. Additionally, their findings suggest that the uncertainty of environmental elements, including rapid 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 concluded that this factor is critical for implementing security controls within organizations. Similarly, Straub and Welke (1998) study the impact of

management training on the implementation of security plans in two technical services organizations. They concluded that managers are not aware of the full spectrum of actions that can be taken to reduce risks, but that 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) saggests that one of the reasons for not reaching 100 percent 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 and Lathrop (2003) study the complexity of wireless networks and the challenges this poses to security practitioners. Jiwnani and Zelkowitz (2002) describe security testing of systems as a lengthy, complex, and costly process. They propose a taxonomy to classify vulnerabilities and assist security practitioners in the prioritization of resources to rectify 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 and 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 this gap. 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?

(3) What are the implications of these challenges for future research?

Our analysis of security challenges is part of the ongoing HOT Admin project (Hawkey *et al.*, 2008), whose long-term goal is to construct a set of guidelines for evaluating and developing tools used for managing IT security. In order to learn about the human, organizational, and technological aspects of IT management, we evaluated the use of work shadowing, contextual interviews (Beyer and Holtzblatt, 1998), and semi-structured interviews. The first two instruments would give us fine-grained data on the work of security practitioners and their challenges, whereas the third would reveal the goals that they had in mind. Recruiting security practitioners can be difficult (Kotulic and Clark, 2004), and none that we contacted were willing to engage in work shadowing or contextual interviews. Therefore, our data consists of *in situ* semi-structured interviews.

A graduated recruitment strategy was employed; this is described in detail in Botta *et al.* (2007). The project obtained 39 completed questionnaires that led to 21 interviews with IT professionals with security responsibilities; the remaining participants were recruited directly through contacts and referrals. When available, the questionnaire provided demographic information, while the semi-structured interviews covered various aspects of IT security. For those participants who did not complete a questionnaire, we requested demographic information during the interview. During the semi-structured interviews, 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.

In total, we conducted 36 interviews with 36 security practitioners from 17 unique organizations (3 academic, 14 non-academic). We refer to interview numbers rather than participant numbers, as some interviews contained two participants (I1, 17, I6, I22). In these interviews, one participant was the primary interviewee, while the other added details or confirmed recollections of events. From two of those interviews (I1, I17), the secondary participant was recruited for an individual interview about their own experiences (I3 and I18, respectively). Furthermore, we re-interviewed two participants (I9, I24) several months later to gather additional details about their challenges during the deployment of an intrusion detection system. We indicate throughout the results whether the challenges were discussed during the initial interview (I9A, I24A) or the follow-up interview (I9B, I24B).

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. In 32 of the interviews (30 + the 2 follow-up interviews), participants explicitly discussed challenges (see Table I for their profiles). We have omitted I6, I13, I13, and I26 from the table as those participants did not directly discuss challenges of IT security management.

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 implementing security controls within their organizations. These situations were coded iteratively, starting with open coding and continuing with axial coding. Results were then organized by the types of challenges (e.g. lack of resources to implement

Type of organization	Interviews	Job description
Financial services 1	I4	IT Security Specialist
Financial services 2	I25	IT Security Specialist
Insurance services	I5, I29	IT Security Specialist
Security consulting services 1	I23	IT Security Specialist
Security consulting services 2	I27	IT Security Specialist
Non-profit medical services	I19	IT Systems Specialist
Retail/Wholesale	I28	IT Systems Specialist
Government	I33	IT Systems Manager
Technology	I30, I31	IT Security Managers
Telecommunications 1	I32	IT Security Specialist
Telecommunications 2	I34	IT Security Manager
Manufacturing	I16	IT Manager
	I21	IT Security Specialist
Research institution	I12	IT Systems Specialists
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 Specialists

