MIS Quarterly

SPECIAL ISSUE

USER PARTICIPATION IN INFORMATION SYSTEMS SECURITY RISK MANAGEMENT

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

Appendix A

Multi-Method Research Design

Research Design Elements	Interviews	Survey	Integration
Research Problem	Rich context needed		
Data Collection	Semi-structured: Derived from (1) Research question (2) Exploratory	Derived from interview data	Sequential data collection: (1) interviews (2) survey
Model Construction	Process	Variance	User participation construct is formative with indices of process
Survey Instrument		Items derived from: (1) Qualitative results (2) Literature (3) Pretest (4) Pilot study	
Data Analysis	(1) Characterize user participation in the context of SRM in business process (2) Identify outcomes	(1) Contstruct validation (2) Hypothesis testing (3) Analysis of variance	Triangulation
Limitations	Filtering data	(1) Cannot measure what you do not know (2) Does not adequately provide context	(1) Time-consuming to collect, analyze, write (2) Requires researcher skill of two diverse methods (3) Debate continues on value
Benefits	Rich context	(1) Clarity (more precise definition) of theoretical concepts (2) Reveals theoretical relationships that may have been missed in qualitative study	(1) Allows for *both* rich context and testability (2) Appreciating value of each methodology

Appendix B

Interview Guide

1. Company's background information (e.g., primary industry, number of employees)
2. Informant's background information (e.g., title, years at firm; current and previous roles)
3. Is the term information security used in your organization? What does that term mean in this organization? What activities are within its scope? How has this changed in the past 2 years?
4. Write a flowchart of information security governance within your organization to include roles, departments, and hierarchical structure involved.
5. When did the SOX initiative start here? When did the company first have to be compliant?
6. How many people initially worked on SOX compliance activities versus how many people work on SOX compliance activities now?
7. Describe the roles that work on SOX compliance and the activities they perform.
8. Were any of these roles created or revised as part of SOX compliance?
9. What roles/groups provided the most relevant information when analyzing potential information security risks in business processes? When defining policies?
10. How do you know that a particular security control is appropriate to meet a specific type of risk? In other words, based on a portfolio of risks, how do you know which practices to implement in order to mitigate specific risks?
11. Of the controls that were created or enhanced for SOX compliance, approximately what percentage do you think were manual versus technical/automated controls?
12. Were manual controls defined by business process owners?
13. What impact has user participation had on information security? Risk management? Discovery of significant weaknesses?
14. How does your organization know if information security has improved? Do you have any specific measures of performance?
15. Does the IT department work in parallel to or in conjunction with users on SOX?
16. Are IT security managers kept abreast of policy decisions and controls developed by users? To what degree?
17. What has changed since the initial SOX compliance effort versus how things are done now?
18. Prior to SOX, did functional business users participate in information security risk management or related policy development?
19. Since achieving SOX compliance, have users continued to participate in SOX activities?
20. Prior to SOX, how much did internal auditing participate in information security?
21. Prior to SOX, what roles and how many people normally worked on information risk management? How about now?
22. How has managing information security changed as a result of SOX initiatives?
23. What have been the high-level outcomes of the SOX compliance initiative?
    a. Any spinoff projects?
    b. Any policies (on security or risk management) developed or changed?
    c. Any new training on information security (or changes to existing training)?
    d. Any new roles (jobs) created?
    e. Any plans for broader involvement on security from other functional areas of business (e.g., marketing, R&D, etc.)?
    f. Any new technologies?
    g. Any significant efficiency enhancements to business processes?
    h. Any noticeable cultural changes within the department or organization as related to information security?
    i. How widespread was the effect of the controls implemented?
24. What has been the biggest effect of business participation in information security initiatives such as SOX? Describe.
25. What would you say have been the critical success factors for this project? Describe.
26. What would you say have been major obstacles of (or limitations to) this project? Describe.
27. What strikes you most from your experience working on this project?
28. Are there any major changes, improvements, fixes that have been made, or are in the process of being made, that were not required for SOX compliance?

