MIS Quarterly

SPECIAL ISSUE

USER PARTICIPATION IN INFORMATION SYSTEMS SECURITY RISK MANAGEMENT[1]

By: **Janine L. Spears**
DePaul University
243 South Wabash Avenue
Chicago, IL 60604
U.S.A.
jspears@cdm.depaul.edu

Henri Barki
HEC Montréal
3000, chemin de la Côte-Ste-Catherine
Montréal, QC H3T2A7
CANADA
henri.barki@hec.ca

Abstract

This paper examines user participation in information systems security risk management and its influence in the context of regulatory compliance via a multi-method study at the organizational level. First, eleven informants across five organizations were interviewed to gain an understanding of the types of activities and security controls in which users participated as part of Sarbanes-Oxley compliance, along with associated outcomes. A research model was developed based on the findings of the qualitative study and extant user participation theories in the systems development literature. Analysis of the data collected in a questionnaire survey of 228 members of ISACA, a professional association specialized in information technology governance, audit, and security, supported the research model. The findings of the two studies converged and indicated that user participation contributed to improved security control performance through greater awareness, greater alignment between IS security risk management and the business environment, and improved control development. While the IS security literature often portrays users as the weak link in security, the current study suggests that users may be an important resource to IS security by providing needed business knowledge that contributes to more effective security measures. User participation is also a means to engage users in protecting sensitive information in their business processes.

Keywords: Information security, user participation, security risk management, Sarbanes-Oxley Act

Introduction

It is estimated that at least half of the breaches to information systems security are made by internal personnel, attributed primarily to unauthorized system access (Gordon et al. 2005). The occurrence of IS security breaches by internal personnel may be reduced if greater emphasis were placed on internal threats to IS security that can occur when employees handle information in their day-to-day jobs. Instead, it is widely believed that organizational efforts to manage IS security are typically focused on vulnerabilities in technological assets such as hardware, software, and networking, at the expense of managing other sources of vulnerabilities, such as people, policies, processes, and culture (see Halliday et al. 1996; Hu et al. 2006; Jahner and Krcmar 2005; Spears 2005; Straub and

[1]Mikko Siponen was the accepting senior editor for this paper. Richard Baskerville served as the associate editor.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

Welke 1998; von Solms and von Solms 2004). Moreover, technology-focused IS security is typically centered on external threats, such as hackers and viruses (see, Doherty and Fulford 2005; Whitman 2004), leaving organizations open to breaches from the inside.

The IS security literature typically portrays users as the weak link in security, either from mistakes or computer crimes (e.g., Dhillon and Moores 2001; Siponen 2000b; Wade 2004). While some authors have noted that users may be both the problem and solution (e.g., Stanton and Stam 2006; Whitman 2008) and that users may have a valuable role in security design (Siponen 2005), the literature is lacking in empirical studies that examine more closely how users can make a positive impact on IS security. Based on the premise that, rather than being the weak link, users may be a valuable resource in managing IS security risks, the present paper's research question asks how users participate in IS security risk management within business processes, and how their participation is perceived to impact IS security.

There are at least two reasons why user participation in IS security risk management can be valuable. First, user awareness of the risks to IS security is widely believed to be fundamental to effective IS security (Aytes and Connolly 2004; Furnell 2008; Goodhue and Straub 1991; Hu et al. 2006; Siponen 2000a, 2000b; Straub and Welke 1998; Whitman 2004). That is, organizational security controls (i.e., policies, procedures, safeguards, and countermeasures that prevent, detect, or minimize an IS security breach) can only be effective to the extent that people handling the information in their day-to-day jobs (e.g., functional business users) are aware of those measures and adhere to them. Indeed, Goodhue and Straub (1991, p. 13) suggested that "since protective measures often require significant managerial vigilance, an appropriate level of awareness and concern may be a prerequisite for adequate security protection." User participation is likely to be useful in achieving this awareness.

Second, security controls need to be aligned with business objectives to be effective (Alberts and Dorofee 2003; Halliday et al. 1996; ITGI 2005; McAdams 2004; Suh and Han 2003). Such alignment requires an understanding of the relative value of information, how information is used within and across business processes, and at what nodes within a process sensitive information is most vulnerable. User participation in IS security risk analysis and control design can provide needed business knowledge, thus contributing to more effective security measures.

User participation in information system development (ISD) and its influence on the eventual success of implemented systems has been an important research topic since at least the 1970s (e.g., Baroudi et al. 1986; Hartwick and Barki 1994; Ives and Olson 1984; Swanson 1974). In ISD contexts, user participation outcomes have largely been attributed to affective outcomes, such as satisfaction and psychological attachment. However, some organizational behavior scholars have argued that the greatest effect of participation may be cognitive, such as information exchange and knowledge transfer (Latham et al. 1994; Locke et al. 1997). While ISD researchers have acknowledged user participation's cognitive effects (Ives and Olson 1984), the literature lacks empirical studies that examine such effects. Thus, the present paper examines the cognitive effects of user participation in IS security contexts. The objective of the present paper is to examine what user participation is in security contexts and how it influences the performance of IS security controls in organizations. In doing so, the paper answers calls for IS security research that applies theory from the IS literature (Dhillon and Backhouse 2000), and calls for research on user participation in current contexts (Markus and Mao 2004).

The remainder of the paper is organized as follows. First, the concept of user participation is characterized by extant theories in ISD, followed by its conceptualization in IS security contexts. Next, the study's multi-method research design is outlined, followed by a qualitative exploratory study that examined user participation in IS security risk management for regulatory compliance. A theoretical model informed by extant user participation theories and the qualitative study is then tested in a confirmatory quantitative study. Finally, the paper concludes with a discussion of the implications of the study, limitations, and suggestions for future research.

Theory

User Participation in ISD

The information systems development (ISD) literature has examined user participation predominantly in the context of business users participating with IS professionals in the planning, design, and implementation of an information system (Baroudi et al. 1986; for informative reviews, see Ives and Olson 1984; Markus and Mao 2004). In ISD contexts, Barki and Hartwick (1994; Hartwick and Barki 2001) defined user participation as the extent to which users or their representatives carry out assignments and perform various activities and behaviors during ISD and conceptualized it along four dimensions: users' hands-on performance of activities, responsibility, relations with IS, and communication with IS staff and senior management.

A recent synthesis of the user participation literature identified three underlying theories, labeled as *buy-in*, *system quality*, and *emergent interactions*, that explain how participation influences system success (Markus and Mao 2004). According to the buy-in theory of participation, the effort users invest during their participation and the influence they have in ISD makes them perceive the system as more personally relevant and important. In turn, this psychological state of increased involvement is thought to positively influence their attitudes (i.e., those who participate tend to like the system more), as well as their usage of the system (Barki and Hartwick 1989, 1994; Hartwick and Barki 1994, 2001).

According to the system quality theory, when users participate in ISD, system developers become better informed about business needs, which then results in higher quality and more successful systems (Markus and Mao 2004). User participation is believed to be particularly useful when an ISD project is large, conceptually new, or the task is complex (e.g., Markus and Mao 2004). Implicit in the system quality theory is the importance of the cognitive effects of participation as a mechanism for improving system quality.

Finally, according to the emergent interactions theory, when users participate in ISD, they develop a relationship with the IS professionals, and the nature of this relationship influences system success. A "good" relationship is likely to lead to success not only in terms of higher quality systems (because the IS professionals become more likely to consider business needs in their designs), but also in terms of relational and affective outcomes (e.g., higher levels of user and designer satisfaction); in contrast, "bad" relationships that are frequently fraught with conflicts and disputes are likely to lead to less positive outcomes (Markus and Mao 2004).

Based on their synthesis of the IS user participation literature and their acknowledgment of evolving IS contexts, Markus and Mao (2004, pp. 523-524) suggested that researchers "reconceptualize IS participation theory's core concepts and the relationships among them" in order to determine how change agents may employ participation practices to increase the chances of success in varied IS development contexts. As a result, the present paper reconceptualizes the success outcomes, actors, activities, and hypothesized links between activities and outcomes of user participation by applying the buy-in, system quality, and emergent interaction theories of user participation in IS security risk management contexts. In doing so, the paper examines how participation may be employed to improve IS security.

Security Risk Management

Security risk management (SRM) is a continuous process of identifying and prioritizing IS security risk, and implementing and monitoring controls (i.e., countermeasures, safeguards) that address those risks (e.g., Alberts and Dorofee 2003; ISO/IEC 2000; ITGI 2005; NIST 2004). The present paper distinguishes between the process of managing security risk and the controls (technological or manual) that are the output of that process. SRM includes the strategies, policies, activities, roles, procedures, and people used to manage security risk, while the resulting controls are intended to reduce the likelihood or impact of a breach. In other words, effective SRM is expected to result in a system of controls that collectively protect IS security, defined as the preservation of an information system's confidentiality, integrity, and availability (ISO/IEC 2000). Thus, IS security, as used in the present paper, encompasses both SRM and the resulting security controls.

Transposing Barki and Hartwick's (1994) conceptualization of user participation in ISD to IS security contexts, user participation in SRM is defined as the set of behaviors, activities, and assignments undertaken by business users during risk assessment and the design and implementation of IS security controls. User participation is expected to add value to SRM, which in turn contributes to effective controls that ultimately improve security; that is, the possibility or severity of a security breach is reduced.

