Beyond Compliance: Empowering Employees' Extra-Role Security Behaviors in Dynamic Environments

Emergent Research Forum Paper

Yaojie Li
Louisiana Tech University
yli018@latech.edu

Tom Stafford
Louisiana Tech University
stafford@latech.edu

Bryan Fuller
Louisiana Tech University
bfuller@latech.edu

Selwyn Ellis
Louisiana Tech University
ellis@latech.edu

Abstract

Information security policies are used to guide employees in order to ensure information security while utilizing organizational information systems in the workplace. However, relatively rigid ISP compliance may not help employees and companies to confront emerging threats in the dynamic environment of modern security threats. Information Security Policies should be developed and improved according to the demands of implementers and in keeping with the changing security environment. To that end, we propose that employees' extra-role behaviors – actions that may seem to go beyond requirements and limitations of security policies – can provide input into forming suitable and feasible security policies that provide insights against the emerging threats in the operating environment.

Keywords

IS security, behavioral security, information security policy compliance, extra-role behaviors, empowerment theory, security cognitive engagement.

Introduction

Employees continue to be considered the weakest link in the security chain of organizational information systems (Bulgurcu et al. 2010a; Crossler et al. 2013; Warkentin and Willison 2009). Consequently, information security policy (ISP) compliance, which we define as "in-role behaviors," has received much notice in recent studies (e.g., Bulgurcu et al. 2010a; Herath and Rao 2009), whereas research on behaviors not specifically addressed in security policies which we term security-related "extra-role behaviors," has not seen nearly as much attention (Hsu et al. 2015). These can reprenset non-malicious behaviors that are not covered by the ISP.

ISP compliance involves employee adherence to security guidelines related to information systems use in the course of performing their jobs (Whitman et al. 2001). Employees are required to conform to a list of expected behaviors and to adapt their working styles to align with those expectations expressed in organizational security guidelines (Katz 1964; Pahnila et al. 2007). In applying precepts of person-environment fit (Ayyagari et al. 2011) we can attribute potential defects of ISP compliance to two disequilibrium relationships: that which exists between (1) ISP requirements and employees' security knowledge and expertise, and (2) the lack of fit between security environment demands and the ISP quality (Bulgurcu et al. 2010b).

Extra-Role Behaviors – Above and Beyond the Security Policy

The notion of extra-role behaviors in regard to security policy compliance has been raised in the literature (Hsu et al. 2015); it is a concept that is similar to non-malicious policy non-compliance (e.g., Colvin,

2016). However, the approach of extra-role behaviors has to do with helping *coworkers*, whereas non-malicious non-compliance is oriented toward the inherent inclinations of individual employees as regards their own on-the-job behavior. Notwithstanding, a multi-dimensional typology of extra-role behaviors in the security context has not yet been developed. Toward that end, a key goal of this paper is to develop an Extra-Role Security Behavior framework (ESB) based on the Van Dyne et al. (1995) two-dimensional typology, which orients around dimensions of affiliative/challenging (interpersonal and cooperative vs. change oriented) and promotive/prohibitive (proactive change vs. protective support). We define ESBs as security behaviors which protect organizational information and information systems, but which are discretionary and not specifically listed in the security polices of the firm. ESBs are conceptually similar to organizational citizenship behaviors (Smith et al. 1983), but are operationally distinct, arising from a sense of empowerment (Spreitzer 1995) rather than notions of altruism, as is the case with organizational citizenship (Smith et al. 1983). ESBs go beyond existing and explicit security-related role expectations, and they are expected to reduce disequilibrium with security policies in dynamic environments by enhancing employee actions beyond the boundaries of the ISP in support of secure technology use. Van Dyne and colleagues (1995; 1998) specify four implications for extra-role behaviors: (1) voluntary action; (2) intentional behavior; (3) intended for positive outcomes (even if "reporting"); and, (4) disinterested from the perspective of the employee.

