The Impact Of Organizational Change On Information Systems Security

Melinda Cline, Texas Wesleyan, USA
Carl S. Guynes, University of North Texas, USA
Andrew Nyaboga, William Paterson University, USA

ABSTRACT

When major change is imposed on organizations, there is often resistance and resentment. Organizational change has been identified as one of the key issues that will present significant challenges to an organization's effective and timely implementation of privacy and security standards. It will be necessary to identify specific implementation requirements that represent the most significant organizational change challenges. Organizations will also have to identify processes and methods to foster acceptance of the change associated with the entire compliance project This research examines changing information security requirements and the strategies organizations are developing to meet the related challenges.

Keywords: Information Security, Organizational Change, Managerial Cognition, Sarbanes Oxley

INTRODUCTION

This paper develops a framework which is used to investigate how organizations are changing in response to new information security requirements. Changing information security requirements is of considerable importance due to the fact that organizations must simultaneously provide information to their employees, customers, and business partners while safeguarding it from inappropriate access, use, and disclosure. It further attempts to validate the framework, proposes a set of interesting research questions for further study, and concludes with a suggested methodology.

Employing an organizational change model to study information security is appropriate because while corporate IS security models have historically emphasized the role of management in setting, maintaining, and implementing security policies, procedures, and standards, many businesses are also developing organizational structures and operational procedures surrounding the technology [19]. This has included setting up basic safeguards such as insurance, audits, system application controls, physical protection systems and surveillance devices as well as developing contingency and disaster recovery procedures.

A MODEL FOR ORGANIZATIONAL CHANGE

In an effort to acknowledge the crucial role played by managerial actions in creating an environmental and organizational context conducive to a firm's strategies, the authors have attempted to present a model which could be useful to management in carrying out their duties in this complex environment. Figure One synthesizes recent organizational change literature to include ideas from the rational, learning, and cognitive theories on organizational change. Table One presents the definitions of the six conceptual model constructs. The model illustrates the interplay of managerial and learning factors inherent in the organizational change process. It acknowledges the direct effects of the environment and organization on changes in strategy; and recognizes that changes in the content of strategy must match the requirements of a firm's environmental and organizational contexts in order to be successful. It further implies that managerial learning is a continuous reshaping of managerial cognition which develops as outcomes from changes in strategy begin to emerge. [15, 17, 22]

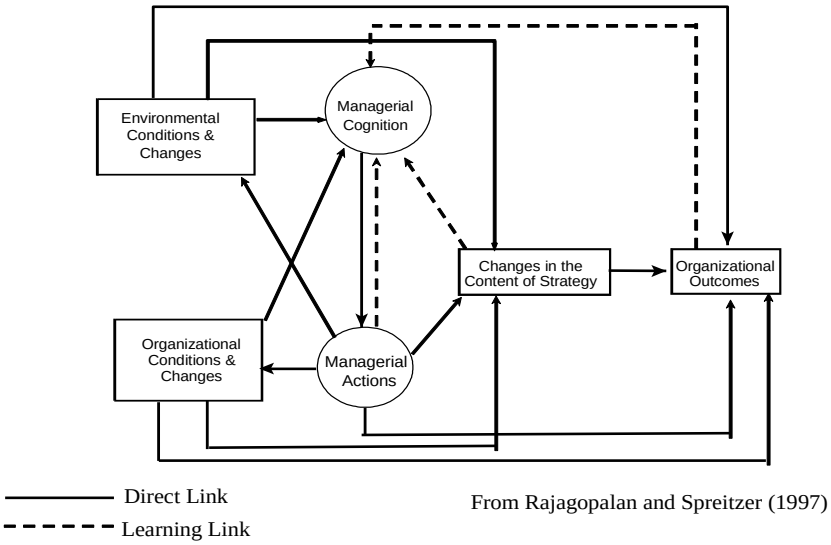

Figure One: Conceptual Model

Table One: Conceptual Model Constructs

Construct	Definition
Environmental Conditions & Changes	Demographic, economic, social, and political forces external to the organization that provide an impetus for change [13]
Organizational Conditions & Changes	Intra-organizational forces that initiate/support organizational change
Managerial Cognition	Manager's interpretation of actual and potential events[2]
Managerial Actions	Actions taken by managers to define and communicate a vision of change [9]
Changes in the Content of Strategy	Organizational responses to internal and external threats and opportunities [8]
Organizational Outcomes	Realized organizational performance