Table I.
Profile of our participants and their organizations

security controls). Posterior analysis was based on further elaboration of "memos" (Charmaz, 2006) written during the coding process. Following a theoretical sampling approach, interview questions were adjusted three times (before interviews 15, 22, and 27), in order to validate emerging theories. For the overall project (Hawkey *et al.*, 2008), five 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. We classified these challenges as human, organizational, or technological using the definitions described in Section 2. Given that some challenges are multi-dimensional and can be classified in different ways depending on the particular interpretation of the researcher, our emphasis is on understanding the different types of challenges that affect the work of security practitioners. Table II provides a summary of these challenges and their distribution across academic and non-academic organizations. We next describe in more detail the human, organizational, and technological challenges identified by our participants. Where appropriate, we illustrate the more general challenges with specific aspects discussed by participants.

4.1 Human factors

We classified three challenges as human factors:

(1) lack of security training;

Type	Challenge	Organization type: Academic	Organization type: Non-academic
Human	Lack of training or experience	I14, I18	I19, I27, I32, I33
	Culture within the organization	I22	I5, I16, I19
	Communicate security issues	I2, I7, I9A, I12, I14	I5, I25
Organizational	Risk estimation	I20	I4, I25
	Open environments and academic freedom	I1, I3, I9A, I11, I15, I20	NA
	Lack of budget	I2, I3, I18	I16, I19, I30
	Security as low priority	I17, I24A	I5, I16, I18, I23, I25, I27, I30, I32
	Tight schedules	I7	I25
	Business relationships with other organizations	I17	I4, I5, I16, I25
	Distribution of IT responsibilities	I2, I9A, I11, I17	I16, I21
	Access control to sensitive data	I9A, I17, I20	I4, I5, I25, I29
	Size of the organization	None	I27, I30, I32, I31
	Top management support	I1, I2, I9A, I24A	I32
Technological	Complexity of systems	I11, I15	I23, I31
	Vulnerabilities (system/application)	I22	I25
	Mobility and distributed access	I14	I27, I32
	Lack of effective security tools	I3, I9A, I9B, I12, I24B	I30, I31

Table II. Summary of challenges of implementing security controls and distribution of those challenges across interviews with participants from academic and non-academic organizations

(2) lack of a security culture; and
(3) communication of security issues.

These factors were particularly challenging for participants who had to actively interact with other people across the organization to implement security controls.

Lack of security training was a common challenge (I14, I18, I19, I27, I32, I33). Specifically, it was found to be 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.

Lack of a security culture within organizations made it difficult to change employees' existing security practices (I5, I16, I19, I22). For example, several employees might use 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).

Communication of security issues was challenging for participants (I2, I5, I7, I12, I19, I24A, I25). Some thought that employees must understand the goals of the security controls without feeling that they have to blindly follow orders from the IT security group (I2, I25). Communication was found to be particularly difficult when stakeholders do not hold a common view of risks (I5, I14). For example, to avoid communication breakdowns with other stakeholders (e.g. business people) who did not share the same perception of security risks, participants had to assume 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:

- risk estimation;
- open environments and academic freedom;
- lack of budget;
- security as a secondary priority;
- tight schedules;
- business relationships with other organizations;
- distribution of IT responsibilities;
- access control to sensitive data;
- size of the organization; and
- top management support.

Risk estimation was mentioned in several interviews (I4, I14, I20, I25). Participants found it difficult to assess both the potential consequences if the risks were not mitigated, as well as the success of mitigation controls (I20, I25). Stakeholders were said to require 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 several participants (I1, I3, I9 A, I11, I15, I20). They 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 were initiated using the organization's IT systems.

Budgetary restrictions for security programs was also a challenge discussed by participants (I2, I3, I16, I18, I19, I30). The implementation of security technologies can be costly (I19). It was also said to be 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 organizations (I5, I16, I17, I18, I23, I24A, I25, I27, I30, I32). As one participant described, "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 non-academic organizations discussed the trade-off between security and 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 of or trained about the security controls in the organization (I17).

