Information Systems Security Leadership: An Empirical Study of Behavioral Influences

Emergent Research Forum (ERF) Papers

Marcus Winkfield
College of Engineering and Computing
Nova Southeastern University
Fort Lauderdale, FL, USA
mw1558@nova.edu

James Parrish
College of Engineering and Computing
Nova Southeastern University
Fort Lauderdale, FL, USA
jlparrish@nova.edu

Gurvirender Tejay
Gus Machado School of Business
St. Thomas University
Miami, FL, USA
gtejay@stu.edu

Abstract

Information Systems Security Leadership (ISSL) uses leadership concepts in the field of information systems (IS) security. Despite the adoption of technical and managerial approaches, organizations still face issues motivating employee security compliance. In this paper, we argue organizations need strong leadership to encourage employees. Using the expectancy theory, we created a theoretical model to help understand the influence of leadership behaviors on non-technical controls IS security controls. Our research in progress is expected to contribute a model for future research in the field of IS security, as well as promote organizations to integrate leadership concepts into their IS security programs.

Keywords

Security, leadership, compliance, control, administrative, behavioral, risk management, expectancy theory

Introduction

The behavioral influences of information systems (IS) security[1] leaders can motivate employees' security compliance. According to Barton et al. (2016), "IS security is a well-informed sense of assurance that risks to information resources are in balance with technical, administrative, and behavioral controls[2]" (p. 9). IS security controls are technical and non-technical measures that are established, implemented, operated, monitored, reviewed, maintained, and improved to ensure the confidentiality, integrity, and availability of organizational information resources (Montesino et al. 2012).

We argue organizations need strong leadership behaviors to encourage employees to adhere with non-technical controls. According to Dunkerley and Tejay (2009), "organizations will require strong leadership that understands how to define information security success within that organization's context, necessitating individuals who understand both information security needs of the organization (p. 5). Research suggests a lack of leadership can have a negative effect on IS compliance (Furnell and Thomson

[1] For the remainder of this paper, security and IS security are used interchangeably.

[2] National Institute of Standards and Technology (NIST) provides three similar classes of security controls: technical, management, and operational.

[3] This study focuses on security compliance with non-technical controls to help organizations mature past a high-reliance on technical controls.

[4] NIST 800-37 also known as RMF was selected because it is widely used by diverse organizations. Although RMF is primarily used for IS security in the United States federal government, NIST publications are also used to develop private sector security programs.

2009, because leadership influences organizational performance (Wang et al. 2011). Unfortunately, IS researchers argue there is a major void in the theoretical and practical understanding of the role of leaders in IS security (Hu et al. 2012). The research problem calls for empirical research to further understand the behavioral influences of leaders on employees' IS security compliance.

In this study, the goal is to tackle the central research question that has not been adequately investigated in IS literature: (1) *What is the influence of leadership behaviors on IS security compliance?* The central research question is then divided into three sub-questions: (1.1) *What leadership behaviors motivate employees to comply with administrative security controls?* (1.2) *What leadership behaviors motivate employees to comply with behavioral security controls?* (1.3) *What leadership behaviors do employees perceive are most prevalent in their organization?* This study utilizes perceptions of how employees view their leader's behaviors when making compliance decisions to address three research questions.

IS Security Compliance and Leadership

Leadership

Although there is no agreed upon definition of leadership, this study defines leadership as: "a process whereby an individual influences a group of individuals to achieve a common goal" (Northouse 2016, p. 6). Leadership motivates intrinsically by satisfying very basic human needs (Kotter 1990). There are two fundamental topics in leadership: are leaders born or made (Marques 2010). In earlier research, it was believed leaders were born with certain unique traits and skills—The Great Man Theory. While the trait approach determines leadership potential based on the characteristics of a person (i.e. intelligence, height, etc.), the skill approach refers to an individual's competency to perform tasks well (i.e. communication, problem solving, etc.) (Northouse 2016). Instead of being born a leader, other studies have focused on how behavioral approaches can make a leader (Northouse 2016).

IS Security Compliance

Security violations are a breach of compliance, which can be defined as "any act by an employee using computers that is against the established rules and policies of an organization for personal gain" (Hu et al. 2011, p. 54). Boss et al. (2009) aimed to understand how organizations could motivate security compliance, and found the act of specifying policies and evaluating behaviors are effective in motivating individuals because policies are viewed as mandatory. However, this is a major assumption, even when policies are specified as mandatory they may still not be followed. In addition, Boss et al. (2009) also found rewards are not a significant factor in influencing compliance through the perception of mandatoriness. Siponen et al. (2010) also found rewards to be negatively associated with security compliance. These research findings suggest a need to look beyond the use of rewards. Vance et al. (2012) argued security non-compliance issues are often caused by habit, which means individuals are caught in routine behavior that goes against security policies. But, bad habits are hard to break.

