Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2011 Proceedings | Southern (SAIS)

2011

Improving Information Security Through Technological Frames of Reference

Derek J. Sedlack
Nova Southeastern University, sedlack@nova.edu

Gurvirender P.S. Tejay
Nova Southeastern University, tejay@nova.edu

Improving Information Security Through Technological Frames of Reference

Derek J. Sedlack
Nova Southeastern University
sedlack@nova.edu

Gurvirender P.S. Tejay
Nova Southeastern University
tejay@nova.edu

ABSTRACT

There is a growing emphasis on robust, organizationally focused information security methods to countermand losses from growing computer security incidents. We focus on using technological frames of reference to study the information security gap created by incongruent member perceptions related to information risk among different stakeholder communities. We argue that reducing member perception incongruity will improve organizational information security effectiveness.

Keywords

Information security, information risk, technological frames of reference

INTRODUCTION

Information security has evolved to include organizationally focused methods (Baskerville, 1993; Bhagyavati and Hicks, 2003; Dhillon, 1995; Dhillon and Backhouse, 1996; Farahmand, Navathe, Enslow, and Sharp, 2003; Liebenau and Backhouse, 1990). Even with a focus on the enterprise, users remain the weakest link in the information security chain (Whitman and Mattord, 2005) and the majority of users who use technology are not specifically trained in IT or security (Hazari, Hargrave, and Clenney, 2008). As users become more accustomed to information technology, they tend to ignore systemic problems regardless of their severity (Vaast, 2007). With federal mandates for converting to electronic, interconnected Healthcare records, it becomes increasingly important for healthcare provider employees to adopt risk perceptions in alignment with organizational goals.

Worker usability may create IS security gaps through circumvented security measures based on misaligned perceptions. Adams and Sass (1999) found that users presented with unreasonable or *not sensible* work practices will either ignore them or circumvent them to accomplish the task at hand that may translate into behavior tendencies. Aligning the perceptions of risk, management and user, Adams and Sass believe that more security conscious behavior result in more security awareness and organizational security. While security awareness is a key element, policies and standards provide methods of dealing with realized breaches. Policies are important because "users may not understand all the events that could be considered a breach nor clearly understand how and when to report a breach" (Rotvold, 2008, p. 37). It is recommended that organizations should develop basic security policies encompassing both internal and external requirements (Bhagyavati and Hicks, 2003; Craig, 1993; Jones and Lipton, 1975).

It is argued that organizational groups form similar views of information security (Vaast, 2007). These common views, or frames (Bijker, 1987) relating to technology create incongruity through changing perceptions that become evident during IT implementations (Davidson, 2006) as each organizational group views outcomes differently through the interaction created by different roles, experiences, and knowledge associated with that technology. Individual incongruity exists, but organizational efficiency is based on an organizational context. This paper presents technological frames of reference as an approach for improving information insecurity from incongruent perceptions related to information risk among different stakeholder communities.

REDUCING INCONGRUITY IN PERCEPTIONS OF RISK

This paper utilizes technological frames of reference (TFR) to understand perceptions of information risk. TFR states that organizational groups develop similar views or frames concerning the assumptions, expectations, and knowledge they use to understand technology in organizations (Orlikowski and Gash, 1994). TFRs are dynamic, guide member interpretations and actions related to technology, and possess variable dimensions that temporally shift in context salience and content, providing

an appropriate lens for studying organizational member perceptions of risk that are equally dynamic and temporally shift in context salience and content.

TFR and proposed information security constructs are presented in Table 1. The nature of information security implies the procedural, structural, conceptual, or physical reasons for information security implementations or *what* technologies are used for in organizations including capabilities and power of effectiveness (Orlikowski and Gash, 1994). The proper installation and operation (Barnard and von Solms, 2000) of information security artifacts is critical to reducing risk (Dhillon and Backhouse, 2000) and that requires understanding why the artifact was purchased and implemented.