As shown in Table 1, a key example of extra-role behavior is "Helping," which represents the convergence of the Affiliative dimension (interpersonal cooperation) with the promotive dimension (proactive assistance) and which results in a construct which can be characterized as emphasizing small acts in support of the work of others (Van Dyne and LePine 1998). This could be construed as informal assistance in work performance, such as tips for how to use a specific security system or informal guidance about security policies. Another important ESB is "Stewardship," which – as an Affiliative approach (i.e., social) – is aimed at prohibitive influence against inappropriate activities (e.g., protection-oriented) and is very much about friendly cautions to colleagues regarding potential pitfalls to avoid; this is best envisioned as "words to the wise" about appropriate security behaviors informally conveyed between colleagues. "Voice" is the ESB that proactively expresses ideas that are change-oriented, representative of the Challenging dimension; this ESB regards proactive instruction from one colleague to another in order to avoid potential security problems, and is bet conceptualized as actual "directing" behaviors between employees as regards security procedures. "Reporting" is the Challenging dimension ESB that has to do with whistle-blowing or the potential report to superiors about security behaviors in contravention of policy. Unlike the other three approaches which are largely supportive, Reporting can potentially damage co-worker relationships (Van Dyne and LePine 1998).

	Prohibitive	***Promotive***
Affiliative	Stewardship	Helping
Challenging	Reporting	Voice

Table 1. A Typology of Extra-Role Security Behaviors

Adapted from Van Dyne et al. (1995)

Motivational Antecedents to ESBs

Because people who feel psychologically empowered are more likely to be creative, to take initiatives and to diverge from the status quo (Spreitzer 1995; Zhang & Bartol 2010), we draw upon empowerment theory to propose that employee psychological empowerment should promote the cognitive and motivational processes that most proximately drive ESBs. The empowered employee is both well informed as to mission and feedback on performance, as well as rewarded for achieving organizational goals (Spreitzer 1995); as such, empowered employees feel motivated and capable to "go the extra mile" in helping their coworkers. Based largely upon psychological empowerment theory, we posit that employees will be motivated to engage in Affiliative ESBs (i.e., helpful to others) when they participate in SETA-based training programs, and more likely to engage in Challenging-based Reporting and Voice-related persuasive direction when rewards are at stake. In like manner, we expect that extrinsic motivations lead most often to Prohibitive ESBs (designed to reduce undesirable security behaviors: Stewardship and

Reporting), whereas intrinsic motivations lead most often to Promotive ESBs (designed to support pro-security behaviors, Helping and Voice).

Antecedents to employee empowerment: training versus rewards

Consistent with Spreitzer's (1995) antecedent model of psychological empowerment, we suggest that employee motivations to engage in ESBs can arise from two specific antecedents related to information and rewards. Information empowerment arises from greater detail on mission expectations and subsequent performance feedback, while rewards serve to highlight the individual contributions of employees, thus empowering through recognition (Spreitzer 1995 pp. 1447-1448). Security education, training, and awareness (SETA) training programs are designed to reduce risks due to accidental security breaches by employees and other parties who come into contract with its information assets and systems (Whitman and Mattord, 2012). SETA programs have been successfully served as a significant driver of IS misuse/compliance (D'Arcy & Hovav 2007) and also contribute to employees' protection-motivated behaviors (Posey et al. 2015). Training, as an information conduit, should be most related to the "supportive" ESBs of Stewardship and Helping, given the synergies involved with the transfer of informational expertise to coworkers. Conversely, rewards structures tend to provide an indication that certain behaviors are valued due to the extent that they contribute to organizational objectives (Spreitzer 1995). Rewards should be most motivating of the more pragmatic and objective "directive" ESBs of Reporting and Voice, being focused as they are on the recognition of individual contribution (Spreitzer 1995).

Antecedents to employee empowerment: extrinsic versus intrinsic

Amabile (1993) developed a spectrum of studies linking employees' intrinsic motivation as the most proximate cause of creative behaviors (which we consider include the Promotive ESBs of Helping and Voice), indicating that intrinsic motivation bridges what an individual can and will do. Further, empowerment theory suggests that intrinsic motivation contributes to innovative/change-oriented behavior (Spreitzer 1995). Additional antecedents are also found in traditional compliance and deterrence approaches found in the literature, which are extrinsic in their motivational perspective (Herath and Rao 2009). In extrinsically motivated situations, employees tend to follow rules without questioning regardless of possible deficiencies and in the absence of providing suggestions for improvement to management or to each other. It takes the interaction with training-related motivations or the influence of sought rewards in extrinsic situations to motivate the subsequent ESBs of Stewardship or Reporting.

