CYBERSECURITY PERSPECTIVES

TOWARD AN IMPROVED BUSINESS INFORMATION SECURITY POSTURE

Derek J. Sedlack, Ph.D.

Paper 3 | October 2019

Suggested Citation:

Sedlack, D.J. (2019). Toward an Improved Business Information Security Posture. *AICL Cybersecurity Perspectives*, Paper 3, accessed on October 28, 2019, https://www.americascyber.org/cyberperspectives.

ABSTRACT

Information-age businesses continue to experience data loss. While technical controls provide some security against illicit activity, a more robust, organizationally focused information security method should be understood and applied to losses from computer security incidents. This paper focuses on how information is defined organizationally to understand the information security gaps created by incongruent member perceptions related to information risk among different stakeholder communities. It is argued that member perception incongruity reduction will improve organizational information security effectiveness.

1. INTRODUCTION

The expected outcome from this paper is to investigate information risks within organizations containing formalized groups and/or divisions. As most organizations grow, distinct functional groups are formed to improve efficiencies and effectiveness, but lack interdepartmental communications directly relating to information risk. This research poses inquiries about certain group perspectives that would reduce an information secure posture to impact exposure to malware or ransomware.

While it is understood that organizations change over time and successful organizations may experience rapid change, the reduction of an information security posture risk might result from the assignment of unqualified personnel due to hiring challenges or convenience. Additionally, purchasing equipment due to industry expectations, tradition, or to accommodate technological gaps occur frequently due to the high-speed nature of modern business. The concern is that short-term technological decisions based on budgeting or project deadlines may irreparably compromise organizational infrastructure to allow undiscoverable entry externally and internally. This work seeks to explore organizational characteristics which could influence the potential for reducing an organization's exposure to information risk.

Information security research traditionally focused on purely technical solutions that have proven less effective (Baskerville, 1993; Bhagyavati and Hicks, 2003; Dhillon, 1995; Dhillon and Backhouse, 1996; Farahmand et al., 2003; Liebenau and Backhouse, 1990). Even with increasingly sophisticated technology and user training, users continue to be the weakest link in the information security chain (Whitman and Mattord, 2005), partially due to mandated employee use of technologies for which appropriate training is ignored or employees are not even interested in (Hazari et al., 2008). More users are becoming accustomed to business information use; however, this leads to systemic problem ignorance regardless their severity (Vaast, 2007). Even institutions like the DoD, believed to be the most secure, experience breaches (Bull and Finkle, 2013). It is becoming increasingly important for organizations to adopt a formal information risk perception alignment model to reduce information security gaps and improve organizational effectiveness.

2. THEORETICAL FOUNDATIONS

Perceptions of organizational members are formed related to information risk based on personal experience (Bijker, 1987), interacting with information security artifacts (Vaast, 2007), and from within organizational groups sharing similar perceptions (Orlikowski and Gash, 1994). Organizations are less likely to publicize, let alone involve external resources relating to information security due to regulatory compliance (Waxer, 2006), a noteworthy lack of faith in law enforcement efforts (Richardson, 2008), negative impacts to organizational perceived capabilities (Zhou and Johnson, 2009) or investor concerns. Incongruent perceptions exist in dynamic environments (Giddens, 1984) commonly associated with businesses in the information age and significant research gaps exist regarding strategic information risk alignment. These inflexible attitudes toward revealing quantitative information security-related data means using a qualitative research approach.

Many researchers applied qualitative methods in attempt to align technological user and management perspectives in use (Shaw et al., 1997), purchasing (Davidson, 2002), communication (Orlikowski and Gash, 1994), and integration (Lin and Cornford, 2000; Yoshioka et al., 2002). Some identified critical incongruities were political (Sanford and Bhattacherjee, 2008), power-based (Barrett, 1999; Dunkerley and Tejay, 2009), or influences (Ovaska, et al., 2005). While recent studies have turned their attention toward technological alignment, the study perceptions relating to information risk from an organization's strategy. This study applied dialogical action research through technological frames of reference in a multi-billion dollar private company in the Southeastern United States. Accepted data collection methods included direct interactions between researcher and practitioner through observations (Sekaran, 2003), one-on-one dialog (Sekaran) from semi-structured interview questions (Denzin and Lincoln, 2005), and organizational charts and procedures (Baskerville, 1999). Informal interactions reduce participant inhibitions regarding confidential or sensitive matters (Mårtensson and Lee, 2004).

3. PROPOSED MODEL

From the proposed model of reduced information risk gaps, the research considers group dynamics that likely affect reduced information security postures. The proposed model accounts for information system controls that are technical, formal, and informal (Backhouse and Dhillon, 1996), and attempts to categorize incongruent risk perceptions within each edifice to formulate an information security posture more aligned with long-term organizational goals.