Employing an organizational change model to study computer security is appropriate because while corporate IS security models have historically emphasized the role of management in setting, maintaining, and implementing security policies, procedures, and standards, many businesses are also developing organizational structures and operational procedures surrounding the technology [19]. This has included setting up basic safeguards such as insurance, audits, system application controls, physical protection systems and surveillance devices as well as developing contingency and disaster recovery procedures.

METHODOLOGY

The first step in our research was to integrate information security issues into the conceptual model. These constructs capture an organization's external and internal information security environments, manager's perceptions about information security, changes to organizational processes resulting from increased security concerns, and organizational outcomes resulting from IT security initiatives. We began our research by performing a qualitative content analysis of the extant literature. The literature review took the form of first noting the ideas of consideration in each research paper or article then organizing these topics into the related constructs [5].

To validate our classification of issues discussed in extant literature and to ensure that we had not omitted other important information security issues, we conducted interviews with three information security executives who hold the title of either Vice President or President and who are directly responsible for the information security strategies of their organization. Our initial organization of topics was presented to each interviewee in separate one-hour meetings and their feedback was used to refine our ideas. Table Two summarizes the results.

Table Two: Information/Computer Security and Privacy Concerns

Construct	Ideas About Information Security
Environmental Conditions & Changes	Representative Legislation • Health Insurance Portability and Accountability Act (HIPAA) • Sarbanes-Oxley Act • Gramm-Leach-Bliley Act of 1999 • National Information Infrastructure Act of 1996 • U.S. Patriot Act of 2001 • Corporate Information Security Act of 2003 • Privacy Act of 2003 • Federal Information Security Act of 2002 Technology vulnerabilities [16] • Generally inadequate technology standards for secure computing • Wi-Fi protocol security flaws [10, 18] • Wireless Equivalent Privacy (WEP) vulnerabilities [3] Information systems threats[11] • Denial-of-service attacks • Unauthorized data access • Web-site penetration • Theft/disclosure of customer data Electronic criminal acts[21] • Identify theft • Internet fraud • Phishing - soliciting personal information through e-mail • Other fraudulent schemes
Organizational Conditions & Changes	Secure distributed corporate data • N-Tier architectures • Across supplier networks • Across outsourced networks Data assurance • Accuracy • Unauthorized Use • Organizational Culture • Internal Software Vulnerabilities • Inadequate internal security controls • Software bugs/errors/omissions/back doors
Managerial Cognition	Managerial concerns [14] • Competitive threats • Legal penalties • Asset protection • Privacy protection Perceived security priorities for 2004 [12] • Security review and assessment • Security policies and standards • Incident response teams

Construct	Ideas About Information Security
Managerial Actions	Managerial oversight [19] • Setting, maintaining, and implementing security policies, procedures, and standards • Increased hiring of certified security professionals • Increased training Installation of security hardware [5] • Biometrics • Smart cards • Firewall applications/VPNs/ intrusion detection systems (IDSs) • Intrusion Prevention Systems (IPSs) Installation of security software [20] • Certificate authorities • Single sign-on • Provisioning • Access controls • Secure e-mail • Encryption • Enterprise security management • Vulnerability assessments • E-mail scanning • Web filtering • Audit software Acquisition of security services[20] • Consulting • Digital forensics • Disaster recovery/business continuity • Executive recruitment • Managed security services • Penetration testing • Outside audit services
Changes in the Content of Strategy	Risk Management[19] • Contingency/disaster recovery plans • Continuity plans • Insurance • Audits
Organizational Outcomes	Loss Prevention • Reduce unauthorized access • Reduce service attacks • Reduce loss of data • Reduce unauthorized disclosure • Improve data accuracy

INTERVIEW FINDINGS

A number of interesting findings emerged from this conceptual analysis. First, all interviewees noted that information security initiatives tend to be a reactive response to stimuli in an organization's external environment rather than proactive and implemented as an integral part of on-going business initiatives. The interviewees believed that a proactive information security strategy would provide substantial positive benefits. They suggested that managers investigate the advantages and disadvantages of having a proactive (internally driven) versus reactive (externally driven) strategic approach to information security.