Zhang and Bartol (2010) argue that psychological empowerment can directly influence engagement in task-related cognitive processes, leading to *intrinsic* motivation. Following Zhang and Bartol (2010), we propose when an individual believes that IS security is *meaningful*, they feel more competent in the IS area, and will devote more cognitive effort to understanding and resolving IS security-related problems. According to Thomas and Velthouse (1990) and Spreitzer (1995), meaning indicates the intrinsic value of one's work task. Meaningful security work linked with SETA-based training can lead to the ESB of Helping, whereas meaningful security concerns linked with reward structures can result in persuasion-based Voice ESBs. In a synthesis of the converging views of training vs. reward structures, crossed with extrinsic and intrinsic motivational bases, we conceptualize a model based on 4 propositions:

Proposition 1: Training programs (SETA) are positively associated with employee's psychological empowerment leading to Affiliative ESBs.

Proposition 2: Rewards (financial incentives) are positively associated with employee's psychological empowerment leading to Challenging ESBs.

Proposition 3: Intrinsic motivations are positively associated with employees' psychological empowerment leading to Promotive ESBs.

Proposition 4: Extrinsic motivations are positively associated with employees' psychological empowerment leading to Prohibitive ESBs.

We embed these propositions in a theoretical network demonstrated in the Figure, below, for purposes of demonstrating the interaction of regular employees with either a) security-knowledgeable coworkers in the firm to whom they might make reasoned fact-based appeals (Voice, for example), or b) management-oriented individuals to whom they might Report on matters of security violations. In turn, each sort of extra-role coworker, security-savvy or management-savvy, might mentor regular employees via the extra-role Stewardship process, for reasons of their own. Lastly, regular employees are highly likely to affiliate at a social level with each other and engage in ESBs related to Promotive relationships; to wit, Helping extra-role behaviors among the regular rank and file.

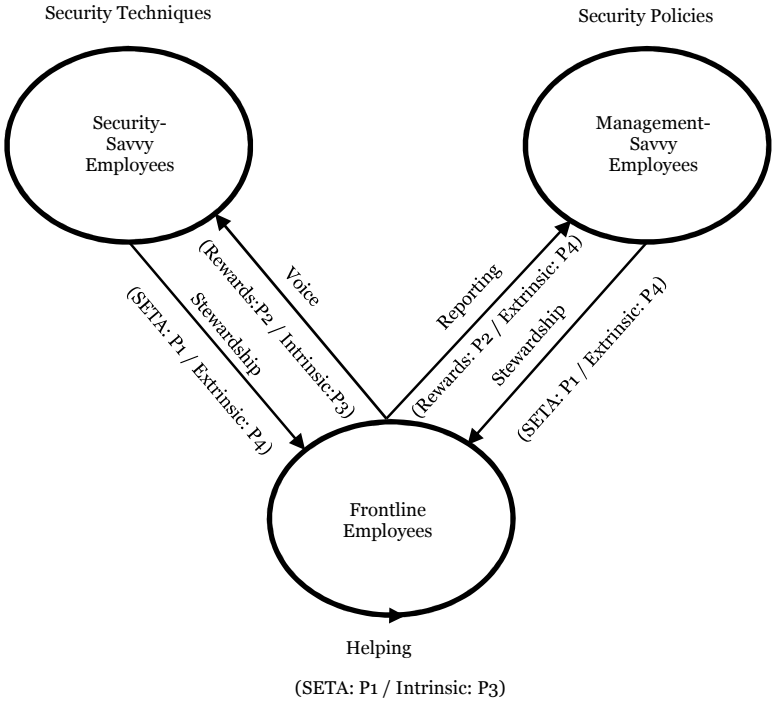

Figure 1. Extra-Role Security Behavior (ESB) Model

Conclusions

To extend conceptualizations of the role of end-users as implementers of security mechanisms, we argue that employees' extra-role security behaviors can enrich an organization's capacity to address internal and external threats. To that end, we propose a contingency perspective that outlines the circumstances in which ESBs might be expected to arise, and the reasons for which they might transpire. Our framework lends itself to exploring boundary conditions under which the motivation processes described here actually lead to ESBs. Our framework also can diagnose the situations in which certain ESBs are most likely to arise, given specific antecedents. We caution that the empowered employee will contribute to pro-security behaviors in the workplace by the empowered motivation to help others comply, but that empowerment can also lead to unanticipated "helping" that might direct behaviors in the wrong direction when security policies are ambiguous or poorly communicated among the workforce. In future research, we hope to obtain supportive evidence for the posited model, which suggests that employees can be empowered to ensure security of organizational information resources through judicious engagement in extra-role behaviors outside of the orthodox confines of the corporate information security policy.