A Multi-Method Research Design

A combination of data collection and analysis methods were used on separate samples to examine user participation in SRM. Interviews were conducted with one sample, followed by a survey study on a different sample of professionals who had worked on compliance with the Sarbanes-Oxley Act for their respective organizations. This multi-method[2] (also referred to as mixed-method and pluralist) approach was chosen based on the premise that separate and dissimilar data sets drawn on the same phenomena would provide a richer picture (Sawyer 2001, p. 180) of the concept of and outcomes associated with user participation than would a mono-method approach. A sequential design (Hanson et al. 2005; Mingers 2001) was used in that the qualitative exploratory study informed a subsequent confirmatory study.

[2]For a detailed discussion on multi-method research, see Mingers (2000) and Newman et al. (2002).

Qualitative methods were appropriate given the high degree of uncertainty surrounding the phenomenon under study (Trauth 2001); that is, not enough was known *a priori* about user participation in the context of SRM to quantitatively measure it or pre-specify its outcomes. Thus, qualitative methods provided a rich understanding of the activities, behaviors, and assignments that define user participation in the context of SRM for regulatory compliance. Secondly, qualitative methods allowed a process model to be constructed by applying the three user participation theories described by Markus and Mao (2004) as a framework for analysis. A process model is based on a narrative explanation of a sequence of events that contribute to a specific outcome (Tsohou et al. 2008, p. 275). While extant user participation theories were used as a framework of analysis, data collection for the qualitative study was not based on any *a priori* theories, concepts, or outcomes, and therefore was exploratory.

Quantitative methods were then employed to test the theoretical model derived from the qualitative study and based on the researchers' understanding (Lee 1991). Hypotheses that were constructed from the qualitative study formed a variance model that examined the degree to which user participation explained variation in pre-specified outcome variables (Tsohou et al. 2008). Thus, combining qualitative and quantitative methods provided both a rich context and testability to the study (Kaplan and Duchon 1988). In addition, this multi-method design strengthened the results through triangulation, meaning cross-validation of both kinds and sources of data were found congruent (Kaplan and Duchon 1988). Details on how qualitative and quantitative methods were employed are summarized in Appendix A.

The Sarbanes-Oxley Act as Context

User participation in IS security was examined in the context of organizational compliance with the Sarbanes-Oxley Act of 2002 (hereafter referred to as SOX) because of the regulation's relevance to both IS security and business processes. SOX attempts to ensure the integrity of publicly reported financial statements by requiring companies to demonstrate internal control over financial reporting (ICOFR), defined as an organization's process for providing reasonable assurance regarding the reliability of their financial reporting (PCAOB 2004, p. 153). In other words, SOX is focused on the integrity objective of IS security by requiring organizations to implement internal controls that effectively protect financial information from computer crimes, employee mistakes, and other security threats and vulnerabilities that could lead to unreliable financial statements. SOX attempts to achieve ICOFR by holding company executives personally liable (accountable) and by requiring an annual external audit of a company's internal controls.

SOX was chosen for the study context as a means to locate an adequate sized sample of companies employing user participation in SRM. SOX likely encourages business participation in SRM for at least two reasons. First, ICOFR is focused on business processes that significantly impact financial information on publicly reported statements. In making company executives, typically the CEO and CFO, accountable for ICOFR, SOX encourages user participation in IS security. Business managers must "sign-off" on the adequacy of their controls as documented evidence of SOX compliance. Senior managers are likely to delegate some of this responsibility to their staff and, as such, business users are likely to participate in the process. Second, while IS security has traditionally focused on external threats, such as hackers and viruses, managing the risk of fraud requires a focus on internal threats, such as employee computer crimes. In other words, technical controls geared toward protecting the network perimeter from external threats are insufficient to manage internal threats and vulnerabilities embedded within business processes. When IS security shifts from a network perimeter to a business process focus, business people are likely to participate since they perform business processes as part of their daily jobs. As a result, focusing on internal threats to IS security is likely to attract broader business participation in SRM.

An Exploratory Study of User Participation in IS Security

An exploratory study was conducted to better understand the specific activities, behaviors, and assignments that constitute user participation in SRM and to investigate their outcomes. A contextual narrative of user participation lays a foundation for a subsequent examination of the effects of participation studied through the lens of three extant user participation theories.

Data Collection

To conduct the exploratory study, informants with SOX experience were first identified at a one-day symposium on information assurance and SOX compliance that was sponsored by the accounting department of a university located in the midwestern United States. Informants were selected because they worked on SOX compliance efforts at their respective companies.

Nine semi-structured interviews were conducted with eleven informants from five companies in three industries; two interviews included two informants. This convenience sample included three informants (senior risk officer, risk manager, and deputy chief information security officer) at a large national bank; two informants (internal audit and IS managers) at one manufacturing firm; three informants (financial comptroller, internal audit director, and IS director) at a second manufacturing firm; one informant (internal audit manager) at a third manufacturing firm; two informants (managers of accounting and internal audit) at a utility firm.

Each interview lasted approximately 90 minutes and was recorded. Informants were told the purpose of the study was to gain a better understanding of the process and outcomes associated with business users' participation in IS security projects, and that SOX compliance was considered to be such a project (Spears and Cole 2006). They were asked to recount the roles and activities employed by their respective companies as part of SOX compliance efforts, along with associated outcomes. Appendix B provides a summary of the interview guide (the complete version can be found in Spears 2007).

Analysis

In qualitative data analysis, classification and connection form the basis of theory development (Urquhart 2001). As such, qualitative data were analyzed by classifying chunks of transcribed text into meaningful codes (i.e., keywords), which were then causally connected (Miles and Huberman 1994, pp. 56-71). An iterative process of three coding techniques was applied to transcribed text (Urquhart 2001). First, selective (or theory-driven) coding was used to develop an initial code list that contained user participation, awareness, and security controls. Next, open-ended coding was used to identify new codes as they emerged from interview transcripts. Finally, axial coding was used to identify relationships among existing code categories.

As informants described the process their companies went through to become SOX compliant, they were asked what roles participated in various activities. In many cases, governance roles (e.g., internal and external auditors) and consultants were the primary actors participating in an activity. In cases where business users participated in a particular activity, informants were asked if there were any notable outcomes from that participation. These semi-structured interviews enabled informants to describe activities and outcomes that were most salient in their organizations.

Once the data had been collected, segments of interview transcripts were coded as user participation when informants reported users performing a particular task. These coded segments were subsequently grouped and assigned new codes that categorized the activities in which users participated. Relationships among codes were then analyzed.

Results of the Exploratory Study

Informants described roles and activities for SOX compliance as an SRM process. Informants described user participation in terms of who participated, the activities that users performed within the SRM process, the types of controls that users worked on, and the roles and responsibilities they were assigned in an effort to establish formal accountability. Each of these aspects is described below, providing contextual detail of user participation in SRM for regulatory compliance.

Security Risk Management in Business Processes and How Users Participated

Users referenced in the study were organizational members from the functional areas of business, from non-managers through the ranks of senior management. Informants consistently reported that users were designated by their superiors to participate because SOX-relevant business processes were part of their day-to-day jobs. SOX compliance efforts focused on business processes whose output had a material (significant) effect on numbers reported in financial statements. After business processes relevant to SOX had been identified by internal auditors, risk managers, or external consultants, users reportedly participated in the SRM activities listed in Table 1 and described next.

Informants across companies consistently indicated that users participated in documenting business processes to determine information use throughout a business process. This information was then used to determine where risks to the integrity of financial information may existed within a business process. Informants at all five companies described a risk-to-control matrix that was created to match existing controls to each identified risk in order to ensure that needed controls exist. Although internal auditors, risk managers, and external consultants led the effort to assess risk and controls, users typically provided input based on their in-depth knowledge of a given business process.

New controls were created in cases where no control existed for a particular risk, or where an existing control was consid-

Table 1. Three Categories of User Participation in IS Security

User Participation in Security Risk Management Activities	# of Orgns	User Participation in Security Controls	# of Orgns	User Participation via Accountability	# of Orgns
Business process workflow	5	Access control	5	Roles and responsibilities documented	5
Risk-control identification	3	Segregation of duties	5	Roles and responsibilities assigned	5
Control design	5	Alerts and triggers	1	Control owners designated	5
Control implementation	5	Exception reports	1	Senior management review	2
Control testing	2	End-user computing	1	iSecurity policy committee	2
Control remediation	2	Training	3	Executive business support demonstrated	3
Communication	3	Risk tolerance	2	IT-user committees used	4

ered to be too weak to mitigate a particular risk. Users were reported to have provided decision criteria or a reality check as input into control designs. They also actively participated in implementing controls, since internal controls were typically integrated into business processes. Next, controls were tested to ensure they functioned as designed. In cases where a control failed its test, a remediation plan was documented to specify how the failed control would be corrected. Failed controls were then retested according to the remediation plan. At multiple companies, users were reported to be responsible for developing remediation plans for failed controls—in other words, determining how and when a control would be corrected. Control testing would also trigger new design activity if it was determined that the control was ineffective. Although auditors conducted formal audits of controls, users were reported to review and test controls, in some cases to ensure readiness for an audit. Finally, users communicated relevant company policies and procedures to peers and staff.

As part of the SRM process, users participated in the identification, design, implementation, testing, and remediation of relevant security controls within their business processes. As such, it is useful to note the types of security controls in which user participation was particularly relevant. Across companies, the security controls most often associated with user participation were segregation of duties (i.e., controls designed to avoid a conflict of interest in the rights assigned to system users that could lead to a security breach) and access control. As listed in Table 1, users were also reported to participate in other controls, such as defining risk tolerance as part of an organizational security policy; enacting exception reports and alerts to flag potential problems in ERP systems; validating calculations and establishing password protection in financial spreadsheets (i.e., end-user computing); and training on required SRM activities.