Tight schedules as a result of business priorities were seen as a related challenge (I7, I25). Tight schedules may result in human errors that could 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 (I4, I5, I16, I17, I25). 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 participants (I2, I9A, I11, I16, I17, I21). 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 challenges posed by interactions with other organizations, as in both cases decisions about IT security involve distributed entities.

Controlling access to data was an important challenge for our participants (I4, I5, I9A, I17, I20, I25, I29). It is particularly challenging for organizations without centralized access control when sensitive data is distributed in different areas of the organization and this data needs to be accessed by stakeholders from different networks and systems.

Size of the organization was a factor that had an impact on the management of IT security solutions (I27, I30, I31, I32). When the organization had many interconnected systems (e.g., servers, networks, databases), it was difficult to understand how security controls could be integrated in the existing infrastructure (I27, I32). Large organizations (in terms of divisions, branches and quantity of people) can find it difficult to recruit managers with the ability of assessing security risk, considering the complexity of technical and managerial aspects (I31).

Top management support was another common challenge (I1, I2, I9A, I24A, I32). One participant (I32) identified it as a determinant factor in the map of challenges. When there is no support from management, security is not a priority within organizations. However, when top management understands the importance of IT security and gives more priority to security practices, employees within the organizations follow this example and incorporate security practices in their day-to-day activities.

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:

- complexity of systems;
- vulnerabilities in systems and applications;
- mobile and distributed access; and
- lack of efficient security tools.

The complexity of systems is a challenge for many (I11, I15, I23, I31). The need for having open and secure networks had an influence on the interactions between participants and security vendors; it can be difficult for vendors to understand the architecture of the network and offer products that suit the organization's needs (I15). The complexity of networks and systems is also a challenge when implementing security controls in organizations (I23). 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.

Vulnerabilities complicated the work of security practitioners who had to protect their systems against potential attacks (I22, I25). Participants had to continually monitor security updates and install security patches to protect their systems. One (I22) uses additional software to keep track of patch management of vulnerabilities in the open-source applications.

Mobility and distribution of user access can make it difficult to control access to internal resources (I14, I27, I32). Laptops, which can be taken from the workplace and

are used by employees without technical expertise, were 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 during home usage.

Lack of effective support from security tools was mentioned as being a problem in performing specific security activities (I3, I9A, I9B, I12, I30, I31, I24B). One participant (I31) complained about the lack of effective support from security tools to perform security audits in the systems. According to him, security tools are too bloated and difficult to use to perform simple, specific tasks (e.g. scan a system). The high number of false positives was another challenge for the reliability and effective use of some security tools, such as network scanners (I31) and intrusion detection systems (I3, I9A, I9B, I12, I24B).

5. Discussion

We discuss our results from three different perspectives:

(1) We describe the interplay among challenges.

(2) We ground our results in prior research and discuss research opportunities to address the challenges by improving security tools and processes. Where possible, we propose characteristics that these tools and processes should have to support security practitioners in real contexts.

(3) We discuss limitations of our approach, particularly with respect to our ability to perform a cross analysis of the challenges described by participants, considering their organizations and positions.

We also discuss the future work required to validate and refine the framework of challenges.

5.1 A holistic view of challenges and their interrelationships

Kankanhalli *et al.* (2003), Knapp *et al.* (2006), and Chang and Ho (2006) relate organizational variables such as size, type of business, environmental elements (e.g. customers' security requirements), and top management support to security effectiveness, security culture, and enforcement of security policies within organizations. Our framework identifies these and other organizational variables that make it more complex to manage 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, the challenge of communicating security issues was adversely affected by both the human challenge of different perceptions of risks and the organizational challenge of IT management distribution. The lack of security training negatively impacted the support and 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.