Constructs	Definitions	Security constructs	Construct definition	Supporting literature
TFR – Nature of technology	Procedural, structural, conceptual, or physical IS implementations.	Nature of information security	Procedural, structural, conceptual, or physical reasons for information security implementations.	(Barnard and von Solms, 2000; Dhillon and Backhouse, 2000)
TFR – Technical strategy	Business requirements governing the adoption, and implementation IS	Information security strategy	Business requirements governing the design, adoption, and implementation of all security policies, education, and training programs, and technological controls.	(Hong, Chi, Chao, and Tang, 2003; Vroom and Von Solms, 2004; Whitman and Mattord, 2005)
TFR – Technology in use	The routines governed by IS and how they employ to members' daily activities.	Use of information security	Daily interaction with information security artifacts through physical interaction, discussions of use, resulting outcomes conditional on, process improvements based on, and barriers presented by information security artifacts.	(Anderson, 2003; Hong, et al., 2003; Siponen, 2000; von Solms, 2000; Whitman and Mattord, 2005)
Reduced member incongruity	When process flow is not inhibited through the over application or ignorance of IS.	Reduced information security incongruity	Realignment of organizational member group perceptions of risk related to information.	(Anderson, 2003; Farahmand, Atallah, and Konsynski, 2008; Farahmand, Dark, Liles, and Sorge, 2009; Flechais and Sasse, 2009; Goodhue and Straub, 1991; Vaast, 2007)
Improved organizational effectiveness	When IS is assured and in balance.	Information security effectiveness	Cumulative effect of the relationship between information systems experience and the user experience within organizational context.	(Dunkerley and Tejay, 2009)

Table 1. Information Security Theoretical Constructs

Information security strategy implies *why* organizations implement technologies. The expectations of technology implementation, desired impact supporting organizational goals (Orlikowski and Gash, 1994), strategic partnerships, and goals are critical to business growth and viability and influence risk decisions, even at the member level.

The use of information security implies *how* organizations implement technologies such as how workers interact with technology (Orlikowski and Gash, 1994), day to day actual conditions and consequences associated with such interaction (Shaw, Lee-Partridge, and Ang, 1997), or worker views of how the technology is used (Barrett, 1999). This construct may also include process improvements (Davidson, 2002) or overcoming socio-cultural, legal, political, or implementation barriers (Sanford and Bhattacherjee, 2008).

When critical stakeholder groups have different notions of what technology is, how it should be used, and why it was implemented, the organization experiences TFR incongruity. As managers, administrators, architects, and other key actors begin to share similar concepts of how these three constructs contribute to organizational output, member incongruity is reduced.

Reduced member incongruity (RMI) ranges from personal values such as reduced skepticism (Orlikowski and Gash, 1994) to better long-term project planning (Sanford and Bhattacherjee, 2008). RMI is important because when organizational member group views become incongruent with organizational technology use, nature, or strategy, organizations experienced reduced effectiveness (Barrett, 1999), completely derailed projects (Sanford and Bhattacherjee, 2008), or other negative affects (Davidson, 2002; Lin and Cornford, 2000; Shaw, et al., 1997). Reduced member incongruity lends to a more effective organization.

Improved Organizational Effectiveness (IOE) can range from increased inter-departmental communications (Orlikowski and Gash, 1994) to derived economic benefit (Sanford and Bhattacherjee, 2008). IOE can also include enhanced user performance (Davidson, 2002), better user perception (Lin and Cornford, 2000), and improved end-user support satisfaction (Shaw, et al., 1997). Reduced information security incongruity leads to improved information security effectiveness.

Toward IOE, organizational members not only need information security awareness, but ideally should be committed to the nature, strategy, and use of information security throughout the enterprise (Siponen, 2000). As associating members build more congruent frames relating to information security, gaps created by misaligned perceptions associated with the nature of information, information security strategy, and use of information security are reduced, improving organizational information security through improved organizational effectiveness. The proposed model is illustrated in Figure 1.