Finally, user participation was described in terms of newly created and revised roles that had specific security objectives, a clear trend observed in all five companies. In other words, user participation was found to be formalized and appeared to be centered on accountability for protecting financial information. Informants used the term accountability in two related ways: (1) formally assigned responsibility, and (2) organizational expectation that a person in a particular role will be informed of and follow policy. For example, informants at all five companies noted new user roles for managing access control, or more broadly, identity management. New roles were created, such as data custodian, data steward, access control specialist, data owner, and control owner. All five companies had created the role of process owner, described as a business (or IS) person responsible for controls within his or her assigned business (or IS) process. As these titles suggest, the new roles that informants recounted were consistently associated with user accountability for tasks aimed at protecting financial information. Depending on the company, roles were assigned at various staff and management levels. In some cases, user participation in SRM was functional (e.g., approving routine access control), while in other cases, user participation was more strategic in nature (e.g., steering committees).

Consistency of User Participation Activities and Assignments across Five Companies

This qualitative analysis spanned across five companies. In an effort to examine the consistency of our findings (Miles

and Huberman 1994) across companies and to limit the impact of common interview pitfalls (Myers and Newman 2007) that could occur within a single company, we counted the number of companies where an informant mentioned users participating in SRM activities and controls, and being held accountable in an IS security context. The results are presented in Table 1 and convey aspects of user participation that were most common across companies. That is, while informants at all five companies described all seven SRM activities listed in Table 1, their accounts varied on which activities included user participation. Thus, Table 1 is focused on the activities, controls, and accountability in which users were said to have participated. User participation was most commonly found in documenting business processes during risk assessments, providing input into control design and implementation, working on access control and segregation of duties, assuming formal roles, and serving on committees.

Outcomes of User Participation in SRM

With a greater understanding of how users participated in SRM within business processes for SOX compliance, this section examines the effects of that participation by applying each of the three theories of participation suggested by Markus and Mao (2004). Research hypotheses are formulated from this analysis, leading to the research model tested in the confirmatory study.

The Buy-In Theory

The buy-in theory of user participation in ISD contexts associates user acceptance with users' psychological involvement that develops during their participation (Markus and Mao 2004). In other words, as users participate in ISD activities, they begin to view the focal system as personally important and relevant, and are therefore likely to be more accepting of the system than they would otherwise be had they not participated.

Support was found for the buy-in theory in SRM contexts within a regulatory compliance environment. That is, as users participated in SRM for regulatory compliance, IS security became more relevant to their respective business processes. However, at an organizational level of analysis, informants emphasized cognitive outcomes associated with user participation, in contrast to the affective outcomes typically emphasized in ISD studies. Only one informant, an accounting manager, discussed a sense of pride that his staff of accountants had developed via their participation. In contrast, there was widespread consensus within and across organizations that as users participated in SRM for regulatory compliance, organizational awareness of security risks and controls increased, and security controls were aligned with the business context. These outcomes are described next.

Organizational Awareness of SRM. Informants consistently indicated that as users participated in SRM activities and security controls, or were held accountable for some aspect of SRM, organizational awareness of SRM in financial reporting increased. For example, Nelson,[3] a senior IS manager at a manufacturing company, recounted that users participated in SRM by performing an access control review and reaching consensus with IS professionals on user-defined access control rules. Accordingly, both users and IS gained greater awareness of IS security risks and needed controls in system access.

> So I would say it made both [users and IS] more aware of what people have access to out there....I think it definitely made us more aware of some of the risks that are out there and what we need to do to remediate them.

Given the recurring theme across companies of increased awareness as an outcome of user participation, informants were asked how awareness was demonstrated. Mark, an internal audit manager at a manufacturing company, described awareness as a greater consciousness of organizational expectations to perform designated security controls. Users demonstrated awareness by asking questions and proactively performing their security responsibilities.

> I think there is more of a consciousness about it.... we ask more questions of them and we can tell, based on that, they are thinking about this stuff. They are actively involved. [For example,] the quarterly or periodic access reviews, the business users are directly involved in the process and they are getting lists of whoever has access to whatever systems they are responsible for, and they are reviewing that. So it's really a part of... it's what is expected; it's certainly an expectation. They are supposed to be on top of this stuff. They should know who has access to their systems. They should be critically reviewing these IS user requests to see should we really be granting this person access. And I can tell based on I guess some of the requests I've seen: "Normally someone in that position

[3]The names of informants have been changed to ensure their anonymity.

> would typically grant access to someone in this position, [but] do they really need it?" So you can tell they are putting some thought into it.

Similarly, Kelly, the director of Internal Audit at another manufacturing firm, suggested that as users participated, they gained greater awareness of security vulnerabilities associated with the availability of information. Awareness was reflected in users demonstrating more vigilance toward sensitive information.

> People have a heightened awareness of the availability of information, internally really, and I guess externally too. [Sensitive information is] more available than they would have expected. So we see people coming back and bringing up things that maybe they wouldn't have done before.

Informants from all five organizations consistently reported that user participation led to increased awareness of IS security risk and organizational controls to manage those risks. In other words, as users performed SRM activities, worked on specific controls, and were assigned various responsibilities, they became more aware of IS security risks in their respective business processes and the organizational controls for mitigating those risks. This finding is further examined in the confirmatory study by testing the hypothesis

> **H1**: User participation in SRM raises organizational awareness of IS security risks and controls.

Business-Aligned IS Security Risk Management. Informants' accounts suggested that users provided important contextual information that enabled SRM to be based on business objectives, values, or needs as opposed to being primarily based on technology or uninformed assumptions of the IS department. For the purposes of this study, SRM that is based on business objectives, values, or needs is characterized as being business-aligned, as opposed to being technology asset focused. Intuitively, security controls within business processes that are aimed at protecting financial information will be more effective if they are oriented toward the local business context. Consequently, risk managers and internal auditors sought business knowledge from users when assessing risk and designing controls embedded in business processes.

In one example, a deputy chief information security officer (CISO) at a national bank described user participation as a means to better align SRM with the local business context. In other words, user participation provides a business perspective of the information flow and usage within business processes so that security risks can be more effectively managed.

> One of the biggest values that end users provide as input into my [security] program is I don't understand the business like they do, so I don't understand the information. I don't understand the relative importance of the information. I don't understand the context of the information in the way people do their daily business, so I don't know what forms people need the information in, how readily accessible it needs to be, how it flows through the business processes, and therefore where the critical junctures are that need to be controlled.

Informants across organizations consistently reported that a key area where users provided needed business knowledge was in documenting business process workflows. This activity is essentially documenting the security risk environment, and is the first step in assessing risk to financial information and identifying where controls are needed in order to manage those risks. In some organizations, users wrote the narratives describing details of the process workflow, while in others, they worked in partnership with internal auditors, risk managers, or consultants to complete the documentation. For example, Betsy, a risk manager at a bank, recalled her interaction with users to document business processes as part of a risk assessment:

> [Betsy speaking to users:] "Here's what I want you to tell me. Here's what I consider are your risks. What do you think? Based upon what you do everyday, is that an accurate assessment?" So there was some learning in that aspect when you had to go down and actually start documenting all the processes with the person who is performing the function who doesn't even think he is managing risk to understand and to help you document what's going on and what a risk is or what their risks are.

Betsy's account implies that user participation provided needed contextual detail of a given business process that enabled her, as a risk manager, to better understand security risk within that business process so that those risks could be appropriately managed. In other words, user participation facilitated alignment of security risk management with the business environment, suggesting the hypothesis

> **H2**: User participation contributes to an alignment between SRM and the business context.

The effects of user participation on awareness appeared to be, in part, channeled through greater alignment of SRM with the business context. In other words, as SRM policies and procedures gained alignment with the business environment,

organizational awareness increased of security risks and controls for financial information systems. Informants suggested that by making SRM a part of business processes, organizational awareness increased in what the security risks were, if or why those risks should be managed, and how those risks could be managed. For example, Dean, an IS director, was asked what was the biggest benefit to having users participate in SRM. He suggested that organizational awareness increases when SRM becomes integrated into (i.e., aligned with) business processes because SRM has greater visibility within the organization and users are more vigilant.

> Self policing. Again, a corporation sets policy. We implement policy. IT puts the technology on it, but the visibility of security across the organization is a lot better than just having a security department in IT. It becomes part of business, I think would be the way to put it. You've got to make security part of business.

SRM policies and procedures that were integrated with business objectives solicited greater attention to IS security risks, policies, and procedures in business processes for financial reporting, as an internal auditor described:

> I would say the key benefit is that you have process owners, and the people who work for them, they have much more attention on and understanding of their internal controls, why they're important, and how they affect the financial statements at the end of the day.

Hence, these findings suggest the hypothesis

> **H3**: Business-aligned SRM contributes to greater organizational awareness of IS security.

In summary, the buy-in theory of user participation, shown in Figure 1, was supported in an SRM regulatory compliance context. In contrast to ISD literature at an individual level of analysis that has largely focused on user acceptance as an outcome, the present study found that user participation's effect was primarily cognitive; user participation raised organizational awareness of IS security risks and controls in business processes, particularly when SRM was aligned with business objectives.