Appendix C

Survey Items

Variable	Survey Item
User participation in the risk management process	In managing risk to financial reporting, do functional business managers/staff in your company actively perform, or contribute to decision-making in, any of the following risk management activities? (check all that apply) _____ documenting business processes or transactions for risk evaluation _____ ensuring key controls exist to mitigate specific types of risks _____ defining procedural controls (for example, rules for access control) _____ implementing controls _____ reviewing or testing controls _____ remediating defective controls _____ communicating SOX policies
User participation in security controls	Have business users (from functional lines of business) in your company actively participated in defining, reviewing, or approving any of the following types of information security controls related to protecting financial information or reporting? (check all that apply) _____ access control _____ separation of duties _____ alerts, triggers, or application controls _____ exception reports _____ spreadsheets or other end-user computing _____ employee training on information security awareness or on IT controls for SOX _____ risk tolerance (acceptable levels of risk)
User participation via accountability	During the past 12 months, have any of the following actions occurred in your company to provide management accountability for information security? (check all that apply) _____ individual roles and responsibilities defined and documented (or reviewed/ revised) _____ roles and responsibilities for protecting information assigned (or reviewed/ revised) _____ data or process owners made responsible for specific controls _____ senior management reviews information security policy _____ information security policies communicated to all employees and contractors _____ executive business management's support demonstrated for information security _____ a committee of IT and business managers did planning for information security
Awareness	"Internal employees working with financial information have a heightened awareness of policies, procedures, and/or the need to ensure integrity of financial reporting for SOX." **1. strongly disagree** (people must often be reminded to follow policy) 2. moderately disagree 3. mildly disagree **4. agree and disagree equally** (many people seem aware, while many others don't) 5. mildly agree 6. moderately agree **7. strongly agree** (people often mention, or ask questions to clarify, what is needed for SOX)

Variable	Survey Item
Demonstrated ownership	"During the past 12 months, functional business users working with financial information have demonstrated a sense of ownership toward protecting the integrity of financial reporting." **1.** **strongly disagree** (must often remind users to comply with controls or policies for SOX) 2. moderately disagree 3. mildly disagree **4.** **agree and disagree equally** (many people take ownership, while many do not) 5. mildly agree 6. moderately agree **7.** **strongly agree** (most users proactive in taking responsibility for integrity of financial reporting)
User business perspective	"Functional business users routinely contribute a business perspective to IT on managing information security risk to financial reporting and/or financial information systems." **1.** **strongly disagree** (no contribution) 2. moderately disagree 3. mildly disagree **4.** **agree and disagree equally** (business contributes, but not routinely) 5. mildly agree 6. moderately agree **7.** **strongly agree** (business users are formally part of routine decision-making in this area)
Business-based IS security strategy	"Strategic decisions on information security policies and solutions are largely business-driven; that is, they are based on business objectives, value, or needs." **1.** **strongly disagree** (decisions based primarily on vulnerabilities in technology) 2. moderately disagree 3. mildly disagree 4. agree and disagree equally 5. mildly agree 6. moderately agree **7.** **strongly agree** (decisions based primarily on business objectives, value, or need)
Perceived improvement in control development	To what extent has there been an improvement, if any, in the definition or implementation of each of the following types of controls as part of your company's SOX efforts? (1 = much worse, 4 = no change, 7 = much better) • access control for systems users • segregation of duties for system users • information security policy
Reduced deficiencies	"During the past 12 months, the total number, or the magnitude, of control deficiencies for key controls over financial reporting has decreased." **1.** **strongly disagree** (control deficiencies much worse) 2. moderately disagree 3. mildly disagree 4. **agree and disagree equally** (total # decreased/increased, while magnitude increased/decreased) 5. mildly agree 6. moderately agree **7.** **strongly agree** (major improvement)

Variable	Survey Item
Increased efficiencies	During the past 12 months, to what degree have there been efficiency improvements made (or are in-progress) to the system of controls, taken as a whole, by redesigning, consolidating, or automating key controls used to manage risk to financial information systems? **1.** **much worse** (important controls stopped, weakening security OR controls very inefficient) 2. significantly worse 3. a little worse 4. no change in improvement 5. a little better 6. significantly better **7.** **much better** (a major focus in the company; extensive improvements made/being made)

Appendix D

Item Correlations

	1	2	3	4	5	6	7	8	9	10	11
User participation (SRM)											
User participation (security controls)	.43***										
User participation (accountability)	.47***	.40***									
Awareness of IS security	.32***	.23***	.31***								
Demonstrated ownership	.34***	.40***	.41***	.51***							
User business perspective	.31***	.45***	.32***	.24***	.48***						
Business-based security strategy	.23***	.33***	.30***	.19**	.38***	.42***					
Control development (access)	.22***	.23***	.22**	.30***	.23***	.12	.14*				
Control development (segregation of duties)	.31***	.23***	.29***	.31***	.27***	.13*	.23***	**.63*** **			
Control development (policy)	.21***	.26***	.33***	.25***	.24***	.18**	.25***	.52***	.43***		
Control performance (deficiencies)	.30***	.20***	.25***	.36***	.38***	.22***	.20**	.24***	.27***	.19***	
Control performance (efficiencies)	.36***	.28***	.39***	.28***	.37***	.27***	.27***	.38***	.38***	.47***	.34***

***p < .001; **p < .01; *p < .05