5.2 Opportunities to address the challenges

The challenges we have described not only illustrate the complexity of the environment where security practitioners work, but also show the limitations that organizations face

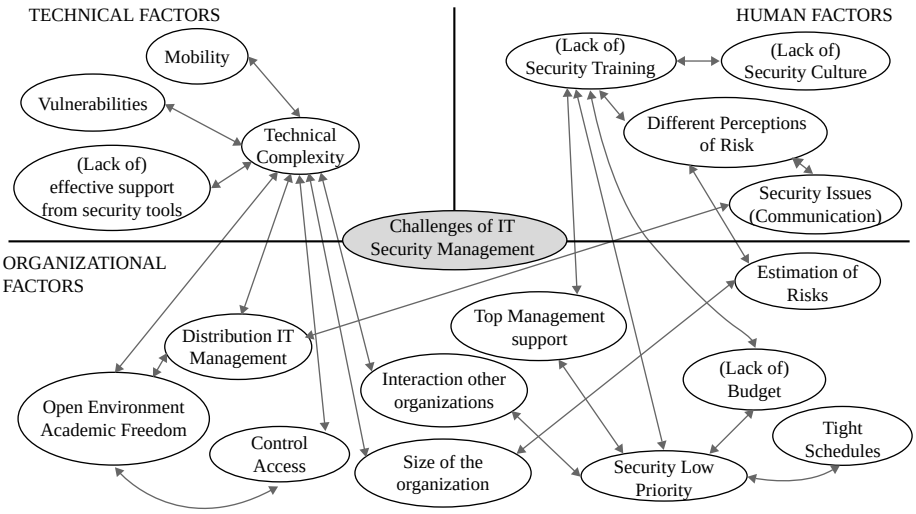

Figure 1.
An integrated view of challenges and their interrelationships. The arrows show the interplay among the different challenges

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 security risks and the need for security controls to other stakeholders. Pattinson and Anderson (2007) highlight the importance of risk perceptions for end-users and how important it is to communicate these risks to them. Koskosas and 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 views different stakeholders (not just end-users) have about security risks. A good starting point for addressing communication issues may be to apply Tsohou *et al.*'s (2006) proposal of using culture theory to communicate security risks, but focusing 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 to communicate security issues (i.e. reports customizable to the security knowledge or position of the recipient) as identified by Botta *et al.* (2007) during preliminary analysis of the first 14 interviews of our data set. Our further analysis, which incorporated 22 more interviews, reveals that improved integration between security and communication tools is also 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 and Carayon (2007) relate the lack of time, resources, and inconsistent communication among the staff with errors 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 show not only security vulnerabilities, but also give better support for determining how security practitioners should prioritize their tasks, considering the different levels of security risks facing the different systems.

Distribution in relation to controlled access to data had two facets:

(1) controlling access by users who are distributed and use different access technologies; and

(2) controlling 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 that can restrict every access and action. We propose that security processes and technologies must be developed with the assumption of use in distributed environments. They should be flexible enough to both provide controlled access to highly distributed data and improve communication channels among the different stakeholders who access those data. Further research on the activities of security practitioners and their interactions with other stakeholders within organizations can be found in Werlinger *et al.* (2008b).

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 should share their experiences about security incidents, vulnerabilities, and culture with other stakeholders. For example, Gonzalez *et al.* (2005) developed mental models that integrate the fragmented knowledge from different experts. These models identify 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 artifacts to enforce best IT practices (Thomson and 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 and Sasse, 2007) look appropriate for spreading the tacit knowledge used to build the policies.

We found that the organizational challenges of 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 on 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 outset. 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.

We have shown that the technical complexity of systems is affected by several organizational factors. Security tools could provide better support to address this complexity by including novel usability features. These features should consider the map of challenges that interplay in the work of security practitioners. For example, the implementation of intrusion detection systems (IDS) could be positively affected if these security tools had better reporting capabilities, as we show in Werlinger *et al.* (2008). In the scenario of IT distribution where stakeholders have different perceptions of risk, reports of alarms from IDSs should be customizable in order to fit the level of abstraction that each stakeholder requires to make informed decisions.