This introduces the need for organizations to have deterrence mechanisms in place to change the habitual behaviors of users. Deterrence mechanisms are highly relied upon to encourage security compliance. Johnston et al. (2015) highlighted the importance of incorporating fear-inducing communication to persuade end-users intentions to follow recommended individual security actions. Johnston et al. (2015) version of the fear appeals model extended the conventional fear appeal model by adding personal relevance with sanctions. There should also be personal relevance with sanctions for deterrence mechanisms to be effective because employees with preconventional moral reasoning make decisions based on personal interest to avoid sanctions (Myyry et al. 2009). Additionally, users apply neutralization techniques and rationalize their workplace behavior violating security polices (Siponen and Vance 2010). In short, deterrence based approaches alone will often fail (Hu et al. 2011).

The weaknesses in deterrence mechanisms suggest a need for intrinsic forms of security compliance (Son 2011), such as: socialization, influence, beliefs and cognition (Ifinedo 2014) or personality factors (Shropshire et al. 2015). Herath and Rao (2009) emphasized the importance of extrinsic and intrinsic motivators to encourage security compliance; however, Son (2011) observed although extrinsic factors are important, intrinsic factors have an increased chance of motivating security compliance. An intrinsic

approach would likely be more successful because individuals are rationally influenced to comply with security policies based on normative beliefs, self-efficacy, and attitudes (Bulgurcu et al. 2010). The perceived benefit often overshadows the perceived risk during the process of rationally calculating security compliance, which introduces a need to examine intrinsic factors such as self-control and moral beliefs (Hu et al. 2011). This approach requires strong awareness programs. Without user awareness, all other measures will likely fall short (Siponen and Kajava 1998); it is important for user's education and training to develop intrinsic motivation to encourage security compliance (Siponen 2000). More advanced awareness programs are necessary for computer savy employees who may believe they can subvert controls (D'Arcy and Hovav 2009). To sum it up, security compliance is a complex issue that requires numerous non-technical considerations to be effective.

Theoretical Foundation

Victor Vroom's (1964) argues individuals behave in a specific manner because they are motivated to choose a distinct behavior over other behaviors based on what they expect the outcome will be (Vroom 1995). Expectancy is the belief that one's effort will result in the attainment of desired performance goals; instrumentality is the belief that a person will receive a reward if the performance expectation is achieved; and valence is the extent to which a person values a given outcome or reward (Vroom 1995). The expectancy theory has several basic assumptions: "(1) a subjective measure of expectancy; (2) independence between expectancies and valences; (3) a multiplicative interaction between expectancies and valences; (4) instrumentality as a determinant of valence" (Reinharth and Wahba 1975, p. 522).

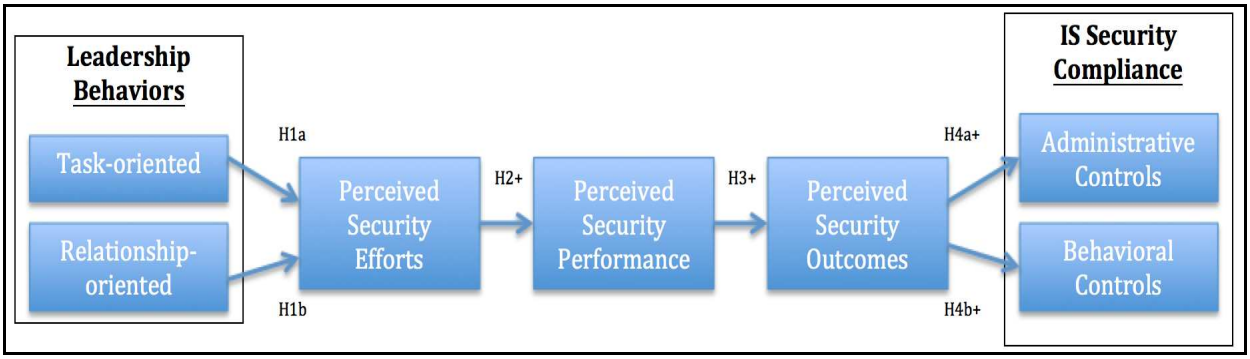

Figure 1: Preliminary Theoretical Model

The expectancy theory is considered a good fit for understanding individual behaviors and work performances (Vroom 1995). However, the expectancy theory has not been used to understand behaviors of leaders that motivate IS security compliance. Since an employee's IS security compliance is part of their work performance, the expectancy theory is appropriate to understand the behavioral influences of leaders that motivate IS security compliance with non-technical controls.

The behavioral approach to leadership focuses on "what leaders do and how they act," and there are two general types of behavior: those focused on accomplishing tasks, as well as others focused on building relationships (Northouse 2016, p. 71). Leadership behaviors have been found to influence organizational security outcomes (Flores and Ekstedt 2016).

H1a: Task-oriented leadership behaviors will have an influence on perceived security efforts.
H1b: Relationship-oriented leadership behaviors will have an influence on perceived security efforts.
H2: Perceived security efforts will have a positive influence on perceived security performance.
H3: Perceived security performance will have a positive influence on perceived security outcomes.
H4a: Perceived security outcomes will have a positive influence on employee compliance with administrative controls.
H4b: Perceived security outcomes will have a positive influence on employee compliance with behavioral controls.

