Impact of User Experience and Comprehension on Awareness Training

Emergent Research Forum (ERF)

Jonathan K Adams
College of BILT, Marymount University,
Arlington, Virginia, United States
jka40138@marymount.edu

Michelle Liu
College of BILT, Marymount University,
Arlington, Virginia, United States
xliu@marymount.edu

Abstract

The human component of information systems is a target of cyberattacks. Firms address the threat using security awareness training, monitoring, controls, and enforcement. User security awareness as a part of the information system is key. Increasing telework, remote access, and collaborative technologies require user security hygiene. The problem is acute with small and mid-sized businesses, more likely to invest less in cybersecurity. This study seeks to assess the effectiveness of security awareness training at influencing user behaviors. The assessment includes the influence of training and culture on policy compliance via leadership prerogative and the moderating effect of user comprehension of security tool messaging. Security tools are integral to defense-in-depth. Little research has examined how security tools use affects user compliance intention. This study seeks to incorporate employee cognition of information from security tools into an understanding of factors that influence user attitudes toward security policy compliance.

Keywords

Security Awareness, Usable Security, Security Policy Compliance, Human-Computer Interaction

Introduction

Security awareness training is a common topic of study. Much of the reason for this lies in the challenges to implementing and maintaining an effective security awareness program. These training programs are often the primary outreach from an organization to its userbase to convey security policy, threat awareness, and to drive positive user hygiene. The challenges to operating a successful program vary, including user adoption of best practices, limited budgets, and constrained resources (Manke and Winkler 2013). Challenges in this area are further complicated by the COVID-19 pandemic and the increased dependence on technology as an enabler of socially distanced work and education. The increasingly adoption of technology, particularly collaboration tools and remote access capabilities to extend corporate networks create new vectors for threat actors to exploit.

Ultimately security awareness training effectiveness is borne out by the ability to drive desired user behaviors. To do this, effective training must have an effective delivery to the target audience (Banfield 2016; Ki-Aries and Faily 2017). Despite the challenges, organizations recognize the need to address the human component of their systems and continue to invest time, money, and effort in these types of education programs. An enterprise cybersecurity program must address both policy awareness and risk awareness in the user community. Defense in Depth (DiD) can be seen as a comprehensive approach for managing security risk in information technology enterprises (Straub 2003). This comprehensive approach leverages technical tools and policy, at multiple layers, to protect against threats, including improving the user awareness of risky behaviors and applying enterprise security policies and controls. DiD depends over interlocking layered defenses to mitigate attacks. The human in the loop should be a component of any DiD approach (Orme 2019).

The human variable in securing enterprise systems is complex to address as humans present a unique risk to protecting key assets. Traditionally, well-thought-out security policies have provided some effectiveness in reducing risk surface (Höne and Eloff 2002). However, to maximize the effectiveness of policy, it is important to have both compliance requirements and enforcement, which implies user awareness. Awareness alone does not result in security policy compliant behavior. Multiple studies (Bulgurcu et al. 2010; Herath and Rao 2009; Ifinedo 2012; Pahnila et al. 2007; Paliszkiewicz 2019) have investigated a variety of factors ranging from psychological theory, organizational culture, and others that can influence users' actions once a security awareness regime has been created. (Herath and Rao 2009) pointed to several factors, including self-efficacy and social influence as well as corporate commitment as factors in security compliance behaviors. One study (Bulgurcu et al. 2010) showed a relationship between employee awareness of cybersecurity and policy affects attitudes toward compliance.

In their study covering the vulnerability of users to phishing, training effectiveness was a key part of the broader mitigation strategy (Luga et al. 2016). Informed by this line of the studies, the motivation for this inquiry is to improve organizations' resilience from cybersecurity attacks targeting the end user. Firms can motivate policy compliance through supporting actions, which could include aspects of the training itself, as well as supporting psychological factors that can optimize users' responses to training.

Theoretical Background

The study focuses on two factors in security policy intention and behaviors: user understanding of cybersecurity and organizational policies and organizational culture, driven downward from leadership. Studies show that security awareness and compliance training have a positive effect. A case study (Eminağaoğlu et al. 2009) found that such training improved both employees' behaviors and practical application of knowledge, such as using better passwords. Recent studies find that an organization's culture can have a significant positive effect on compliance (Da Veiga and Martins 2015; Nasir et al. 2019). Considering the organizational culture and how it influences the other policy, education, and technical methods used to secure IT assets is consistent with proven holistic approaches like DiD . A holistic approach to security is inclusive of security policies, procedures, and ultimately influencing how work is done to incorporate cybersecurity (Goodyear et al. 2010). Security awareness factors into the perception of organizational commitment to security and contribute to the broader corporate security culture. For example, (Schlienger and Teufel 2002) discussed organizational culture and management buy-in in the context of security awareness.

At a most basic level, when considering whether or not to follow rules, humans consider social norms and expectations and consequences in a complex calculus that includes perceived self-interest (Zink 2008, Jun 10). Both the influence of security awareness training and organizational culture, particularly vis-à-vis social consequence, can be contributing factors in attitude toward security and behavioral intentions.