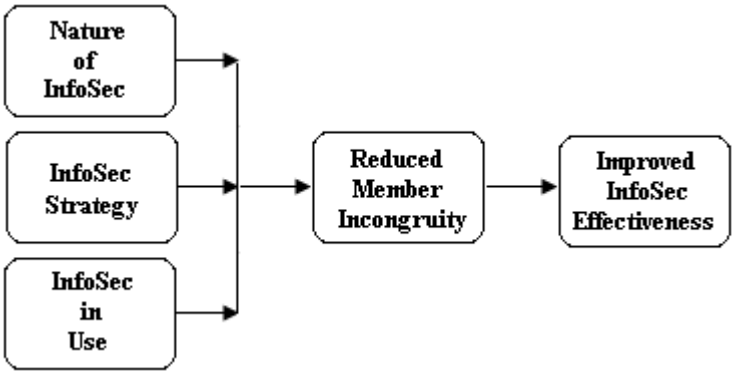

Figure 1. IS Security Frame Alignment Model

CASE FOR HEALTHCARE

Damages from patient information losses top $6 billion per year in 2010 and may exceed $450 per record (Greenberg, 2010). Administrators have to focus on reducing overhead and increasing profitability, physicians and nurses focus on increased information for diagnosis and treatment, and strategic partners must ensure 100% equipment availability, but all must be patient information stewards. Understanding this challenge, the proposed theoretical model could help healthcare organizations improve information security by reducing the incongruity of member perceptions toward information risk.

Information security perceptions

Healthcare providers demand the highest integrity of data and frequently their patients' lives depend on it. It is important for anyone interfacing with information security artifacts to understand how the artifact is supposed to function and the inherent capabilities over isolated functionality. Physicians and nurses directly interact with patients during stressful circumstances and their primary concern is patient health, not information security. However, while easier access to patient records for the staff, may also mean easier access to patient records for defalcators.

With the growing acceptance of portable computing, phones, tablets, and carts, it becomes easier to leave a device logged onto the system during procedures. This provides open access to health and possibly financial records. Imagine a staff member attending a patient when a serious injury enters the ER. The staff member immediately puts down the artifact to attend to the patient. This device is now usable by another staff member, perhaps without appropriate permissions, or, worst case, is picked up and utilized for more nefarious purposes.

An appropriate healthcare study on improving information security would detail technological use, security strategy, and nature of information security from multiple group perspectives within an organization. The research instrument based on proposed theoretical framework would allow researcher to evaluate how different organizational groups view risk to critical information and how such perspectives are formed. A subsequent comparative analysis between different group perspectives and organizational policies would highlight any incongruity with respect to information risk. Any incongruent perceptions among organizational groups can then be realigned through meaningful information security policies, security education, and awareness.

How Healthcare provider members use information systems is a critical component to organizational efficiency. If a staff member access a malicious site, or opens an infected Email, the entire hospital network may be compromised. If the hospital is inter-networked with local or national Healthcare providers, the entire network becomes at risk. If a patient logon system is used quickly to access staff schedules or individual financial data, remote access to those systems may remain active even after switching screens.

Reduced incongruity

While security education training and awareness (SETA) helps reduce obvious information risks, it does not contribute to organizational effectiveness. Since information security perceptions coalesce in groups (Vaast, 2007), understanding how each department views information security is important to reducing inherent incongruities. Aligning perspectives does not mean making them equal since each department has varying functions and expertise, it means getting each department to understand, adopt and adhere to information security activities that are aligned with organizational goals. This would empower members to make decisions that support management goals, maintain HIPAA compliance, and promote patient information security.

An appropriate healthcare study on improving information security would detail technological use, security strategy, and nature of information security from multiple group perspectives within an organization. The research instrument based on proposed theoretical framework would allow researcher to evaluate how different organizational groups view risk to critical information and how such perspectives are formed. A subsequent comparative analysis between different group perspectives and organizational policies would highlight any incongruity with respect to information risk. Any incongruent perceptions among organizational groups can then be realigned through meaningful information security policies, security education, and awareness.

CONCLUSION

We have proposed IS security frame alignment model that would improve organizational information security effectiveness. The proposed model has been discussed in the context of healthcare. Different vertical markets may be studied to determine variances in the incongruity gap. Organizations should be able to apply this model to determine incongruity of group members in comparison to organizational groups.

REFERENCES

1. Adams, A. and Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.
2. Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.
3. Barnard, L. and von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security, 19*(2), 185-194.
4. Barrett, M. I. (1999). Challenges of EDI adoption for electronic trading in the London Insurance Market. *European Journal of Information Systems, 8*(1), 1-15.
5. Baskerville, R. L. (1993). Information systems security design methods: implications for information systems development. *ACM Computer Surveys, 25*(4), 375-414.
6. Bhagyavati and Hicks, G. (2003). A basic security plan for a generic organization. *Journal of Computing Sciences in Colleges, 19*(1), 248-256.
7. Bijker, W. (1987). *The social construction of Bakelite: Toward a theory of invention*. Cambridge, MA: MIT Press.