The System Quality Theory

The system quality theory of user participation associates improvements in system development with needed information that is gained from user participation. Support was found for the system quality theory in SRM within a regulatory compliance environment. Moreover, the system quality theory was found to be an extension of the buy-in theory discussed above. That is, user participation encouraged business alignment in SRM and raised organizational awareness; the outcome appeared to be improvements in control development (i.e., the design and implementation of IS security controls) and control performance (i.e., greater efficiency and reduced deficiencies in the system of IS security controls), as discussed next.

Control Development. Knowledge derived from user participation on the business use of information was taken into account by security control designers. Depending on the company, control designers included internal auditors, risk managers, and external consultants. From a risk manager's or an auditor's perspective, informants described two components of a control: its design and performance. The design of a control is assessed to determine if it is appropriate to mitigate a particular security risk. The performance of a control is assessed to determine if it is functioning as designed. User participation in SRM contributed to control development in two ways.

First, user participation contributed to improvements in control development by providing needed information to control designers. For example, one informant described the valuable feedback that users provided on whether or not the controls designed by internal auditors "made sense" and could feasibly be performed in the day-to-day business environment. Based on this feedback, controls were modified as needed. Dorothy, a comptroller, explained,

> As we documented the processes and identified controls, and maybe found an area where we needed to add a control, we had to go back to the [business] process owner. We had to understand more of what they were doing. And we had to work with them to identify the appropriate controls to put in place. We didn't just go and slam a new control in without them having any say. We had to make sure that it was something that they could live with, that they could perform on a regular basis, and that it made sense for the process we were adding it to. So yes, they were decision makers from that standpoint.

In another example, Bob, an accounting manager at a utility company, was asked if any manual controls had been implemented that reduced security risk. He discussed protecting the integrity of financial information by simplifying information flow. Unnecessary steps in the business process were eliminated.

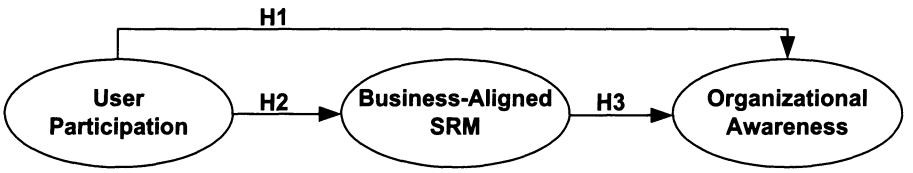

Figure 1. The Buy-In Theory of User Participation in SRM Contexts

> It's more data integrity....in some instances actually by eliminating steps helped to improve control because there were areas where we saw—especially on paper it helps to see the flow charts—this business unit is providing this data out to this business unit who then is doing this step with it and then providing it to us. That seems like an unnecessary handoff. So what is that adding? It's not adding any value.

As Bob suggested, simplifying information flow increases the control of information, and therefore its security. For example, the fewer nodes in a data flow, the fewer points of intersection that must be secured in order to protect that information. User participation aided control development by documenting and simplifying information exchange in business processes. User participation provided needed information that enabled improvements in control design and implementation. This finding suggests

> **H4**: User participation contributes to perceived improvements in control development.

Secondly, the contribution of user participation to organizational awareness was also found to affect control development. For example, Tim, a senior vice president of Risk Management at a national bank, recounted user participation in documenting the decision criteria used to provide system access. His account implies that users gained greater awareness (i.e., consciousness) of why someone should get system access. In turn, this awareness enabled control designers to implement the control more consistently based on documented criteria. Thus, control development improved.

> One of the biggest things that we saw not only in SOX, but also in application access control, we needed to design a process that allowed us to define decision criteria as to whether we would or would not give someone access to a certain application. ... The individuals who have the responsibility to approve the access at the application level...have that knowledge because they have been doing it on a day-to-day basis. They have been with the bank for 25 years. "I just know they require that access." "How do you know?" "Because I've been here for 25 years." "No, how do you know? What is that process, that decision criterion, that's going on in your head for you to come to that conclusion because if you get hit by a bus we need someone else to step in and perform this control no different than you have." We now need that documentation in place.

Similarly, an IS manager at a manufacturing company implied that control testing as part of SRM for SOX compliance raised organizational awareness, which in turn, resulted in more consistent implementation of access control. That is, greater awareness of a control to validate system access resulted in more consistent implementation of the control.

> [Prior to SOX,] the company had that IS user request. We had to get their proper approval for them to get access, and the approval comes from the business, not IS; all we do is add the user. So we were doing some of that already. I guess the biggest thing [with SOX] is that we had to go back and do another review two to four times a year to ensure that people did have the right amount of access. It made [users] more aware of who has access to their systems and is it valid, which we weren't doing before.

Indeed, the IS security literature suggests that the purpose of security awareness (and training) is to "modify employee behavior so that the individual performs according to organizational standards" (Whitman 2008, p. 141). This observation suggests that control implementation improves when there is greater awareness of IS security controls.

> **H5**: Organizational awareness of SRM within a business process contributes to perceived improvements in control development for controls within that business process.

Control Performance. Control performance was said to have improved in that informants reported a reduction in the

number or significance of control errors (i.e., deficiencies) and an increase in efficiency across the system of controls in place to protect financial information from security risks. For example, Nelson, an IS manager at a manufacturing firm, described increased efficiency in the system of controls via greater balance in the number of controls and the level of detail or constraint posed by the controls. His account implies that organizational awareness of security risks and controls needed for SOX compliance enabled the firm to improve efficiency in the system of controls.

> It's just ensuring that we are doing the proper level [of controls] and then understanding enough to constantly automate it. I think between the first year and this year [of SOX compliance], we've gotten a lot better in just the amount of time it takes to do this stuff.

In another example, Mark, an internal auditor suggested that the "mentality" (i.e., awareness) that control deficiencies were being monitored may have encouraged the company's plant controllers to better manage control deficiencies.

> Our control requires the plant controllers to report how many deficiencies they have, whether they are outstanding or not, whether they fixed them. That is all new with SOX, because now, getting a deficiency from an internal auditor and a fine from internal audit I think has a higher level of significance now than...before. So it kind of creates a little bit of that mentality.

H6: Organizational awareness of SRM within a business process positively influences the perceived performance of security controls.

Mark's account also suggests that user participation may directly affect control performance. In other words, users were required to remediate control deficiencies as part of their SRM activities. User participation in control test remediation encourages a reduction in control deficiencies by holding users responsible for specific controls.

In some cases, user participation was found to improve control performance, not necessarily because of users' knowledge, but because users were being held accountable to perform assigned security tasks. This finding is particularly relevant to a compliance context. For example, a SOX manager at a manufacturing company was asked if SOX compliance efforts had been useful in her organization.

> **Susan**: You know what, it has and I hate to say it because people hate it so much.
>
> **Researcher**: ....Why do they hate it?
>
> **Susan**: Because they think it's so much bureaucracy. They have to sign for everything. They have to keep things that maybe they didn't used to keep. They are being held accountable for a lot more things than they used to be.
>
> **Researcher**: These are the process owners?
>
> **Susan**: Yes. If they are required to review and approve every purchase order over $100,000, they better do it because it's going to be tested and the ones that they don't do might be...and then they have to explain why they didn't do it and how they're gonna fix it. Where before [in the past], that might have been, "That's what we're going to do." It wasn't written down anywhere. Nobody ever checked to see that's what they were doing. And now they are really held accountable for all these things.

Susan's account suggests that business users were held accountable to perform assigned controls. Control performance improved because controls were more closely monitored. In cases where controls were not performed as designed, users had to document a remediation plan outlining how they would correct control performance. These accounts suggest that user participation directly contributed to control performance. Hence,

H7: User participation positively influences the performance of security controls.

Finally, better designed and implemented controls should result in better control performance from fewer errors or increased efficiency in the system of controls. Hence,

H8: Improvements in control development positively influences the performance of security controls.

In summary, informant accounts supported the system quality theory of user participation. When users participated in SRM, organizational awareness of security risks and controls in business processes increased, resulting in perceived improvements in control development and performance. Again, the effect of user participation in SRM was found to be primarily cognitive. The hypothesized relationships of the system quality theory in SRM are shown in Figure 2.

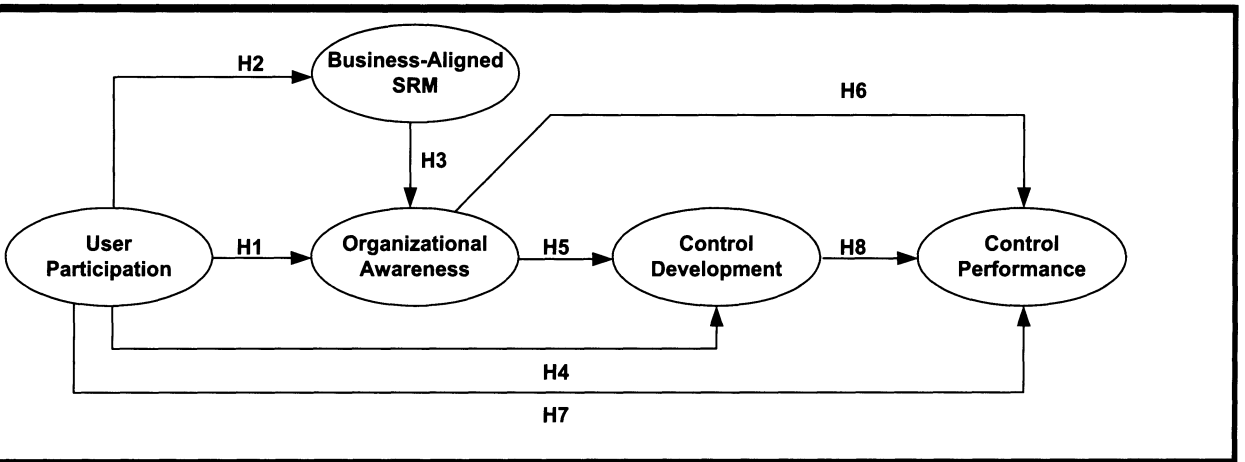

Figure 2. A Research Model of User Participation in SRM

The Emergent Interactions Theory

The emergent interactions theory of user participation associates outcomes with relationships that develop between users and IS personnel when users participate. In general, good relationships between users and IS are expected to yield good outcomes (e.g., higher quality controls), while bad relationships are expected to yield bad outcomes (Markus and Mao 2004).