This study will bundle these factors and integrate the moderating effect of the usability of the information system (IS) and the users' cognition of the messaging that it provides. There is a thread of research that covers the ability of security messaging to adequately convey information about consequence, threats and their magnitude and the subsequent impact on decision making. There is a compelling case for the need for warning messages to provide enough comprehensible information for the user to make the correct informed decisions (Felt et al. 2015). Error messages with bad user experience, particularly through poor design and poor conveyance of threats can have a negative effect on users' security policy compliance and ability to avoid risks as evidenced in (Akhawe and Felt 2013). The idea that user experience via security messaging and tools ultimately influences user threat comprehension and actions is significant and in a broad view has the potential to counteract the complex decision calculus that will influence users' actions toward compliance and security hygiene behaviors.

Objective of the Study

The objective of this study is to address the broad research problem of the enhancing the understanding of users' security compliance behaviors. More acutely, security awareness programs are an almost de-facto approach in larger firms to address the human component of cybersecurity. Generally, the literature, a la (Bulgurcu et al. 2010) supports the concept of information security awareness as a positive influence on

compliance. Further studies such as Banfield (2016), Bulgurcu et al. (2010), and Ifinedo (2012) each have considered some form of subjective norms and culture, peer, or direct supervisor influence on security policy compliance behavior. Finally, the presentation of information in a cybersecurity context can affect the awareness of threats and possibly behaviors. Akhawe and Felt (2013) and Felt et al. (2015) provide two example studies showing the presentation of security information can affect threat comprehension and behavior. The study proposes three research questions:

RQ1: What is the relationship between influence of security awareness training and employees' intention to comply with policy?
RQ2: What is the relationship between leadership commitment to security policy compliance and employees' intention to comply with policy?
RQ3: Does employee comprehension of security messaging moderate either of the above main effects?

RQ1 is intended to establish a linkage or lack of linkage between employees' intention to comply and organizations' application of security awareness training programs. This is notable during the COVID-19 pandemic with new risks to firms' data and technology assets via collaboration and remote work. RQ2 seeks to understand the influence of leaders and leader-driven organizational culture on security policy compliance intentions. Finally, RQ3 abstracts the concept of security information presentation and how comprehension of that information can add or detract from the compliance intentions.

Methodology

A single quantitative survey will analyze IT workers in the greater Washington, DC area. An instrument has been developed that will ultimately enable analysis of users' intentions to comply with security in relation to both the influence of security awareness training and via the firms' leadership commitment to security policy compliance. Further analysis will be conducted, evaluating the moderating impact of employee user experience with the security component of firm's IS and employee comprehension of the IS security related messaging. The framework for this study is reflected in figure 1.

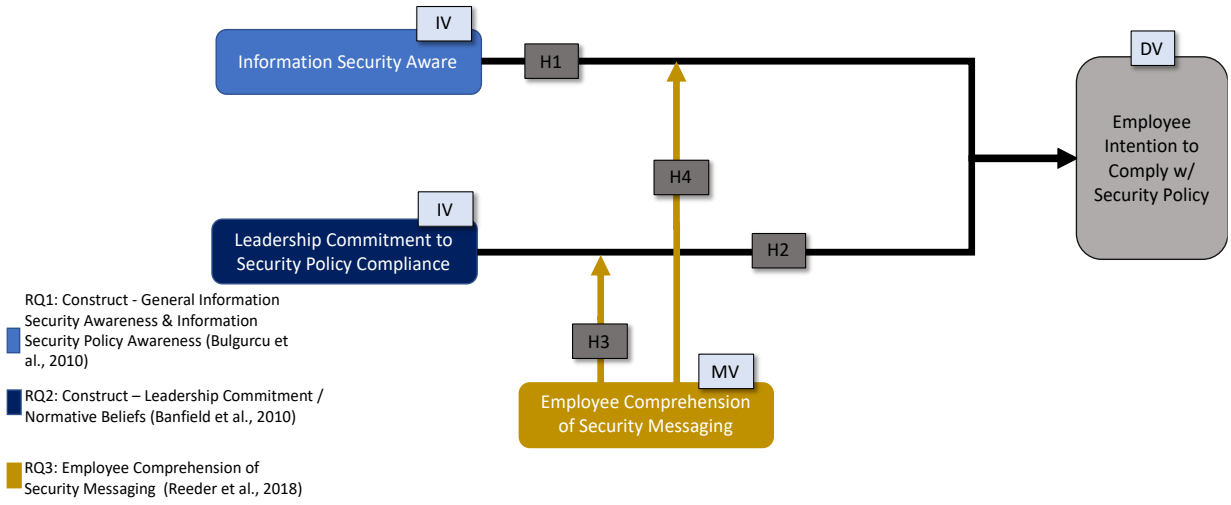

Figure 1: Conceptual Framework for Study

We propose that leadership intent will influence user compliance as leadership intentions as a component of normative beliefs (Banfield 2016; Ifinedo 2012). Normative beliefs have been shown as a component of compliance intentions (Bulgurcu et al. 2010).