8. Craig, J. (1993). *Developing a computer use policy at the University of California at Berkeley*. Paper presented at the Proceedings of the 21st annual ACM SIGUCCS conference on User services, San Diego, California, United States.
9. Davidson, E. J. (2002). Technology frames and framing: A socio-cognitive investigation of requirements determination. *MIS Quarterly, 26*(4), 329-358.
10. Davidson, E. J. (2006). A technological frames perspective on information technology and organizational change. *The Journal of Applied Behavioral Science, 42*(1), 23-39.
11. Dhillon, G. (1995). *Interpreting the management of information systems security.* Doctoral dissertation, London School of Economics and Political Science.
12. Dhillon, G. and Backhouse, J. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management, 16*(1), 65-74.
13. Dhillon, G. and Backhouse, J. (2000). Information system security management in the new nillennium. *Communications of the ACM, 43*(7), 125.
14. Dunkerley, K. and Tejay, G. (2009, August 6th-9th). *Developing an Information Systems Security Success Model for eGovernment Context.* Paper presented at the Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, CA.
15. Farahmand, F., Atallah, M., and Konsynski, B. (2008). *Incentives and perceptions of information security risks.* Paper presented at the Twenty Ninth International Conference on Information Systems, Paris, France.
16. Farahmand, F., Dark, M., Liles, S., and Sorge, B. (2009). *Risk perceptions of information security: A measurement study*. Paper presented at the 2009 International Conference on Computational Science and Engineering, Vancouver, Canada.
17. Farahmand, F., Navathe, S. B., Enslow, P. H., and Sharp, G. P. (2003). *Managing vulnerabilities of information systems to security incidents*. Paper presented at the Proceedings of the 5th international conference on Electronic commerce, Pittsburgh, Pennsylvania.
18. Flechais, I. and Sasse, M. A. (2009). Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science. *International Journal of Human-Computer Studies, 67*(4), 281-296.
19. 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*(1), 13-27.
20. Greenberg, A. (2010). Data Spills Cost U.S. Hospitals $6 Billion a Year. *The Firewall*. Retrieved from http://blogs.forbes.com/andygreenberg/2010/11/08/data-spills-cost-u-s-hospitals-6-billion-a-year
21. Hazari, S., Hargrave, W., and Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy & Security, 4*(4), 3-20.
22. Hong, K., Chi, Y., Chao, L., and Tang, J. (2003). An integrated system theory of information security management. *Information Management and Computer Security, 11*, 243-248.
23. Jones, A. K. and Lipton, R. J. (1975). *The enforcement of security policies for computation*. Paper presented at the Proceedings of the fifth ACM symposium on Operating systems principles, Austin, Texas, United States.
24. Liebenau, J. and Backhouse, J. (1990). *Understanding information: an introduction*. London: Palgrave Macmillan.
25. Lin, A. and Cornford, T. (2000). *Framing implementation management*. Paper presented at the Proceedings of the twenty first international conference on information systems, Brisbane, Queensland, Australia.
26. Orlikowski, W. J. and Gash, D. C. (1994). Technological frames: making sense of information technology in organizations. *ACM Transactions on Information Systems, 12*(2), 174-208.
27. Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal, 42*(6), 32-34,36-38.
28. Sanford, C. and Bhattacherjee, A. (2008). IT implementation in a developing country municipality: A sociocognitive analysis. *International Journal of Technology and Human Interaction, 4*(3), 68-93.
29. Shaw, N. C., Lee-Partridge, J. E., and Ang, J. S. K. (1997). *Understanding end-user computing through technological frames*. Paper presented at the Proceedings of the eighteenth international conference on Information systems, Atlanta, Georgia, United States.
30. Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31.
31. Vaast, E. (2007). Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare. *The Journal of Strategic Information Systems, 16*(2), 130-152.
32. von Solms, B. (2000). Information security -- The third wave? *Computers & Security, 19*(7), 615-620.
33. Vroom, C. and Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.
34. Whitman, M. and Mattord, H. (2005). *Principles of information security*. Boston: Course Technology.