REFERENCES

Amabile, T.M. 1993. "Motivation Synergy: Toward New Conceptualizations of Intrinsic and Extrinsic Motivation in the Workplace," *Human Resource Management Review* (3), pp. 185-201.

Ayyagari, R., Grover, V., Purvis, R.2011. "Technostress: Technological Antecedents and Implications," *MIS Quarterly* (35:4), pp. 831-858.

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

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010b. " Quality and Fairness of an Information Security Policy as Antecedents of Employees' Security Engagement in the Workplace: An Empirical Investigation," in *Proceedings of the 43rd Hawaii International Conference on System Sciences*, Sprague, R. (ed.), Honolulu, HI, pp. 1-7.

Colvin, R.G. 2016. Management and Organizational Influences on the Compliance Behavior of Employees to Reduce Non-malicious IT Misuse Intention. Unpublished doctoral dissertation, Kennesaw State University: Kennesaw GA.

Crossler, R., Johnston, A., Lowry, P., and Hu, Q. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), pp. 90-101.

D'Arcy, J. and Hovav, A. 2007. "Deterring Internal Information Systems Misuse," *Communications of the ACM* (50:10), pp.113-117.

Herath, T., Rao, H.R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hsu, J.S., Shih, S.P., Hung, Y. W., and Lowry, P.B. 2015. " The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282-300.

Katz. D. 1964. "The Motivational Basis of Organizational Behavior," *Behavior Science* (9:2): 131-146.

Pahnila, S., Siponen, M., and Mahmood, A.2007. "Employees' Behavior towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences*, Sprague, R. (ed.),

Posey, C., Roberts, T., and Lowry, P. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179-214.

Posey, C., Roberts T., Lowry, P.B., Hightower, R.T. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders, " *Information & Management* (51:5), pp. 551-567.

Smith, C.A.,Organ, D.W., and Near, J.P. 1983. Organizational Citizenship Behavior; Its Nature and Antecedents," *Journal of Applied Psychology* (68:4), 653-663.

Spreitzer, G.M. 1995. "Individual Empowerment in the Workplace: Dimensions, Measurement, Validation," *Academy of Management Journal* (38), pp. 1442-1465.

Thomas, K.W. and Velthouse, B.A. 1990. "Cognitive Elements of Empowerment: An 'Interpretive' Model of Intrinsic Task Motivation," *Academy of Management Review* (15:4), pp. 666-681.

Van Dyne, L., Cummings, L. L., and McLean Parks, J. 1995. "Extra-role behaviors: In pursuit of construct and definitional clarity (a bridge overmuddied waters)," In L. L. Cummings & B. M. Staw (Eds.), *Research in organizational behavior,* pp. 215–330. Greenwich, CT: JAI Press.

Van Dyne, L., & LePine, J. A. 1998. "Helping and voice extra-role behaviors: Evidence of construct and predictive validity," *Academy of Management Journal* (41), pp. 108–119.

Warkentin, M., and Willison, R. 2009."Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105.

Whitman, M.E., and Mattord, H. J. 2012. "*Principles of Information Security*," 4th ed. Boston, MA: Course Technology.

Whitman, M.E., Townsend, A.M., and Aalberts, R.J. 2001. "Information Systems Security and the Need for Policy," in *Information Security Management-Global Challenges in the Next Millennium*, Dhillon, G. (Ed.), London: Idea Group, pp. 9-18.

Zhang, X. and Bartol, K. 2010. "Linking Empowerment Leadership and Employee Creativity: The Influence of Psychological Empowerment, Intrinsic Motivation, and Creative Process Engagement," *Academy of Management Journal* (53:1), pp. 107-128.