Research Plan

We will conduct our study in Fall 2017 in the Washington District of Columbia (DC) metropolitan area using an electronic survey. Risk Management Framework (RMF) non-technical security controls and concepts from leadership research will be used to develop a survey instrument. The plan is to survey employees of large organizations with established IS security programs using hypothetical scenarios to reveal what behavioral influences motivate participants to comply. Additionally, we will survey participants to discover leadership behaviors perceived most prevalent in their organization. Business cards with a web link and information about the study will be passed out at local security events. Prospective participant's email address will be obtained to track individual completions and provide a reminder if necessary.

Administrative Security Control Compliance

Administrative security controls refer to policies and procedures aimed at securing the IS environment (Talib et al. 2012). Administrative security controls are how management outlines the responsibility and control of systems in their organization. For instance, an administrative security control is an acceptable use policy, which aims to reduce the risk associate with the misuse of systems in the organization.

Behavioral Security Control Compliance

Behavioral security controls refer to deterrents or penalties and pressures to ensure policies influence the intentions of users (Hazari 2008). Behavioral security controls attempt to reinforce the usefulness of policies and procedures. Personnel sanction is an example of a behavioral control.

Conclusion

This study takes a slightly different approach from existing security compliance research by using the expectancy theory to understand the influence of leadership behaviors from the perspective of employees. Results from this study will help identify the usefulness of the expectancy theory for understanding leadership behaviors in IS security. Our research in progress is expected to contribute a leadership model for future research in the field of IS security, as well as promote organizations to integrate leadership concepts into their IS security programs.

REFERENCES

Barton, K. A., Tejay, G., Lane, M., and Terrell, S. 2016. "Information System Security Commitment: A Study of External Influences on Senior Management," *Computers & Security* (59), pp. 9-25.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone is Watching, I'll do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

D'Arcy, J., and Hovav, A. 2009. "Does One Size Sit all? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics* (89:1), pp59-71.

Dunkerly, K., and Tejay, G. 2009. "Developing an Information Systems Security Success Model for eGovernment Context," *in AMCIS 2009 Proceedings*. Retrieved from http://aisel.aisnet.org /amcis2009/346/

Flores, W. R., and Ekstedt, M. 2016. "Shaping Intention to Resist Social Engineering Through Transformational Leadership, Information Security Culture and Awareness," *Computers & Security* (59) pp. 26-44.

Furnell, S., and Thomson, K. L. 2009. "From Culture to Disobedience: Recognising the Varying User Acceptance of IT Security," *Computer Fraud & Security* (2), pp. 5-10.

Hazari, S., Hargrave, W., and Clenney, B. 2008. "An Empirical Investigation of Factors Influencing Information Security Behavior," *Journal of Information Privacy and Security* (4:4), pp. 3-20.

Herath, T., and Rao, H. R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), pp. 54-60.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences* (43:4), pp. 615-660.

Ifinedo, P. 2014. "Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition," *Information & Management* (51:1), pp. 69-79.

Johnston, A. C., Warkentin, M., and Siponen, M. T. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Kotter, J. P. 1990. *Force for Change: How Leadership Differs From Management*, New York, NY: Simon and Schuster.

Marques, J. F. 2010. "Awakened Leaders: Born or Made?," *Leadership & Organization Development Journal* (31:4), pp. 307-323.

Montesino, R., Fenz, S., and Baluja, W. 2012. "SIEM-based Framework for Security Controls Automation," *Information Management & Computer Security* (20:4), pp. 248-263.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Northouse, P. G. 2016. *Leadership: Theory and Practice*, Thousand Oaks, CA: Sage publications.

Reinharth, L., and Wahba, M. A. 1975. "Expectancy Theory as a Predictor of Work Motivation, Effort Expenditure, and Job Performance," *Academy of Management Journal* (18:3), pp. 520-537.

Shropshire, J., Warkentin, M., and Sharma, S. 2015. "Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior," *Computers & Security* (49), pp. 177-191.

Siponen, M. T., and Kajava, J. 1998. "Ontology of Organizational IT Security Awareness-From Theoretical Foundations to Practical Framework," *in WET ICE 1998 Proceedings*. Retrieved from http://ieeexplore.ieee.org/document/725713/

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

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2), pp. 64-71.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Son, J. Y. (2011). "Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies," *Information & Management* (48:7), pp. 296-302.

Talib, M. A., El Barachi, M., Khelif, A., and Ormandjieva, O. 2012. "Guide to ISO 27001: UAE Case Study," *Issues in Informing Science and Information Technology* (7), pp. 331-349.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS Security Compliance: Insights From Habit and Protection Motivation Theory," *Information & Management* (49:3), pp. 190-198.

Vroom, V. (1995). *Work and Motivation*, New York, NY: John Wiley.

Wang, H., Tsui, A. S., and Xin, K. R. 2011. "CEO Leadership Behaviors, Organizational Performance, and Employees' Attitudes," *The Leadership Quarterly* (22:1), pp. 92-105.