5.3 Limitations and future work

While our approach allowed us to investigate in detail the challenges that security practitioners face within organizations, this approach was not without limitations. Semi-structured interviews provided us with rich data about the challenges faced by security practitioners. While rich, this data is limited to a small number of security practitioners. Furthermore, during the semi-structured interviews, not all topics were discussed at the same level of detail with all of the participants. Our analysis, therefore, does not focus on differences in the challenges faced by participants. Rather, our findings are centered on the commonalities in their descriptions. For example, 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.

The variety of organizations whose participants we interviewed, in terms of industrial sector (Table I) and size (ranging from <5 employees to large, multinational companies), has given us a broad perspective about the challenges faced by security practitioners. One difference we found was that those participants from academic institutions face challenges related to academic freedom and the need for an open environment that limit their ability to impose security practices and mitigate risks. However, the other challenges appear to be comparable across sectors, even if not mentioned uniformly by participants from academic and private sectors (Table II). For example, challenges related to the distribution of IT management were similar for both academic and non-academic 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 argue that most differences are explained by the dynamic nature of the semi-structured interviews. As participants were asked to talk about their challenges rather than if they experienced specific challenges, lack of discussion of a particular challenge does not necessarily mean that it is not applicable.

The broad perspective of challenges given by the variety of organizations in our sample also represents a limitation of this study. For example, we lack a sufficient number of organizations of the same size in each sector to perform an analysis considering the effect of organizational factors – such as organization size – on our results. Our findings do validate and extend prior research, as our sample of

participants contrasts in quantity and type with those from similar studies (Koskosas and Paul (2004) performed 15 interviews in three organizations; Kraemer and Carayon (2007) performed 16 interviews in two academic laboratories). However, more data are necessary in order to empirically test similarities and differences according to position, employment sector, and other organizational attributes such as size of the organization. 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.

Despite these limitations, we believe that our framework of challenges (Section 5.1) provides enough information to understand the complexity of security-related challenges. It can be used to explain the interplay of different factors faced by security practitioners when they perform their activities, and might help to improve security processes and tools. However, as noted above, more data are needed to expand and refine the framework. For example, validation of the framework with a large number of participants from organizations of different sizes within each sector may allow us to extend it to understand if and how the size or the sector of the organization is a challenge for security practitioners. Furthermore, variations of the framework could be developed that focus on the challenges perceived by participants at different levels within the organization (e.g. manager vs analyst; security-focused vs general IT). Another option is to break down the framework into individual, smaller sub-frameworks specific to each challenge faced by security practitioners.

6. Conclusion

We have used empirical data and prior work to provide an integrated view of the various human, organizational, and technological challenges that security experts face within their organizations. To the best of our knowledge, this is the first empirical study to provide 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 in implementing security policies, and determine what is relevant when making decisions regarding IT security. We have discussed how the different challenges interplay, and have suggested various research opportunities for addressing these challenges through improvements to security processes and technologies, considering their human and organizational factors. More research is needed to fully understand how security challenges interplay, as this interaction affects the improvements organizations can make in their management of IT security. In this vein, we are currently developing a survey to administer to security practitioners that will help us refine and generalize our results.

References

Audestad, J. (2005), "Four reasons why 100% security cannot be achieved", *Telektronikk*, Vol. 1, pp. 38-47.

Beyer, H. and Holtzblatt, K. (1998), *Contextual Design, Defining Customer-Centered Systems*, Morgan Kaufmann Publishers, San Francisco, CA.

Beznosov, K. and Beznosova, O. (2007), "On the imbalance of the security problem space and its expected consequences", *Information Management & Computer Security*, Vol. 15 No. 5, pp. 420-431(12).

Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S. and Fisher, B. (2007), "Towards understanding IT security professionals and their tools", *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, A*CM*, *Pittsburgh, PA*, pp. 100-11.

Chang, S.E. and Ho, C.B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106, pp. 345-61.

Charmaz, K. (2006), *Constructing Grounded Theory*, Sage, Newbury Park, CA.

Flechais, I. and Sasse, M.A. (2007), "Stakeholder involvement, motivation, responsibility, communication: how to design usable security in e-science", *International Journal of Human-Computer Studies*.