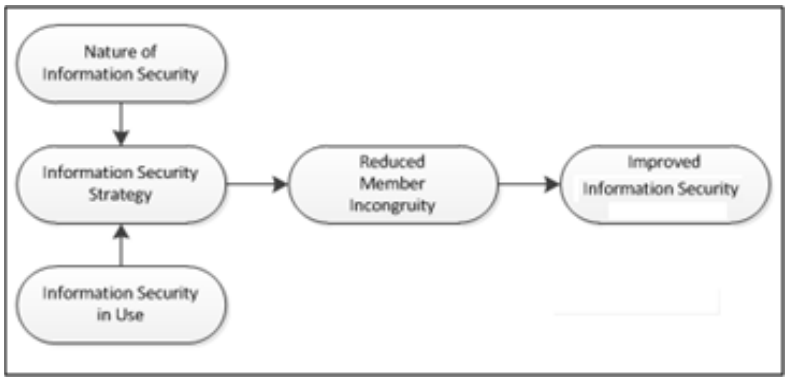

Figure 1. Information security improvement model.

In this proposed model of reduced information risk incongruity, see Figure 1, we considered personal characteristics that would impact group perceptions to influence strategic misalignment. The model accounted for personal and professional interaction with security-related technology and related personal perceptions. Preliminary investigations through technological frames of reference (TFR) explored employee perceptions of technology in use, technical capabilities, and purpose of implementation. Early TFR indications suggested the equally poignant constructs of uses, capabilities, and strategy relating to information security; however, a better model was obtained through the direct application during an enterprise project with a focus on information security through pervasive technology.

While literature supports project size relating to project success (McFarlan, 1981; Nelson and Ravichandran, 2004), research through information security literature does not indicate such a correlation from a project or organizational perspective. In fact, data breaches at Target, TJMaxx, and Sony, along with ransomware victims Methodist Hospital and Hollywood Presbyterian Medical Center (Pagliery, 2016), would indicate they are higher targets, increasing the likelihood for failure. In each information security failure, employees failed to properly identify and assess risks resulting in data and ultimately significant financial loss. This research suggests a model that would have provided a tool for management and users alike to better understand and measure the consequence of actions preceding each failure.

4. RESEARCH QUESTIONS

Group representations were considered through social representation theory (Moscivici, 1981) given related published information systems research (Vaast et al., 2006; Vaast, 2007); however, the framing element of group representations (Vaast and Walsham, 2005) does not lend to the inherent social elements of social representation. This research aims to understand group dynamics that contribute to information security gaps were better served through TFR and produced an improved related model.

The first research question asked how incongruent risk perceptions related to individual members are formed. Structuration theory (Giddens, 1984) suggests that dynamic environments create individual perceptions relative to that environment. Each organizational member identifies and evaluates information risk individually unless otherwise trained or conditioned. One employee becomes accustomed to receiving Email attachments at work and understands them to be equally beneficial and benign (Pagliery). Members with computer-related academic training might understand business and personal Email attachments to be independent and evaluated separately. While members of professional organizations focused on information security, like ISACA, should access each attachment, even internal communications with attentiveness and even suspicion.

The second research question asked if individual member risk perception contributes to the community. Community in this study meant business group or division. Some research suggests that risk perception derives from demographics (Liang and Xue, 2009) while others found job-related tasks highly influential in risk perception formation (Choi et al., 2008). Davidson and Chismar (2007) suggest that as companies integrate more technology to control and manage data, organizations must consider that technology to be as vital to organizational output as the traditional pen and paper. When employees are exposed to and rely upon information security artifacts throughout daily task completion, it is expected they understand or even master tool use. The best designed tools are those users want to share and even train others to use. It may seem unrealistic to expect modern business workers to become experts in technology and/or information risk management, but data breaches are occurring because those workers are not even properly trained. Improperly trained workers share their tool use and understanding with other ignorant workers, posing a significant organizational risk despite fortunes spent on technical solutions.