While evidence of emergent interactions in SRM was found, the resulting relationships did not appear to affect outcomes. There was evidence of emergent interactions; that is, new, or in some cases stronger, interactions between users and IS personnel had been recently formed to manage IS security at all five companies. Informants described the value of user and IS staff interactions in SRM. However, outcomes were not attributed to good or bad relationships between users and IS personnel.

Emergent interactions between users and IS were reported at the staff level on access control and at the senior management level on strategic security issues, such as data classification (e.g., public, proprietary, or restricted) and risk tolerance. For example, at one manufacturing firm, a security council of senior business and IS managers had formed during the previous two months to classify information and to develop global policies on protecting intellectual property. These policies essentially defined elements of a security policy. The council had weekly meetings. When asked if there were any obstacles that occur in such a council, the IS director anticipated future disagreements when the council begins to coordinate how strict or lenient system access should be across organizational units.

In a second example of emergent interactions between senior management, new alliances had recently been developed between senior-level IS and business management at a large national bank for the purpose of reaching an agreement on the appropriate level of protection for business information. Leslie, the deputy CISO, explained,

> So these two people way up here are making sure they're in sync of "Are you protecting my information?" "Yes, I'm protecting your information. Here's how I'm doing it. Here's what's not protected. Are you okay with that?" "Yes, I'm okay with that."

In both companies, these senior partnerships were newly formed. While informants noted value in that at least senior managers were now talking about data protection, they did not note positive or negative relationships. Instead, outcomes were associated with better alignment of SRM with business objectives, greater organizational awareness of security risks and controls within business processes, and better design, implementation and performance of security controls. Thus, evidence of emergent interactions in SRM within a regulatory compliance context equated to the system quality theory, as shown in Figure 2.

A Confirmatory Study of User Participation in IS Security

The research model of Figure 2 depicts the influence of user participation in IS security contexts at an organizational level of analysis. The model was developed to test the validity of the hypotheses that emerged from the exploratory study and

to provide triangulation of results from the exploratory study (Lee 1991; Mingers 2001).

Measures

The survey items used to measure the research model variables were primarily derived from the qualitative study and are listed in Appendix C (the complete questionnaire can be found in Spears 2007). All five model constructs were latent variables that were measured with two or more indicators, described next.

User participation. Three items were used as formative (i.e., causal) indicators of user participation in SRM for SOX compliance. Each indicator was an index of seven activities derived from the exploratory study and the IS security literature. User participation in the SRM process (UP_{srmp}) assessed the comprehensiveness of the SRM process activities performed by users. User participation in IS security controls (UP_{ctrls}) assessed the comprehensiveness of the types of controls relevant to business users in a SOX context and in which they participated. Both the SRM process and security controls were based on informants' accounts. Finally, user participation via accountability (UP_{acct}) is an index of activities that security standards recommend to establish accountability (Alberts and Dorofee 2003; ISO/IEC 2000; ITGI 2005). For each index, a score of 1 or 0 was assigned to each activity, depending on whether the respondent answered that users in his or her organization did or did not participate in the activity, resulting in an index score that ranged from 0 to 7. As the three indices constitute user participation in IS security, they were modeled as formative indicators (Jarvis et al. 2003).

Organizational awareness. Consistent with informants' accounts during the qualitative study, IS security literature has associated awareness with a raised consciousness (Dinev and Hu 2007) and an enhanced adoption of security policies and countermeasures (Tsohou et al. 2008). Thus, organizational awareness refers to different target groups (e.g., end users, IS professionals, senior management, third parties, etc.; Siponen 2001) that exhibit a consciousness about organizational policies, procedures, or the need to protect sensitive information. In this sense, organizational awareness is conceptualized as a state that is reflected in the behavior of target groups, such as employees working with financial information. As such, organizational awareness was assessed with two reflective items on seven-point Likert scales: (1) heightened awareness of policies, procedures, or the need for IS security, and (2) the extent to which users exhibited a sense of ownership (i.e., proactiveness) in protecting financial information.

Business-aligned SRM. There is a growing school of thought in IS security literature that SRM can only be effective if it is in alignment with organizational objectives, business requirements, and relative business value (e.g., Halliday et al. 1996; Spears 2005; Suh and Han 2003) so that the business impact of security incidents is minimized (ITGI 2005, p. 119) and IT professionals can build a better business case for the need to invest in security (Kokolakis et al. 2000; Mattord and Want 2008). Therefore, business-aligned SRM was measured via two reflective items: (1) the extent to which security policies and controls are based on business objectives, value, or needs, and (2) the extent to which business users routinely contribute a business perspective to IT on managing security risk. Both items were measured via seven-point Likert scales.

Control development. As internal auditors and risk managers recounted in the qualitative study, controls are evaluated based on their design and performance. In the context of SOX compliance, a control must be implemented for two months before its performance can be audited. Thus, for the purposes of this research, control development refers to the design and implementation of IS security controls. Control development was assessed via three 7-point scales as perceived improvements that had occurred in the definition or implementation of access control, segregation of duties, and security policy. These three controls were most commonly associated with user participation in IS security within business processes. Security policy contains rules of acceptable and unacceptable behavior, serving as organizational law (Whitman 2008) and was associated with senior business management's participation in defining organizational policies, such as risk tolerance and data classification. As these items were expected to have the same causal antecedents, they were modeled as reflective indicators (Jarvis et al. 2003).

Control performance. Informants during the qualitative study associated improved security with improvements in the system of controls in place to manage security risk to financial information systems. Given the routine audits required for SOX compliance, and perhaps compliance with other regulations and standards, auditors, and business and IS process owners paid attention to (1) audit results and (2) resources expended to maintain the current system of controls. In other words, informants consistently indicated, both directly and indirectly, that the organizational goals were to be SOX compliant as efficiently as possible. Internal auditors documented deficiencies found in key (i.e., high-priority) controls for SOX. A remediation plan had to be documented and executed. The cumulative total of all outstanding control deficiencies had to be estimated prior to the external audit. There was a financial incentive to getting fewer and/or less costly deficiencies, from a resources-expended perspective. Informants also described automating

identity management controls in order to have fewer control deficiencies and reduce resources expended on maintaining security controls. Therefore, the performance of security controls was measured via two reflective seven-point items as the extent to which (1) deficiencies (i.e., gaps in a control's design or errors in its execution) and (2) efficiencies (e.g., through automation or fewer steps) had improved in an organization's system of controls for financial IS.

Data Collection

Content validity. An effort was made to ensure the survey items were clearly understood by the respondents and that they responded to questions that the researchers intended to ask. First, survey items contained language used by informants in the qualitative study. Second, anchor descriptors were added to item scales to clarify the meaning of items. Finally, the survey instrument was pretested at an industry symposium with 16 respondents. The pretest resulted in some items being added, deleted, or revised.

Survey study. To test the research model, data were collected from organizations that complied with SOX. While U.S.-based respondents were targeted, a cross-representation of industries and company sizes were sought. The targeted respondents were experienced IS managers and senior staff knowledgeable of SOX compliance efforts in their respective companies and, therefore, knowledgeable of the procedures and people involved in compliance activities. As such, they were well positioned to provide reliable assessments of the study variables which were at the organizational level. Thus, the sample frame consisted of members of U.S. chapters of the Information Systems and Audit Control Association (ISACA), a practitioner association specializing in IT governance, audit, and security and affiliated with the COBIT framework (ITGI 2004, 2005) that is widely used for IT compliance with SOX.

An ISACA staff member was asked to send an e-mail to individual members, asking them to participate in an on-line survey by clicking on a link to the survey. The invitation was e-mailed to 14,000 members; 336 eligible members responded, resulting in 228 usable questionnaires.

The sample included respondents who were knowledgeable of their organization's SOX compliance and assumed one or more roles as IT auditor (54.5%), IS security manager (30.4%), SOX process owner (20.2%), or "other" IT professional (17.6%). Of those responding, 45 percent percent of respondents were managers; 23 percent were directors; 15 percent were senior analysts; 8 percent were consultants responding for a single firm; 7 percent were executives; 2 percent were junior analysts. Commercial firms comprised 91 percent of the sample: 74.3 percent were publicly traded and 16.5 percent were privately held. The remaining 9 percent of respondents worked for government (4.0%) and nonprofit (5.2%) organizations. The two largest industry groups in the sample were financial services at 21.8 percent and manufacturing at 12.1 percent, suggesting that no one industry dominated the sample. Sampled organizations had annual revenues ranging from less than $10 million to over $10 billion, with the largest representation over $10 billion (28.1%), $1 billion–$5 billion (25.0%), and $500 million–$1 billion (15.1%). Thus, the sample contains over 14 industries, a variety of organizational sizes based on revenue, and a variety of respondent roles and management levels, and is, therefore, thought to provide a reasonably adequate representation of the target population.

