Spring 5-19-2016

The Influence of Outcome-Oriented Security Policy on Security Perceptions and Intentions

Jeffrey D. Wall
Michigan Technological University, jdwall@mtu.edu

Mari W. Buche
Michigan Technological University, mwbuche@mtu.edu

The Influence of Outcome-Oriented Security Policy on Security Perceptions and Intentions

Jeffrey D. Wall
Michigan Technological University
jdwall@mtu.edu

Mari W. Buche
Michigan Technological University
mwbuche@mtu.edu

ABSTRACT

With security breaches occurring regularly, organizations must employ strong security countermeasures to protect private, valuable information. Organizational insiders pose a major threat to the security of organizations by direct and intentional misuse of information assets and by the careless and negligent use of information. Developing strong information security policy (ISP) is important to thwarting insider security threats. To date, behavioral information security research has primarily examined ISP from a procedural viewpoint. Outcome-oriented security policy is understudied. This research-in-progress proposes a study of security policy to determine how the inclusion of outcome-oriented security policy influences insiders' attitudes toward and intentions to follow procedural security policy. An experiment is proposed to test the hypotheses.

Keywords

Information security policy, outcome oriented policy, procedural policy, experiment.

INTRODUCTION

Organizational security breaches are increasingly frequent and costly, making information security an important management concern (Willison and Warkentin, 2013). Organizational insiders, such as employees and board members, pose a major threat to information security because they are entrusted with valuable and confidential information. When insiders handle information insecurely, they create security vulnerabilities that others can exploit. Organizations adopt controls to manage insiders' security behaviors, such as security-related sanctions and rewards and security training. These controls are instituted to support information security policy (ISP). ISP resides at the core of organizational attempts to thwart misuse of information and to promote positive security behaviors by insiders.

Most behavioral information security studies, examine ISP from a procedural viewpoint (Wall, Stahl and Salam, 2015). However, this is only one of two viewpoints. Policy can be instituted as procedurally oriented or as outcome oriented (Wall, Lowry and Barlow, 2016). *Procedurally oriented policy* sets forth antecedent behaviors that are likely to lead to a desired outcome, such as security behaviors that are likely to maintain the safety of organizational information (e.g., creating strong passwords). Conversely, *outcome oriented policy* sets forth desired outcomes that individuals work toward without specifying specific behaviors, such as security goals and objectives. Importantly, outcome oriented policy tends to lead to better outcomes than procedurally oriented policy (Wall et al., 2016).

This paper proposes an experimental design to test whether outcome oriented ISP improves security-related perceptions, beliefs and intentions.

LITERATURE REVIEW

Behavioral information security research has focused extensively on ISP as procedurally oriented (Wall et al., 2015). Most studies examine ISP as a dependent variable in the form of intentions to comply with or violate ISP. Many of these studies examine procedural behaviors such as: sharing passwords and failing to report computer viruses (Vance, Siponen and Pahnila, 2012). Other studies measure procedural behaviors broadly, such as: following requirements of the ISP (e.g., Bulgurcu, Cavusoglu and Benbasat, 2010).

Only a few studies examine ISP as outcome oriented. Again, these studies largely treat ISP as the dependent variable. For example, Boss, Kirsch, Angermeier, Shingler and Boss (2009) measured policy behavior as: paying attention to security during work routines and staying aware of the latest security threats. Such behaviors focus on security outcomes, rather than on procedural behaviors.

By primarily treating ISP as a dependent variable, behavioral information security research understands little about the characteristics of ISP that lead to better security attitudes and behavior. The few studies that examine ISP as an independent variable have found that awareness of ISP influences beliefs about security outcomes (Bulgurcu et al., 2010), sanctions (D'Arcy, Hovav and Galletta, 2009), and the manditoriness of ISP (Boss et al., 2009). These treatments are solely procedural. Studies have not adequately addressed outcome oriented ISP.

We seek to examine how including outcome oriented policy in procedural ISP influences security perceptions and attitudes and intentions to comply with procedural ISP.

THEORY DEVELOPMENT

Outcome oriented policy draws insiders' attention to achieving security outcomes, while procedurally oriented policy draws attention to a specific set of security behaviors (Wall et al., 2016). By drawing attention to a checklist of procedural security behaviors, insiders may perceive that they are in compliance with ISP when the checklist is complete (Dhillon and Backhouse, 2001). With outcome oriented policy, however, insiders are likely to perceive that work is not complete until the desired outcomes are achieved. Thus, outcome oriented policy is likely to improve security efforts.

Further, procedural policy requires no creativity in achieving security outcomes. Yet, outcome oriented policy promotes creative efforts to achieve outcomes (Wall et al., 2016). According to self-determination theory (Deci, Koestner and Ryan, 1999), individuals want to feel that their behaviors are self-determined. Self-determination leads to improved intrinsic motivation to accomplish outcomes (Deci et al., 1999). Because outcome oriented policy allows for self-determined behavior, such policy may lead to intrinsic security motivations. Improved intrinsic motivation improves well-being and leads to persistent behavior. Thus, long-term security outcomes may be improved by using outcome oriented ISP.