Second, the interviewees all mentioned executive management cognition as a major issue. They acknowledged the importance of a champion for successful security implementation, but voiced frustration about the level of understanding of executives in this area. The findings indicate that management is concerned with the negative consequences of security breaches, but that security issues are considered secondarily, which exposes the organization to considerable risk. The interviewees thought that it is important to investigate how executive awareness of security issues and best practices can be raised and how security personnel can better asses and communicate the level of threats.

Third, while discussing security implementations, the interviewees indicated that they encounter substantial resistance among organizational members. Executives often demand to be excluded from even simple security measures like having to regularly change their passwords and others within the organization find ways to circumvent controls. For those trying to successfully protect information assets this is very frustrating because even though they are held responsible for systems security, they usually have little direct authority to enforce security policies. The interviewees thought that it is important to investigate what characteristics of an organization's culture must be adhered to in order to establish and maintain successful governance of its information security strategies.

Last, while discussing organizational outcomes, an Interviewee noted that it is difficult to understand the results of information security initiatives because business requirements are often not in alignment with security models. This to some degree may be a result of organizations being reactive rather than proactive, but it may also be the result of a lack of understanding as to how to best assess and communicate the outcomes of an organization's security initiatives. One way to resolve this problem is to determine the most effective ways to communicate organizational outcomes related to information systems security, so that managers can adjust future initiates to better serve the organization's employees, suppliers, and customers.

CONCLUSION

To investigate the research questions posed, the authors suggest using a "practice lens" methodological approach (Orlikowski, 2000). Examining the application of technology from this perspective accommodates people's situated use of dynamic technologies making no assumptions about the stability, predictability, or relative completeness of the technologies. This is important for the study of information security technology because it is so dynamic. A "practice lens" assumes that people are purposive, knowledgeable, adaptive, and inventive agents who engage with technology in a multiplicity of ways. Focusing attention on recurrent social practices acknowledges that while users can and do use technologies as they were designed, they also can and do circumvent inscribed ways of using the technologies – either ignoring certain properties of the technology, working around them, or inventing new ones that may go beyond or even contradict designers' expectations and inscriptions.

When major change is imposed on organizations, there is often resistance and resentment. Organizational change has been identified as one of the key issues that will present significant challenges to an organization's effective and timely implementation of privacy and security standards. It will be necessary to identify specific implementation requirements that represent the most significant organizational change challenges. Organizations will also have to identify processes and methods to foster acceptance of the change associated with the entire compliance project [5]. This will involve identifying the tools and resources that an organization can utilize to effectively manage change in reaching compliance.

AUTHOR INFORMATION

Melinda Cline is an Associate Professor of Information Systems at Georgia Gwinnett College.
She received her Ph.D. from Florida State University. Her research interests include information technology investment, organizational change, knowledge-based systems, impacts of new technologies, and international business. She has published articles in *the Journal of Information Systems Management, Information Strategy, Decision Support Systems, Computers and Society, Managerial Auditing Journal, Journal of Computer Information Systems and Computer Science Education.*

Carl S. Guynes is a Regents Professor of Business Computer Information Systems at the University of North Texas. He received a doctorate in quantitative analysis from Texas Tech University. Dr. Guynes' areas of specialization are client/server computing, end-user computing, data administration, and information resource management. His most recent research efforts have been directed in the areas of client/server computing and data administration. Some of the journals in which Dr. Guynes has published include and *Communications of the ACM, Information & Management, The Journal of Information Systems Management, Journal of Accountancy, Journal of Systems Management, The Journal of Database Management, The CPA Journal, The Journal of Computer Information Systems, Information Strategy, Computers and Security, and Computers and Society*.