Analysis

Partial least squares (PLS) is an approach that has minimal distributional requirements of the data and allows latent constructs to be modeled either as formative or reflective indicators (Chin 1998). As the research model incorporated both formative and reflective constructs and the distribution of some of the items was non-normal, the research model of Figure 2 was analyzed using PLS-Graph Version 3.00.

Descriptive statistics of the sample and the correlation matrix for all indicator variables are provided in Table 2 and Appendix D, respectively. The correlation matrix for all constructs, and the composite reliabilities of reflective constructs along with their AVEs (average variance extracted) are provided in Table 3. The composite reliabilities of organizational awareness, business-aligned SRM, control development, and control performance were .85, .83, .87 and .80, thus supporting reliability. The AVEs of the four constructs were greater than the inter-construct correlations (.74, .71, .69, and .66, respectively), supporting convergent and discriminant validity. The weights of the three formative user participation index scores (UP_{srmp}, UP_{ctrls}, and UP_{acct}) were .35, .45, and .49, respectively (all p-values < .001).[4]

[4]Interestingly, modeling the indices UP_{srmp}, UP_{ctrls}, and UP_{acct} as reflective indicators of user participation yielded construct loadings of .79, .77, and .79, respectively, a composite reliability of .83 and AVE of .62, providing evidence of reliability, and convergent and discriminant validity. However, the UP_{srmp}, UP_{ctrls}, and UP_{acct} indices are conceptually more appropriate as formative indicators of user participation and were kept as such in the analysis. The correlations between the three indices were UP_{srmp} with UP_{ctrls} = .43; UP_{srmp} with UP_{acct} = .48; UP_{ctrls} with UP_{srmp} = .41.

Table 2. Sample Descriptive Statistics

Indicator	N	Mean	Std. Dev.	Min.	Max.
User participation (in SRM process)	228	4.92	1.82	1	7
User participation (in controls)	228	3.63	1.78	1	7
User participation (via accountability)	213	4.31	2.01	1	7
Awareness of IS security	227	5.60	1.32	1	7
User ownership of IS security	224	4.99	1.42	1	7
User business perspective	228	4.31	1.62	1	7
Business-based IS security strategy	228	4.74	1.79	1	7
Control development (access control)	228	5.52	1.17	1	7
Control development (segregation of duties)	227	5.40	1.12	1	7
Control development (security policy)	228	5.35	1.19	1	7
Deficiency reduction	224	5.58	1.41	1	7
Efficiency improvement	227	5.37	1.07	1	7

Table 3. Correlations between Latent Constructs

	User participation	Organizational Awareness	Business-aligned SRM	Control development	Control performance
User participation	N/A				
Organizational awareness	.49***	.85 (.74)			
Business-aligned SRM	.49***	.46***	.83 (.71)		
Control development	.40***	.37***	.25***	.87 (.69)	
Control performance	.46***	.48***	.35***	.49***	.80 (.66)

***p < .001. Values in the diagonal indicate composite reliability and (AVE). N/A = not applicable.

Figure 3 depicts the path coefficients, construct indicator loadings (weights in the case of User Participation), and the proportion of explained variance in each construct. Bootstrapping with 100 samples was used to calculate the t-values of path coefficients. As can be seen in Figure 3, the eight hypothesized links of the research model were significant at $p < .001$. User participation, organizational awareness, and control development explained 38 percent of the variance in control performance. In turn, user participation, organizational awareness and business-aligned SRM explained 20 percent of the variance in control development. User participation and business-aligned SRM explained 30 percent of the variance in organizational awareness, and user participation explained 24 percent of the variance in business-aligned SRM.[5] Overall, these results support the study's research model, and therefore both the buy-in and system quality theories of user participation in SRM compliance contexts.

Discussion

The present paper examined user participation in terms of the types of SRM activities users performed, the types of controls they worked on, and the extent to which accountability had been established in managing IS security. User participation in SRM was found to raise organizational awareness of security risks and controls within targeted business processes, and facilitated greater alignment of SRM with business objectives, values, and needs. As a result, development and performance of security controls improved. Thus, user participation was found to add value to an organization's SRM.

[5] As a check, the research model was also analyzed with the indicators of both control development and control performance modeled formatively. For the three formative constructs, all indicator weights were significant at $p < .01$ or better, except one (access control item of control development). Four of the eight path coefficients remained the same, while the magnitude of the change in the other coefficients was less than .02. Moreover, all four r-squares remained the same. Thus, the results were very similar to those reported for the reflective model of Figure 3, and suggest that the paths and explanatory power of the research model were largely unaffected by the formative or reflective conceptualization of the study measures.

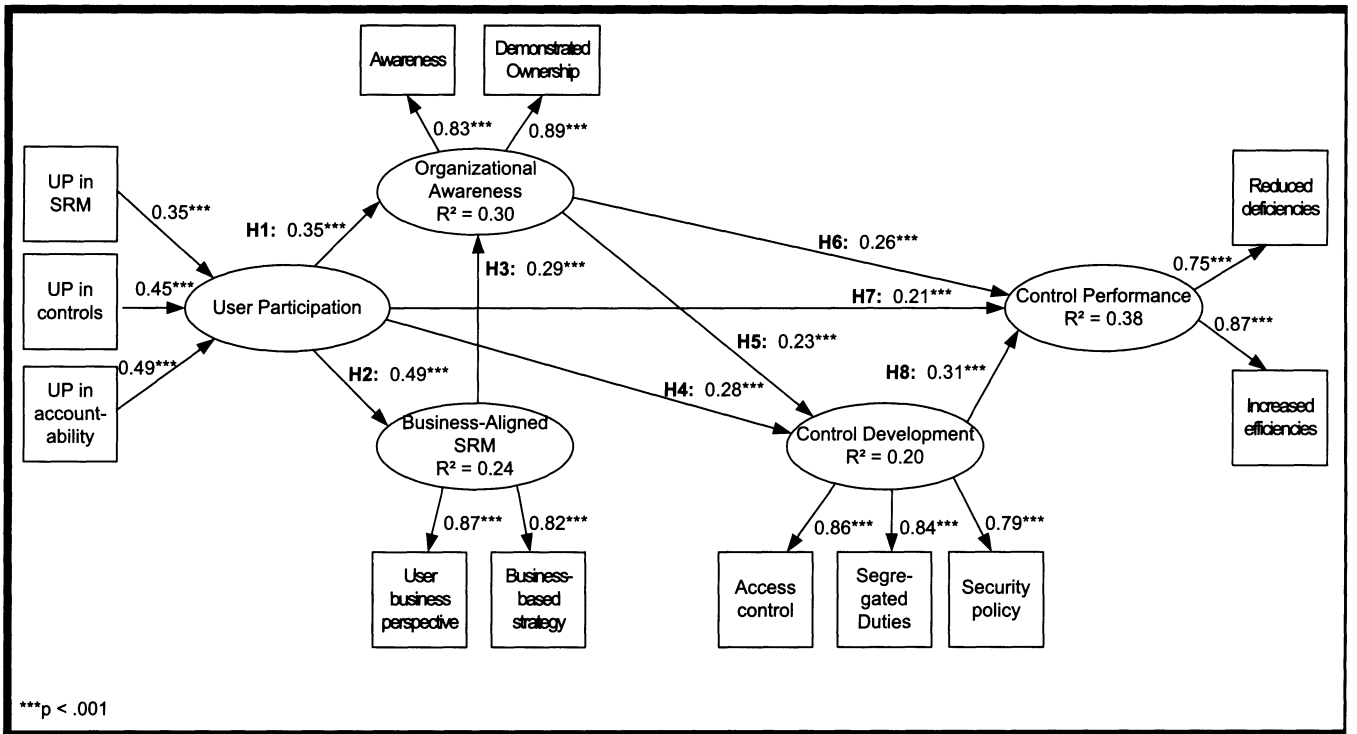

Figure 3. Results of Research Model Testing

User participation's effect was strongest in aligning SRM with the business context. In turn, users became more attentive (i.e., aware) as business-alignment increased. This finding suggests that users are likely to be more attentive when IS security is something to which they can relate. That is, when SRM becomes part of business processes, and users are assigned hands-on SRM tasks, security becomes more visible and relevant to users. Consequently, user participation may be a mechanism for managing user perceptions on the importance of security.

Accountability was found to contribute most to user participation in SRM. One explanation for this finding is that the study context was regulatory compliance for a law that required annual external audits. In other words, compliance has a coercive component whereby users may have been required to participate. This finding suggests that regulation may provide an opportunity for security managers (and regulators) to engage business users in security risks and controls when regulatory compliance has a business process orientation (e.g., maintaining electronic health records, customer identity information, etc.). Secondly, regardless of regulation, study findings suggest that efforts at accountability for SRM may be more effective if there are routine audits with documented results and follow-up for control deficiencies.

Research Contribution

Research on security awareness has primarily focused on how to develop effective awareness programs and psychological and behavioral outcomes, such as changes in user attitude, intention, or perceptions (e.g., D'Arcy et al. 2009; Dinev and Hu 2007; Rudolph 2006; Siponen 2000a; Whitman 2008). In contrast, the present study examined how awareness impacts security controls. Both the qualitative and quantitative studies found evidence that greater awareness of security risks and controls contributes to improvements in both control development (i.e., design and implementation) and performance (i.e., reduced deficiencies and greater efficiency). Secondly, as an alternative or supplement to conventional security awareness training for users, the present study advocates raising awareness by engaging users in the process of managing specific security risks within their business processes. By having users participate in SRM, security becomes more relevant to users **and** security measures become better aligned with business objectives. As such, user participation becomes a valuable awareness strategy for users, IS, and security professionals.