A number of mediating and dependent variables are used in behavioral information security research, including: self-efficacy to comply with ISP, the response efficacy of security countermeasures, attitudes toward security, and intentions to comply with procedural ISP (e.g., Bulgurcu et al., 2010; Johnston and Warkentin, 2010). Because outcome oriented ISP is likely to promote self-determined behavior and promote intrinsic motivation and general well-being, outcome oriented ISP is likely to increase *self-efficacy perceptions*—the belief that one is capable of complying with security requirements. Outcome oriented ISP is also likely to increase *response efficacy*—the belief that a security countermeasure will be effective—by allowing insiders to choose security tasks (i.e., self-determination) they believe to be effective in achieving security outcomes. By increasing self-determination, outcome oriented policy is also likely to improve attitudes toward security. By enhancing self-determination and intrinsic motivation, outcome oriented behaviors are likely to increase intentions to comply with procedurally oriented ISP as well. In summary, we suggest:

> *H1: the inclusion of outcome oriented policy in a procedural ISP will increase insiders' self-efficacy to comply with procedural ISP.*
>
> *H2: the inclusion of outcome oriented policy in a procedural ISP will increase insiders' response efficacy perceptions.*
>
> *H3: the inclusion of outcome oriented policy in a procedural ISP will improve insiders' attitudes to information security.*
>
> *H4: the inclusion of outcome oriented policy in a procedural ISP will increase insiders' intentions to comply with procedural ISP.*

PROPOSED METHODS

To test the proposed hypotheses, a scenario-based experiment will be employed. Respondents will be presented with a security policy and then asked questions pertaining to each of the outcome variables (i.e., self-efficacy, response efficacy, security attitudes, and compliance intentions). One of two policies will be presented at random to each respondent. The policy for the treatment group will include an outcome oriented policy (i.e., a security goal), followed by a few procedural security policies. The policy for the other group will include only the few procedural policies. Analyses will then be conducted to determine whether differences exist between the groups for the outcome variables. Common security variables, such as self-efficacy and response efficacy will also be included as control variables.

DISCUSSION

Although procedural ISP is common in organizations, outcome oriented ISP could enhance efforts to improve insiders' security behaviors. This paper describes why the inclusion of outcome oriented ISP is likely to improve security perceptions,

attitudes, and intentions. By conducting the suggested experiment, we will better understand how outcome oriented ISP influences information security within organizations.

From a theoretical standpoint, we draw attention to the nature of ISP (i.e., procedural and outcome oriented) and theorize around an understudied type of ISP. We have the potential to demonstrate how outcome oriented policy can improve self-determined security behavior, which has been identified as an important direction for future research (Wall, Palvia and Lowry, 2013).

From a practical standpoint, we identify a simple security countermeasure (i.e., outcome oriented ISP) that can be added to existing countermeasures to improve information security. If the results are as predicted, managers may be able to improve insiders' security efforts simply by setting and making insiders aware of security goals and objectives.

CONCLUSION

ISP research should place greater emphasis on characteristics of ISP to identify aspects of ISP that improve security attitudes, intentions, and outcomes.

REFERENCES

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, W. R. (2009) If Someone Is Watching, I'll Do What I'm Asked: Manditoriness, Control, and Information Security, *European Journal of Information Systems*, 18, 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, 523-548.

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

Deci, E. L., Koestner, R., and Ryan, R. M. (1999) A Meta-Analytic Review of Experiments Examining the Effects of Extrinsic Rewards on Intrinsic Motivation, *Psychological Bulletin*, 125, 6, 627-668.

Dhillon, G., and Backhouse, J. (2001) Current Directions in Is Security Research: Towards Socio-Organizational Perspectives, *Information Systems Journal*, 11, 2, 127-153.

Johnston, A. C., and Warkentin, M. (2010) Fear Appeals and Information Security Behaviors: An Empirical Study, *MIS Quarterly*, 34, 3, 549-566.

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

Wall, J. D., Lowry, P. B., and Barlow, J. B. (2016) Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess, *Journal of the Association for Information Systems*, 17, 1.

Wall, J. D., Palvia, P., and Lowry, P. B. (2013) Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy, *Journal of Information Privacy and Security*, 9, 4, 52-79.

Wall, J. D., Stahl, B. C., and Salam, A. F. (2015) Critical Discourse Analysis as a Review Methodology: An Empirical Example, *Communications of the Association for Information Systems*, 37, 1, 257-285.

Willison, R., and Warkentin, M. (2013) Beyond Deterrence: An Expanded View of Employee Computer Abuse, *MIS Quarterly*, 37, 1, 1-20.