How employees learn ISP compliance behavior: toward a social learning perspective

ABSTRACT

Information security attacks usually exploit the weakest link in the chain — in many cases the end user at the workplace. While major advances have been made in understanding and explaining information security behavior, little is known about how such behavior is acquired in the first place. This research approaches the phenomenon through the lens of social learning theory. We argue that the behavior of a new employee is initially learned through differential associations within the social network rather than via knowledge of formal policies and related sanctions. Moreover, we suggest that this changes over time. Reinforcements through sanctions become more important at the maintenance stage, while imitation of others becomes less relevant.

INTRODUCTION

A key instrument for achieving information security in organizations is information security policy (ISP). Following recommendations in the best practice literature (e.g., ISO 27002, BSI 200-1), organizations often implement a wide range of mechanisms to motivate employees to follow ISPs. However, evidence from research regarding the efficiency of such measures has been mixed and non-compliance with ISPs remains one of the major challenges for information security management.

Research has adopted several perspectives to explain this phenomenon of non-compliance, often building models upon theoretical lenses such as rational choice theory, protection motivation theory, or the theory of planned behavior (D’Arcy and Lowry 2018; Herath and Rao 2009; Menard et al. 2017). While this stream of research has made significant progress in explaining employees’ non-compliance with ISPs, there is still little known about the initial acquisition of ISP behavior (Willison et al. 2018). A better understanding of initial adoption is crucial for two reasons: First, initial behavior is just as important as continued ISP compliance behavior, as attackers usually target the weakest link in the security chain. Moreover, research emphasizes the difficulties of altering behaviors after behavioral patterns become routinized (Vance et al. 2012). Second, the phenomenon of non-compliance at the initial adoption stage has certain characteristics that are poorly explained by current theories. For example, rational choice theory assumes at least a high degree of information transparency. However, new employees usually lack access to practical knowledge regarding the likelihood of non-compliance being detected and actual, realized punishments. Moreover, the social context in which a behavior takes place often plays just a minor role. While ISP studies that draw upon the theory of planned behavior typically include a concept of subjective norms (Herath and Rao 2009), this idea refers rather to a broad definition of organizational norms and does not focus on the process of learning. However, research on learning generally acknowledges the importance of social embedding.

This research aims to explain differences in the process of learning ISP compliance behavior, which in our case refers to behavior that has non-malicious motives (Willison et al. 2018). We borrow from social learning theory with a focus on Akers et al.'s (1979) interpretation of differential associations in the context of criminology and deviant behavior.

Reviewing Social Learning Theory

Social learning theory addresses social behavior and learning. The basic premise is that behavior is learned through social interaction with others. It thus extends the perspective of operant conditioning (Skinner 1938). Operant conditioning argues that behavior is acquired through direct conditioning, i.e., when an individual makes an association between a particular behavior and a corresponding consequence. Social learning theory adds that behaviors can also be learned by observing and imitating others (Bandura 1963). Moreover, it argues that learning is a cognitive process (Akers et al. 1979). The learner does not passively adapt to observed behavior; instead, the learning process is formed by the cognitions of other behaviors and their translation under consideration of further individual and environmental factors as well as one’s own context.

Both theories can be transferred to the learning of information security behaviors. Let us, for example, imagine a clean desk policy stipulating that employees lock their notebooks in the docking station. Through the lens of operant conditioning, desired employee behavior can be trained through regular clean desk checks with associated penalties. Operant conditioning predicts that recurring unpleasant consequences will lead employees to associate not locking their notebooks with the repercussions and therefore to adjust their behavior. Through the lens of social learning theory, training employee behavior does not necessitate that they be directly affected by an unpleasant consequence; learning to comply with the clean desk policy can occur vicariously. Observing the notebook-locking behavior of colleagues and whether they were penalized for non-compliance can be sufficient to learn the behavior. Social learning theory also states that learning from vicarious experiences is cognitive rather than purely behavioral. An employee does not just see the policy compliance behaviors of others and adapt to it; instead, the individual cognition under consideration of his or her individual environment is what leads to a potential behavior change. Employees are more likely to copy the compliance or non-compliance behavior of colleagues if the observed situation is transferable to their own contexts. For example, an employee who works with strictly confidential information on their notebook is more likely to adopt the notebook-locking behavior of his direct team colleagues than that of a low-level case worker he might have met on a business trip in another country.