Secondly, the multi-method research design of the study contributed a rich contextual description of user participation in SRM within business processes, thereby answering calls

for studies of user participation in current contexts (Markus and Mao 2004) and multi-method studies in IS (Mingers 2001). Semi-structured interviews in the exploratory study enabled informants to narrate the tasks, documentation, roles, current outcomes, past comparisons, and future organizational plans for SRM in business processes. Secondly, by applying a two-stage research approach, an exploratory study was conducted without preconceived outcomes, followed by a confirmatory study that tested the researchers' interpretation of qualitative results (Lee 1991). Triangulation between data sources strengthened the study results (Kaplan and Duchon 1988). In addition to applying language from the field to survey items, the qualitative study provided the added benefit of gauging the level of sensitivity informants had in answering questions on the sensitive topic of SRM. As a result, the qualitative study provided some degree of content validity to the quantitative study. Although time-consuming, combining qualitative and quantitative methods was found to be beneficial and complementary (Gable 1994; Mingers 2001; Sawyer 2001).

Implications for Practice

The results of the present study suggest that user participation provides security professionals with contextual business requirements for security from which to build a better, more convincing business case for security investment. Indeed, the literature has often noted security managers' difficulty in building a business case for IS security that explains the relevance of IS security to the overall business strategy (see Mattord and Want 2008). When users provide input into the security program on evolving business usage of and employee behavior toward sensitive information, security professionals can use this input to develop more effective controls, as well as to a build a business case for further security investment.

A second implication of the study is the paradox between transparent and visible security controls. Some degree of transparency in security controls may be desirable so that they function seamlessly in the background. However, study findings suggest that there is also benefit to explicit, hands-on participation in security tasks so that SRM is visibly present in the daily work routine. Such visibility raises awareness of security risks and the need to protect sensitive data.

Finally, study findings suggest that user participation in SRM acts as on-the-job security training that is tailored to specific business processes. During user participation in SRM, users provide their expertise in the contextual details of how information is used in routine business operations and, while doing so, they learn from control designers more about the organization's risk tolerance, policies, and procedures. Such context-specific on-the-job training goes beyond generic IS security training. Instead, security training via user participation is specific to business processes, and therefore is likely to have greater meaning, and perhaps interest, for users, encouraging greater commitment in protecting sensitive organizational information.

Study Limitations

Several limitations of the study need to be acknowledged. First, user participation was measured using three 7-item indices that defined the comprehensiveness of participation. However, these indices do not measure the degree (i.e., amount or frequency) of participation. Unlike in an ISD study where user participation is typically examined at an individual level of analysis by self-report, the present study examined user participation at an organizational level of analysis by informants reporting their understanding of user participation across the organization in protecting financial information. Therefore, use of indices enabled a global assessment of activities that a respondent (e.g., IS manager, internal auditor) was able to objectively observe.

A second limitation of the study is its focus on compliance with a single U.S. regulation, the Sarbanes-Oxley Act. Though SOX is a U.S. law and its effects are more pronounced in the U.S., international companies traded on U.S. stock exchanges must comply. In addition, the European Union (for a comparative analysis, see Girasa and Ulinksi 2007) and several countries (e.g., Japan, Australia, and Canada) have enacted legislation similar to SOX. Thus, study findings may be noteworthy beyond the United States. Moreover, although the qualitative and quantitative studies focused on SOX compliance efforts, study findings of the outcomes of user participation are largely expected to apply beyond a regulatory context. That is, user participation in SRM activities for specific controls within business processes is expected to result in greater awareness, better business-aligned SRM, and improved control development and performance. However, regulatory compliance places greater emphasis on accountability and control monitoring that may vary in noncompliance contexts. In this sense, regulatory compliance may be an impetus to greater business participation in, and organizational awareness of, SRM.

A third limitation of the present study stems from the relatively low response rate that was obtained to the questionnaire survey, and the potential for non-response bias. Although e-mail surveys have been found to result in significantly lower response rates than mail surveys, in part due to e-mails being sent to wrong addresses, routed to junk folders, unopened by recipients (Ranchhod and Zhou 2001), or sent to members

who did not fit the target population, it was not feasible for ISACA staff to administer a mail or telephone survey to its members on behalf of the researchers. Furthermore, follow-up contact with non-respondents, a technique consistently found to be the most effective method of increasing response rates (e.g., Deutskens et al. 2004), was not possible because the researchers did not have access to ISACA's member database. Finally, of those targeted members who read the email, a significant percentage may have worked for organizations with policies prohibiting employees from participating in surveys in general, or security studies in particular, as was found in another security study (Kotulic and Clark 2004). Given these considerations it is likely that the e-mail request reached considerably less than the initial list of 14,000, and that many of those who were reached did not fit the target population or were prohibited from responding. While the low response rate suggests that non-response bias may be present in the survey sample, it is unlikely to have affected the study results given the convergence between the findings of the qualitative and survey studies.

Suggestions for Future Research

The present study suggests two areas where future research would be valuable. First, an examination of user participation at an individual level of analysis would increase our understanding of participation in SRM contexts. The present qualitative study interviewed informants who were knowledgeable of SOX compliance efforts and included auditors, risk managers, IS managers, and users. Increased awareness was a consistent outcome associated with user participation across informants and companies, based on users posing questions and demonstrating a consciousness about security. Only one informant, a user, recounted psychological involvement as an outcome of participation. In contrast, user participation studies in ISD contexts are typically conducted at the individual level via self-report and find psychological involvement to be a key outcome. Research on user participation in SRM is needed at an individual level to examine psychological and affective outcomes such as involvement, attitude, intention, and acceptance.

Given that user participation was found to contribute to greater alignment between SRM and the business context, a second suggestion for future research is to further examine the effects of business-aligned SRM. For example, when SRM is better aligned with the business context, do security breaches from internal personnel decrease? Are security managers better skilled at building a business case for further investments in security? Is it more or less costly to maintain security controls? How are technology solutions for IS security impacted?

Conclusions

Although the IS security literature has often cited users as the weak link in IS security due to user errors and negligence, the present study provides evidence that supports an opposing view. That is, business users were found to add value to IS security risk management when they participated in the prioritization, analysis, design, implementation, testing, and monitoring of user-related security controls within business processes. User participation raises organizational awareness of security risks and controls within business processes, which in turn contributes to more effective security control development and performance. The need for regulatory compliance may encourage user participation in SRM within targeted business processes. Security managers can harness regulatory compliance as an opportunity to engage users, raise organizational awareness of security, and better align security measures with business objectives.

Acknowledgments

The authors wish to thank the senior editor, associate editor, and three anonymous reviewers for their insightful comments and recommendations that contributed to significant improvements in the paper. They also wish to thank Russell Barton, John Calderon, John Lindquist, Alain Pinsonneault, and Suzanne Rivard for their valuable feedback on early versions of the paper. They are also grateful for the financial support of the Canada Research Chairs program, the Center for Digital Transformation at the Smeal College of Business, EWA Information Infrastructure and Technologies, and the Smeal College of Business.

References

Alberts, C., and Dorofee, A. 2003. *Managing Information Security Risks: The Octave Approach*, Upper Saddle River, NJ: Addison-Wesley.

Aytes, K., and Connolly, T. 2004. "Computer Security and Risky Computing Practices: A Rational Choice Perspective," *Journal of Organizational and End User Computing* (16:3), pp. 22-40.

Barki, H., and Hartwick, J. 1989. "Rethinking the Concept of User Involvement," *MIS Quarterly* (13:1), pp. 53-63.

Barki, H., and Hartwick, J. 1994. "Measuring User Participation, User Involvement, and User Attitude," *MIS Quarterly* (18:1), pp. 59-82.

Baroudi, J. J., Olson, M. H., and Ives, B. 1986. "An Empirical Study of the Impact of User Involvement on System Usage and Information Satisfaction," *Communications of the ACM* (29:3), pp. 232-238.

Chin, W. W. 1998. "The Partial Least Squares Approach to Structural Equation Modeling," in *Modern Methods for Business Research,* G. A. Marcoulides (ed.), Mahwah, NJ: Lawrence Erlbaum Associates, pp. 295-336.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Deutskens, E., de Ruyter, K., Wetzels, M., and Oosterveld, P. 2004. "Response Rate and Response Quality of Internet-Based Surveys: An Experimental Study," *Marketing Letters* (15:1), pp. 21-36.

Dhillon, G., and Backhouse, J. 2000. "Information System Security Management in the New Millennium," *Communications of the ACM* (43:7), pp. 125-128.

Dhillon, G., and Moores, S. 2001. "Computer Crimes: Theorizing About the Enemy Within," *Computers & Security* (20:8), pp. 715-723.

Dinev, T., and Hu, Q. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the Association for Information Systems* (8:7), pp. 386-408.

Doherty, N. F., and Fulford, H. 2005. "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis," *Information Resources Management Journal* (18:4), pp. 21-39.

Furnell, S. 2008. "End-User Security Culture: A Lesson That Will Never Be Learnt?" *Computer Fraud & Security* (2008:4), pp. 6-9.

Gable, G. G. 1994. "Integrating Case Study and Survey Research Methods: An Example in Information Systems," *European Journal of Information Systems* (3:2), pp. 112-117.

Girasa, R. J., Ulinksi, M. 2007. "Comparative Analysis of Select Provisions of the Sarbanes-Oxley Act with the European Union's Eighth Directive," *The Business Review* (9:1), pp. 36-41.