The third research question asked if interaction with artifacts can impact the strategic alignment of risk perceptions. Deterrence measures are an accepted form of information security; however, this study focused on security education, training, and awareness (SETA) as the focal point of employee empowerment given the proliferation of deterrents and continued reporting of data breaches. While researchers agree that SETA are a critical foundation toward adequate information assurance (Choi et al., 2008; Roper, et al., 2006; Siponen, 2001) not enough organizations provide programs with adequate dedicated resources (Tarna et al., 2008). Those that do educate and train have to find the balance between too much training that will desensitize (Adams and Sasse, 1999) or too little training employees forget about. Given distinct differences commonly found between organizational layers (McGovern and Hicks, 2004), it would be three times as expensive to produce functional SETA programs for executives, middle managers, and the workers, ignoring the individual learning modalities of auditory, visual, and kinesthetic. Vasst (2007) posited that users increasingly accustomed to information technology tend to ignore systemic issues and Johnston, Wech, Jack, and Beavers (2010) suggest external cues to

influence awareness, but employees that specialize in information risk fields (security auditing, secure programming design, CISO, etc) are more attuned to systemic anomalies that commonly produce the gaps exploited by hackers.

5. CONCLUSION

As modern business designs further consolidate (through growth and M&A), the progression toward centralization seems obvious and appears supported by the notion of strategic alignment. This would appear supported by a reduction in corporate duplication across most departments to improve costs and efficiency. The strategic alignment of structure would also seem to follow this notion of centralized information security; however, Giddens (1984) found the constructs of human behavior represented in the notion of structure as abstract and as malleable, like corporate policies or government compliance standards. The critical element in this research is not to find a solution to corporate design, but a useful construct toward implementing a universal information security perspective that aligns and intersects divisions and hierarchies with a unified approach toward a stronger security posture. Centralized or decentralized, small or enterprise, the business unit framework is not abstract through which we should align, but that which we should understand only to apply our strategic designs relating to technical, formal, and informal outcomes and objectives. As we consider how to interact and with what we should interact in technological implementations, the overall focus and demand should remain a unifying feature of the corporate design: information security strategy.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46. doi: 10.1145/322796.322806

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

Barnard, L., & von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. *Computers & Security, 19*(2), 185-194.

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. doi: Document ID: 40032383

Baskerville, R. L. (1993). Information systems security design methods: implications for information systems development. *ACM Computer Surveys, 25*(4), 375-414. doi: 10.1145/162124.162127

Bettman, J. R. (1973). Perceived risk and its components: A model and empirical test. *Journal of Marketing Research, 10*(2), 184.

BGH (2011). Privacy & Security. Retrieved from http://www.massgeneral.org/notices/privacy.

Bhagyavati, & Hicks, G. (2003). A basic security plan for a generic organization. *Journal of Computing Sciences in Colleges, 19*(1), 248-256.

Bijker, W. (1987). *The social construction of Bakelite: Toward a theory of invention*. Cambridge, MA: MIT Press.

Bull, A., & Finkle, J. (2013). Fed says internal site breached by hackers, no critical functions affected. Retrieved from http://www.reuters.com/article/2013/02/06/net-us-usa-fed-hackers-idUSBRE91501920130206.

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.

Davidson, E. J. (2002). Technology frames and framing: A socio-cognitive investigation of requirements determination. *MIS Quarterly, 26*(4), 329-358. doi: Document ID: 275116671

Davidson, E. J. (2006). A technological frames perspective on information technology and organizational change. *The Journal of Applied Behavioral Science, 42*(1), 23-39. doi: 993103771

Dhillon, G. (1995). *Interpreting the management of information systems security.* Doctoral dissertation, London School of Economics and Political Science.

Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within

organizations. *International Journal of Information Management, 16*(1), 65-74.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new nillennium. *Communications of the ACM, 43*(7), 125.

Dunkerley, K., & 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.

Dvorak, K. (2016 Feb). *California Hospital Pays Hackers $17K After Ransomware Attack*. FierceHealthIT. Retrieved from http://www.fiercehealthit.com/story/california-hospital-pays-hackers-17k-after-ransomware-attack/2016-02-18.

Farahmand, F., Atallah, M., & Konsynski, B. (2008). *Incentives and perceptions of information security risks.* Paper presented at the Twenty Ninth International Conference on Information Systems, Paris, France.

Farahmand, F., Dark, M., Liles, S., & 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.

Farahmand, F., Navathe, S. B., Enslow, P. H., & 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.

Flechais, I., & 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.

Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration*. Univ of California Press.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27. doi: 10.1016/0378-7206(91)90024-v

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/?boxes=Homepagechannels

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy & Security, 4*(4), 3-20.

HHS (2011). Resolution Agreement. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralracap.pdf.

Hong, K., Chi, Y., Chao, L., & Tang, J. (2003). An integrated system theory of information security management. *Information Management and Computer Security, 11*, 243-248.

Johnston, A., Wech, B., Jack, E., & Beavers, M. (2010). Reigning in the remote employee: Applying social learning theory to explain information security policy compliance attitudes. *AMCIS*

2010 Proceedings, Paper 493.

Jones, A. K., & 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.