RESEARCH MODEL

In this study, we aim to gain a better understanding how ISP compliance behavior is initially learned and later maintained. The research model is informed by two theoretical lenses: deterrence theory and social learning theory. Deterrence theory mirrors the classical understanding of compliance behavior that focuses primarily on ISP design and individual rational decision making (Willison et al. 2018). It is implemented with its core construct that refers to sanctions related to non-compliance. Social learning theory (Akers et al. 1979) extends this perspective, considering differential associations as the primary source of behavioral learning. Moreover, the process of learning allows for a crisp differentiation between how a new employee's initial behavior and an established employee's maintained behavior are learned. The research model is depicted in Figure 1.

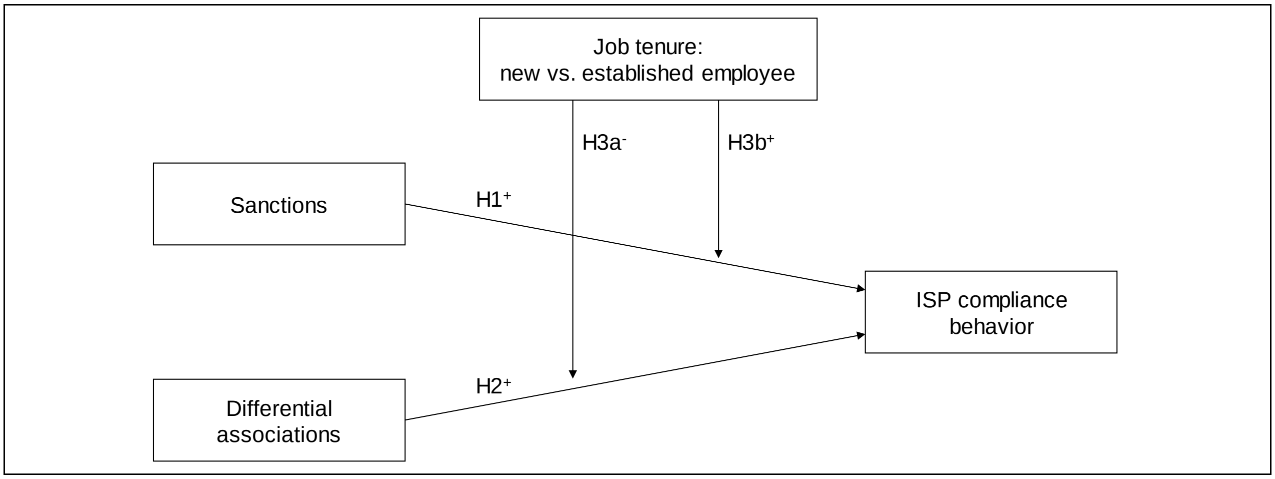

Figure 1. Research Model

A common measure for ensuring that employees adhere to ISP regulations is the implementation of deterrence, which organizations deliver through disciplinary sanctions such as warnings, fines, demotions, and dismissals (D'Arcy et al. 2009; Herath and Rao 2009).

Deterrence theory assumes a rational actor who deliberately weighs the potential benefits and costs of non-compliance before taking action. Drawing on this reasoning, it is argued that the more severe the sanctions are, the more likely employees are to follow the regulations. Accordingly, we posit the following:

Hypothesis 1 (H1): Sanctions lead to a higher degree of ISP compliance behavior.

Differential associations are the behaviors and attitudes exhibited within an individual's social network (Pratt et al. 2006). In an organizational context, such a network can include relationships with direct team colleagues, specific members from project teams, or friends across departments. Employees learn ISP compliance behavior from this group through the concept of vicarious learning and imitation (Warkentin et al. 2011). If network members demonstrate non-compliance, an employee is more likely to register the non-compliance as a good behavior. The peer group thus influences how an employee balances the pros and cons of compliant behavior. Therefore, we propose the following hypothesis:

Hypothesis 2 (H2): Differential associations lead to a higher degree of ISP compliance behavior.

Social learning theory predicts that initial behavior is learned primarily through imitation. Transferred to the realm of ISP compliance, it is argued that new employees learn predominately through observation rather than by directly weighing any potential cost and benefits. Through the lens of deterrence theory and a rational actor, a newcomer might know that sanctions exist and that they might even be monitored; however, the high degree of uncertainty regarding the true impact of non-compliance renders it difficult to evaluate this equation objectively. Adding to this unpredictability is that the likelihood of deviant behavior being monitored, detected, and then sanctioned is generally low. Social learning theory therefore posits that imitating others is the first step to acquiring a new behavior. Building upon the subsequent experiences of positive or negative consequences, people then form their own attitudes regarding what is good or bad. When a behavior is maintained, imitating others in one's peer group becomes less important.