Garigue, R. and Stefaniu, M. (2003), "Information security governance reporting", *EDPACS*, Vol. 31 No. 6, pp. 11-17.

Gonzalez, J.J., Qian, Y., Sveen, F.O. and Rich, E. (2005), "Helping prevent information security risks in the transition to integrated operations", *Telektronikk*, Vol. 1, pp. 29-37.

Hawkey, K., Botta, D., Werlinger, R., Muldner, K., Gagne, A. and Beznosov, K. (2008), "Human organizational, and technological factors of IT security", *CHI'08 Extended Abstract on Human Factors in Computing Systems*, Florence, pp. 3639-44.

Jiwnani, K. and Zelkowitz, M. (2002), "Maintaining software with a security perspective", *Proceedings of the International Conference on Software Maintenance*, pp. 194-203.

Kankanhalli, A., Teo, H-H., Tan, B.C. and Wei, K-K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, p. 23.

Karyda, M., Mitrou, E. and Quirchmayr, G. (2006), "A framework for outsourcing IS/IT security services", *Information Management & Computer Security*, Vol. 14, pp. 403-16.

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N. (2006), "Information security: management's effect on culture and policy", *Information Management & Computer Security*, Vol. 14 No. 1, pp. 24-36.

Koskosas, I.V. and Paul, R.J. (2004), "The interrelationship and effect of culture and risk communication in setting internet banking security goals", *Proceedings of the 6th International Conference on Electronic Commerce*, ACM Press, New York, NY, pp. 341-50.

Kotulic, A.G. and Clark, J.G. (2004), "Why there aren't more information security research studies", *Information & Management*, Vol. 41 No. 5, pp. 597-607.

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*, Vol. 38, pp. 143-54.

Pattinson, M.R. and Anderson, G. (2007), "How well are information risks being communicated to your computer end-users?", *Information Management & Computer Security*, Vol. 15 No. 5, pp. 362-71.

Rayford, B., Vaughn, R.H. Jr and Fox, K. (2001), "An empirical study of industrial security-engineering practices", *The Journal of Systems and Software*, Vol. 61, pp. 225-32.

Sandelowski, M. (2000), "Whatever happened to qualitative description?", *Research in Nursing & Health*, Vol. 23 No. 4, pp. 334-40.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision making", *MIS Q*, Vol. 22 No. 4, pp. 441-69.

Sveen, F.O., Sarriegi, J., Rich, E. and Gonzalez, J. (2007), "Toward viable information security reporting systems", *HAISA'07: Human Aspects of Information Security and Assurance*, pp. 114-27.

Thomson, K. and von Solms, R. (2005), "Information security obedience: a definition", *Computers and Security*, Vol. 24 No. 1, pp. 69-75.

Tsohou, A., Karyda, M. and Kokolakis, S. (2006), "Formulating information systems risk management strategies through cultural theory", *Information Management & Computer Security*, Vol. 14 No. 3, pp. 198-217.

Welch, D. and Lathrop, S. (2003), "Wireless security threat taxonomy", paper presented at: Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, pp. 76-83.

Werlinger, R., Hawkey, K. and Beznosov, K. (2008a), "Human, organizational and technological challenges of implementing IT security in organizations", *HAISA'08: Human Aspects of Information Security and Assurance*, *Plymouth, England*, pp. 35-48.

Werlinger, R., Hawkey, K. and Beznosov, K. (2008b), "Security practitioners in context: their activities and interactions", *CHI'08 Extended Abstracts on Human Factors in Computing Systems*, Florence, pp. 3789-94.

Werlinger, R., Hawkey, K., Muldner, K., Jaferian, P. and Beznosov, K. (2008c), "The challenges of using an intrusion detection system: is it worth the effort?", *Proceedings of the Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, Pennsylvania*, pp. 107-16.

Corresponding author
Rodrigo Werlinger can be contacted at: rodrigow@ece.ubc.ca