Liebenau, J., & Backhouse, J. (1990). *Understanding information: an introduction*. London: Palgrave Macmillan.

Lin, A., & Cornford, T. (2000). *Framing implementation management*. Paper presented at the Proceedings of the twenty first international conference on information systems, Brisbane, Queensland, Australia.

Mårtensson, P., & Lee, A. S. (2004). Dialogical action research at Omega corporation. *MIS Quarterly, 28*(3), 507-536.

McFarlan, F. W. (1981). Portfolio Approach to Information Systems. *Harvard Business Review 59*(5), 142-150.

Moscivici, S. (1981). *On social representation*. The Hague: Nijhoff.

Nelson, M. and Ravichandran, T. (2004). Repeating Failure in Large-scale Government IT Projects: A Taxing Story. *Proceedings of the Tenth Americas Conference on Information Systems*, New York, New York.

Nonaka, I. (1988). The knowledge-creating company. In Harvard Business Review on knowledge management. Boston: Harvard Business School Press.

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. New York: Oxford University Press.

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: making sense of information technology in organizations. *ACM Transactions on Information Systems, 12*(2), 174-208.

Pagliery, J. (2016). U.S. hospitals are getting hit by hackers. *CNN Money*. Retrieved from http://money.cnn.com/2016/03/23/technology/hospital-ransomware/index.html.

Roper, C., Grau, J., & Fischer, L. (2006). *Security education, awareness, and training: From theory to practice*. Burlington, MA: Butterworth-Heinemann.

Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal, 42*(6), 32-34,36-38. doi: 1601672801

Sanford, C., & Bhattacherjee, A. (2008). IT implementation in a developing country municipality: A sociocognitive analysis. *International Journal of Technology and Human Interaction, 4*(3), 68-93. doi: Document ID: 1486559821

Sedlack, D. J. (2012). *Reducing incongruity of perceptions related to information risk: Dialogical action research in organizations*. (Nova Southeastern University). P*roQuest Dissertations and Theses*, 178.

Sekaran, U. (2003). *Research methods for business. A skill-building approach* (4th ed.). New York: John Wiley & Sons, Inc.

Shaw, N. C., Lee-Partridge, J. E., & 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.

Siponen, M. T. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society, 31*(2), 24-29.

Tarna, J., Nelson, S., & Razia, M. (2008). Exploring wireless campus security and legality. *The XVIII ACME Internation Conference on Pacific Rim Management*, (pp. 70-75), Toronto, Ontario, Canada.

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.

Vaast, E., & Walsham, G. (2005). Representations and actions: the transformation of work practices with IT use. *Information and Organization, 15*(1), 65-89.

von Solms, B. (2000). Information security -- The third wave? *Computers & Security, 19*(7), 615-620.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Whitman, M., & Mattord, H. (2005). *Principles of information security*. Boston: Course Technology.

AUTHOR BIOGRAPHY

Dr. Derek Sedlack is a published author, patented inventor, and distinguished international lecturer in the areas of Cybersecurity, Risk Management, and Enterprise Integration Engineering. For more than 20 years, Dr. Sedlack held business positions with escalating privileges that integrated software engineering solutions for many of the Fortune 100 companies like: Boeing, AT&T, Dayton Hudson Corporation (Target), Sony, Carrier, and Ford Motor Co. Dr. Sedlack designed software engineering solutions that focused on efficiency for IBM, HP, and Dell led to multiple patent designs (awarded by the US P&TO) generating millions in revenue and reducing either manual labor or human error.

As CIO of an established Virginia federal contracting company, Dr. Sedlack researched, wrote, and managed multi-million dollar contracts that included partnerships with NASA (JPL), multiple NCAA Universities, and specialized research organizations to enhance space travel and combat global pollution. As CTO with a national mortgage company, Dr. Sedlack redesigned the IT architecture to reduce Cyber threats coming from China and Romania, and improved the efficiency of VoIP by more than 260% in a short duration of time.

Dr. Sedlack holds an appointment as Lead Faculty and Associate Professor at Colorado Technical University, Colorado. He has consulted 4-star General Wolter's Staff for the United States Air Force Allied Command in Europe and Africa on topics of behavioral and organizational security, distinguished speaker for The Armed Forces Communications and Electronics Association in Germany, and been invited speaker as enterprise integration consultant. For 3 years in a row, Dr. Sedlack was invited as Visiting Professor to the Technical University of Kaiserslautern (Germany) to teach graduate courses on information security with a focus on risk management to computer science, engineering, and robotics students.