Goodhue, D. L., and Straub, D. W. 1991. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security," *Information & Management* (20), pp. 13-27.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. 2005. "CSI/FBI Computer Crime and Security Survey," Computer Security Institute (available online at http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf).

Halliday, S., Badenhorst, K., and von Solms, R. 1996. "A Business Approach to Effective Information Technology Risk Analysis and Management," *Information Management & Computer Security* (4:1), pp. 19-31.

Hanson, W. E., Creswell, J. D., Creswell, J. D., Plano Clark, V. L., and Petska, K. S. 2005. "Mixed Methods Research Designs in Counseling Psychology," *Journal of Counseling Psychology* (52:2), pp. 224-235.

Hartwick, J., and Barki, H. 1994. "Explaining the Role of User Participation in Information System Use," *Management Science* (40:4), pp. 440-465.

Hartwick, J., and Barki, H. 2001. "Communication as a Dimension of User Participation," *IEEE Transactions on Professional Communication* (44:1), pp. 21-36.

Hu, Q., Hart, P., and Cooke, D. 2006. "The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective," in *Proceedings of the 39th Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computer Society Press.

ISO/IEC . 2000. "Information Technology—Code of Practice for Information Security Management," ISO/IEC 17799:2000(E), International Organization for Standardization (available online at http://www.iso.org/iso/catalogue_detail?csnumber=33441).

ITGI. 2004. "IT Control Objectives for Sarbanes-Oxley," Rolling Meadows, IL: IT Governance Institute .

ITGI. 2005. *COBIT* (4.0 ed.), Rolling Meadows, IL: IT Governance Institute.

Ives, B., and Olson, M. H. 1984. "User Involvement and MIS Success: A Review of Research," *Management Science* (30:5), pp. 586-603.

Jahner, S., and Krcmar, H. 2005. "Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk Management," in *Proceedings of the 11th Americas Conference on Information Systems,* Omaha, NE, August 11-14.

Jarvis, C. B., Mackenzie, S. B., and Podsakoff, P. M. 2003. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *Journal of Consumer Research* (30:2), pp. 199-218.

Kaplan, B., and Duchon, D. 1988. "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study," *MIS Quarterly* (12:4), pp. 571-586.

Kokolakis, S. A., Demopoulos, A. J., and Kiountouzis, E. A. 2000. "The Use of Business Process Modeling in Information Systems Security Analysis and Design," *Information Management & Computer Security* (8:3), pp. 107-116.

Kotulic, A., and Clark, J. G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41), pp. 597-607.

Latham, G. P., Winters, D. C., and Locke, E. A. 1994. "Cognitive and Motivational Effects of Participation: A Mediator Study," *Journal of Organizational Behavior* (15:1), pp. 49-63.

Lee, A. S. 1991. "Integrating Positivist and Interpretive Approaches to Organizational Research," *Organization Science* (2:4), pp. 342-365.

Locke, E. A., Alavi, M., and Wagner, J. A. 1997. "Participation in Decision Making: An Information Exchange Perspective," *Research in Personnel and Human Resources Management* (15), pp. 293-331.

Markus, M. L., and Mao, J.-Y. 2004. "Participation in Development and Implementation—Updating an Old, Tired Concept for Today's IS Contexts," *Journal of the Association for Information Systems* (5:11-12), pp. 514-544.

Mattord, H. J., and Want, T. 2008. "Information System Risk Assessment and Documentation," in *Information Security: Policy, Processes, and Practices,* D. W. Straub, S. Goodman, and R. L. Baskerville (eds.), Armonk, NY: M. E. Sharpe, Inc., pp. 69-111.

McAdams, A. 2004. "Security and Risk Management: A Fundamental Business Issue," *Information Management Journal* (38:4), pp. 36-44.

Miles, M. B., and Huberman, A. M. 1994. *Qualitative Data Analysis* (2nd ed.), Thousand Oaks, CA: Sage Publications.

Mingers, J. 2000. *Multimethodology: The Theory and Practice of Combining Management Science Methodologies*, Chichester, England: John Wiley & Sons.

Mingers, J. 2001. "Combining IS Research Methods: Towards a Pluralist Methodology," *Information Systems Research* (12:3), pp. 240-259.

Myers, M. D., and Newman, M. 2007. "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization* (17:1), pp. 2-26.

Newman, I., Ridenour, C., Newman, C., and DeMarco, G. M. P. 2002. "A Typology of Research Purposes and Its Relationship to Mixed Methods Research," in *Handbook of Mixed Methods Social and Behavioral Research,* A. Tashakkori and C. B. Teddlie (eds.), Thousand Oaks, CA: Sage Publications.

NIST. 2004. "Chapter 7: Computer Security Risk Management," 800-12, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC.

PCAOB. 2004. "Auditing Standard No. 2: An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," Public Company Accounting Oversight Board, New York.

Ranchhod, A., and Zhou, F. 2001. "Comparing Respondents of E-Mail and Mail Surveys: Understanding the Implications of Technology," *Marketing Intelligence & Planning* (19:4), pp. 254-262.

Rudolph, K. 2006. "Implementing a Security Awareness Program," in *Handbook of Information Security,* H. Bidgoli (ed.), New York: John Wiley & Sons, Inc., pp. 766-785.

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, July 30, 2002, 116 Stat. 745, 107th Congress (available online at http://corporate.findlaw.com/industry/corporate/docs/publ107.204.pdf)

Sawyer, S. 2001. "Analysis by Long Walk: Some Approaches to the Synthesis of Multiple Sources of Evidence," in *Qualitative Research in IS: Issues and Trends,* E. M. Trauth (ed.), Hershey, PA: IDEA Group Publishing, pp. 163-189.

Siponen, M. T. 2000a. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1), pp. 31-41.

Siponen, M. T. 2000b. "Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice," *Information Management & Computer Security* (8:5), pp. 197-210.

Siponen, M. T. 2001. "Five Dimensions of Information Security Awareness," *Computers and Society* (31:2), pp. 24-29.

Siponen, M. T. 2005. "Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods," *Information and Organization* (15:1), pp. 339-375.

Spears, J. L. 2005. "A Holistic Risk Analysis Method for Identifying Information Security Risks," in *Security Management, Integrity, and Internal Control in Information Systems,* P. Dowland, S. Furnell, B. Thuraisingham, and X. S. Wang (eds.), New York: Springer, pp. 185-202.

Spears, J. L. 2007. *Institutionalizing Information Security Risk Management: A Multi-Method Empirical Study on the Effects of Regulation*, Ph.D. Dissertation, The Pennsylvania State University (available through ProQuest Digital Dissertations).

Spears, J. L., and Cole, R. J. 2006. "A Preliminary Investigation of the Impact of the Sarbanes-Oxley Act on Information Security," in *Proceedings of the 39th Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computer Society, p. 218.

Stanton, J. M., and Stam, K. R. 2006. *The Visible Employee*, Medford, NJ: Information Today, Inc.

Straub, D., and Welke, R. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Suh, B., and Han, I. 2003. "The IS Risk Analysis Based on a Business Model," *Information & Management* (41:2), pp. 149-158.

Swanson, E. B. 1974. "Management Information Systems: Appreciation and Involvement," *Management Science* (21:2), pp. 178-188.

Trauth, E. M. 2001. "The Choice of Qualitative Methods in IS Research," in *Qualitative Research in IS: Issues and Trends,* E. M. Trauth (ed.), Hershey, PA: IDEA Group Publishing, pp. 1-19.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2008. "Process-Variance Models in Information Security Awareness Research," *Information Management & Computer Security* (16:3), pp. 271-287.

Urquhart, C. 2001. "An Encounter with Grounded Theory: Tackling the Practical and Philosophical Issues," in *Qualitative Research in IS: Issues and Trends,* E. M. Trauth (ed.), Hershey, PA: IDEA Group Publishing, pp. 104-140.

von Solms, B., and von Solms, R. 2004. "The 10 Deadly Sins of Information Security Management," *Computers & Security* (23), pp. 371-376.

Wade, J. 2004. "The Weak Link in IT Security," *Risk Management* (51:7), pp. 32-37.

Whitman, M. E. 2004. "In Defense of the Realm: Understanding Threats to Information Security," *International Journal of Information Management* (24), pp. 43-57.

Whitman, M. E. 2008. "Security Policy: From Design to Maintenance," in *Information Security: Policy, Processes, and Practices,* D. W. Straub, S. Goodman, and R. L. Baskerville (eds.), Armonk, NY: M. E. Sharpe, Inc., pp. 123-151.

About the Authors

Janine L. Spears is an assistant professor in the College of Computing and Digital Media at DePaul University. She received her Ph.D. in 2007 in Information Systems from the Smeal College of Business at the Pennsylvania State University and was subsequently a Postdoctoral Fellow at HEC Montreal. Her research focuses on information security risk management, assurance, regulatory compliance, and governance.

Henri Barki is Canada Research Chair of Information Technology Implementation and Management at HEC Montréal and a member of the Royal Society of Canada. His research focuses on the development, introduction, and use of information technologies in organizations and has appeared in the *Canadian Journal of Administrative Sciences, Database, IEEE Transactions on Professional Communication, Information Systems Journal, Information Systems Research, Information & Management, INFOR, International Journal of Conflict Management, International Journal of e-Collaboration, International Journal of e-Government Research, Journal of the AIS, Journal of Information Technology, Journal of MIS, Management Science, MIS Quarterly, Organization Science,* and *Small Group Research.*