Hypothesis 3a (H3a): The influence of differential associations on ISP compliance is higher for new employees than for established employees.

Hence, deterrence through the threat of sanctions is more powerful in the maintenance phase than in the acquisition phase of a new behavior. Established employees who have already built their attitudes in regard to ISP compliance are less prone to the influence of peer behavior, responding instead to reinforcements. This includes negative reinforcements, such as potential punishments. Accordingly, we posit a final hypothesis:

Hypothesis 3b (H3b): The influence of sanctions on ISP compliance is higher for established employees than for new employees.

RESEARCH DESIGN

To test the research model, we will implement a full factorial experimental 2 x 2 x 2 between-subjects design. The between-subjects factors will be the three independent variables: sanction, differential associations, and job tenure. We propose using a vignette design (Johnston et al. 2016). The base scenario describes a typical situation for Julia, an employee in her daily work. At the end of the scenario, Julia decides to violate the internal clean desk policy due to time pressure. The scenarios differ in terms of the vignettes. For job tenure, the scenarios include one of two statements: "Julia has just finished university and started a job in the management accounting department of a large company" or "Julia has worked for over five years in the management accounting department." For sanction, the scenario specifies either that "Julia knows that policy violations lead to disciplinary warnings or loss of pay" or that "Julia does not know whether there are any consequences related to policy violations." For differential associations, some of the scenarios note, “Lukas is a close colleague and friend with whom you regularly go to the cafeteria. Julia notes that Lukas does not always lock his computer when he leaves the office.” The other scenarios state, “Lukas is a close colleague and friend with whom you regularly go to the cafeteria. However, you have never seen whether Lukas locks his computer when he leaves the office.”

Behavioral measures and control variables will be measured with a questionnaire. ISP compliance intention will be measured through items referring to the scenario, e.g., “In this situation, I would do the same as Julia did” (Johnston et al. 2016). The sample will comprise students nearing graduation. With a focus on how initial ISP compliance behavior is learned, such a sample is ideal, as students have comparably weak definitions in regard to policy violation behaviors. A power analysis with G*Power 3.1.9.2 assuming a small effect size reveals a lower bound of at least 132 participants (linear multiple regression for a fixed model and significant single regression coefficients, $f = .10$, $\alpha = .05$, power = .95, 5 predictors).

CONCLUSION

With this research in progress, we aimed to gain insights into how new employees learn ISP security behaviors. Drawing on social learning theory, we argued that new behaviors are learned primarily through the social environment rather than via formal sanctions. Moreover, we posited that initial ISP compliance behavior is different from maintained behavior. While new employees learn through observing and imitating others, established employees also learn from reinforcements in the form of official sanctions. This has important implications for practice. Organizations often rely solely on formal policies with sanction mechanisms that are signed during the onboarding stage. However, the (non-)application of the wide range of security policies and procedures in daily behaviors might in fact be learned on the job. Organizations should ensure that such behaviors do not become routine at this early stage. Measures to achieve this could include programs accompanying the onboarding process, such as dedicated security mentoring programs, self-reflections, or security training groups for new employees.

REFERENCES

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., and Radosevich, M. 1979. "Social Learning and Deviant Behavior: A Specific Test of a General Theory," *American Sociological Review* (44:4), pp. 636–655.

Bandura, A. 1963. *Social Learning and Personality Development*, New York: Holt, Rinehart, and Winston.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98.

D'Arcy, J., and Lowry, P. B. 2018. "Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study," *Information Systems Journal* (forthcoming), pp. 1–27.

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), Elsevier B.V., pp. 154–165.

Johnston, A. C., Warkentin, M., McBride, M., and Carter, L. 2016. "Dispositional and Situational Factors: Influences on Information Security Policy Violations," *European Journal of Information Systems* (25:3), pp. 231–251.

Menard, P., Bott, G. J., and Crossler, R. E. 2017. "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self- Determination Theory," *Journal of Management Information Systems* (34:4), pp. 1203–1230.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., and Madensen, T. D. 2006. "The Empirical Status of Deterrence Theory: A Meta-Analysis," in *Taking Stock: The Status of Criminological Theory*, New Brunswick: Transaction Publishers, pp. 367–395.

Skinner, B. F. 1938. *The Behavior of Organisms: An Experimental Analysis*, New York: Appleton-Century.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information and Management* (49:3–4), Elsevier B.V., pp. 190–198.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention," *European Journal of Information Systems* (20:3), pp. 267–284.

Willison, R., Lowry, P. B., and Paternoster, R. 2018. "A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research," *Journal of the Association for Information Systems* (forthcoming).