Andrew B. Nyaboga earned his Ph.D at Stevens Institute of Technology, Hoboken New Jersey in 2000.Currently he is an associate professor of Accounting and Law at William Paterson University in Wayne New Jersey and teaches courses in accounting and accounting Information System. His research interests are in technology management, knowledge management and strategic Management. His work has been published in numerous refereed journals.

REFERENCES

1. Austin, R. D. and C. Darby. "The Myth of Secure Computing," *Harvard Business Review*, 81:6, 2003, pp.120 – 126.
2. Bowman, E. and D. Hurry. "Strategy Through the Option Lens: An Integrated View of Resource Investments and the Incremental-Choice Process," *Academy of Management Review*, 18:4, 1993, pp. 760-782.
3. Cam-Winget, N., R. Housley, D. Wagner, and J. Walker. "Security Flaws in 802.11 Data Link Protocols," *Communications of the ACM*, 46:5, 2003, pp. 35 – 39.
4. Culnan, M. and P. Armstrong. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, 10:1, 1999, pp. 104 – 115.
5. Detert, J., R. Schroeder, and J. Mauriel. "A Framework for Linking Culture and Improvement Initiatives in Organizations," *Academy of Management Review*, 25:4, 2000, pp. 850 - 863.
6. Fisher, D. "Agencies Beef Up IT Security," *eWeek*, January 5, 2004, pp. 9 – 10.
7. Fonseca, B. and J. McCarthy. "Identity Management: Technology of Trust," *Infoworld*, June 23, 2003, pp. 55 – 61.
8. Ginsberg, A. "Measuring and Modeling Changes in Strategy: Theoretical Foundations and Empirical Directions," *Strategic Management Journal*, 9, 1988, pp559-575.
9. Guha, S., V. Grover, W. Kettinger, and J. Teng. "Business Process Change and Organizational Performance: Exploring an Antecedent Model," *Journal of Management Information Systems*, 14:1, 1997, 119-154.
10. Housley, R. and W. Arbaugh. "Security Problems in 812.11 – Based Networks," *Communications of the ACM*, 46:5, 2003, pp. 31 – 34.
11. Hulme, G. "Security Threats Won't Let Up," *Informationweek*, January 5, 2004, pp. 59 – 62.
12. *Garvey, M. J.* "What's to Come," *InformationWeek*, November 10, 2003.
13. March, J. "Footnotes to Organizational Change," *Administrative Science Quarterly*, December 1981, pp. 563 – 577.
14. Melymuka, K. "Too Much To Do!," *Computerworld.com*, January 2, 2003.
15. Orlikowski, W. "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations," *Organization Science*, 11:4, 2000, pp. 404 – 428.
16. Panda, B. and J. Giordano . "Defensive Information Warfare," *Communications of the ACM*, 42:7, 1999, pp. 30 - 32.
17. Rajagopalan, N. and G. Spreitzer. "Toward a Theory of Strategic Change: A Multi-lens Perspective and Integrative Framework," *The Academy of Management Review*, 22:1, 1997, 48-79.
18. Schmidt, T. and A. Townsend. "Why WiFi Wants to be Free," *Communications of the ACM*, 46:5, 2003, pp. 47 – 52.
19. Segev, A., J. Porra, and M. Roldan. "Internet Security and the Case of Bank of America," *Communications of the ACM*, 41:10, 1998, pp.81 – 87.
20. Slater, D. "How Does Your Company Stack Up?," *CSO Online*, January 2005.
21. Sullivan, A. "Identity Theft, Internet Fraud Reports Up in U.S.," *Reuters*, January 22, 2004.
22. Van De Ven, A. "Nothing is Quite So Practical as a Good Theory," *Academy of Management Review*, 14:4, 1989, 486 - 489.