H1: The influence of security awareness training is associated positively with employee compliance intentions.

We propose that security awareness training is intentioned on addressing components of information security awareness. A study (Bulgurcu et al. 2010) demonstrated a relationship between security awareness and compliance intentions.

H2: Employee perceptions of leadership intent is associated positively with compliance intentions.

We propose that employee comprehension of security messaging, influences security awareness training's influence on compliance, as degraded comprehension of messaging limits the ability to apply prior knowledge of threats and policy. Security Awareness Training is in part focused on developing accepting attitude toward security policy and leadership commitment as both attitude and normative beliefs factor into compliance intentions (Bulgurcu et al. 2010). Prior research shows that poorly made messaging can limit the ability of users to make right decisions (Reeder et al. 2018). Leadership commitment drives compliance through normative beliefs, we propose that a lack of comprehension of threats and policy via unclear messaging undermines built-in intentions to follow policies and adapt best practices.

H3: Employee comprehension of security messaging and prompts has a moderating effect on security awareness training influence on compliance intentions.

H4: Employee comprehension of security messaging and prompts has a moderating effect on leadership commitment influence on compliance intentions.

Multiple data analysis methods will be applied to the data. The demographic data provides an observational view of the sample. Quantitative summary values will be provided, including multivariate analysis of the various characteristics of the sample. For the remainder of the survey data, because the data are being collected using Likert scales, aggregated data will be used for the analysis after conducting normality testing. Moderated regression will be conducted to test the moderation effects of employee user experiences (UX) with security prompt and their comprehensions of security messaging. Further study will refine approaches to assessing user comprehension and UX factors

Expected Contributions

An acknowledged limitation, given the stage of research, is the ability to assert the contributions of the study. An expected outcome is understanding whether and to what degree the factors of the IS environment influence user security behaviors. This is important in the context of limited investment in security awareness and training efforts, the complexity of human behaviors, and the limited insight into the determinants of user security behaviors. Another potential contribution from this study is to identify directions of further study that incorporate usability and aspects of comprehension related to IS use and security policy enforcement that influence user compliance behaviors. This study can serve as a foundation to look at the effectiveness common approaches to user policy compliance to provide insight toward a future that will include more socially distanced remote work, including embracing new technologies balancing productivity and security.

Conclusion

This study aims to contribute to the understanding of how to best encourage users to comply with security policies, particularly given the increase in remote work. Increasingly, users are the focus of attacks. Identifying factors within the IS that either support or undermine broader security education, policy, and enforcement allows for a holistic framework that drives compliance and user protection.

REFERENCES

Akhawe, D., and Felt, A.P. 2013. "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness," In *Proceedings of the 22nd USENIX Security Symposium (USENIX Security 13)*, pp. 257-272.

Banfield, J.M. 2016. *A Study of Information Security Awareness Program Effectiveness in Predicting End-User Security Behavior*.

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.

Da Veiga, A., and Martins, N. 2015. "Information Security Culture and Information Protection Culture: A Validated Assessment Instrument," *Computer Law & Security Review* (31:2), pp. 243-256.

Eminağaoğlu, M., Uçar, E., and Eren, Ş. 2009. "The Positive Outcomes of Information Security Awareness Training in Companies–a Case Study," *Information Security Technical Report* (14:4), pp. 223-229.

Felt, A.P., Ainslie, A., Reeder, R.W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., and Grimes, J. 2015. "Improving Ssl Warnings: Comprehension and Adherence," In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 2893-2902.

Goodyear, M., Goerdel, H., Portillo, S., and Williams, L. 2010. *Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers*, Available at SSRN 2187412).

Herath, T., and 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.

Höne, K., and Eloff, J. 2002. "What Makes an Effective Information Security Policy?," *Network Security* (2002:6), pp. 14-16.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.

Ki-Aries, D., and Faily, S. 2017. "Persona-Centered Information Security Awareness," *Computers & Security* (70), pp. 663-674.

Krol, K., Moroz, M., and Sasse, M.A. 2012. "Don't Work. Can't Work? Why It's Time to Rethink Security Warnings," In *Proceedings of the 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*: IEEE, pp. 1-8.

Luga, C., Nurse, J.R., and Erola, A. 2016. "Baiting the Hook: Factors Impacting Susceptibility to Phishing Attacks," *Journal of Human-Ccentric Computing and Information Sciences* (6:8).

Manke, S., and Winkler, I. 2013. "The Habits of Highly Successful Security Awareness Programs: A Cross-Company Comparison," *in SecureMemtem*. pp. 1-33.

Nasir, A., Abdullah Arshah, R., and Ab Hamid, M.R. 2019. "A Dimension-Based Information Security Culture Model and Its Relationship with Employees' Security Behavior: A Case Study in Malaysian Higher Educational Institutions," *Information Security Journal: A Global Perspective* (28:3), pp. 55-80.

Orme, S. 2019. *Addressing Issues with Defense-in-Depth, Apts, and Iot with Active Cyber Defense Cycle and Cyber Resilience*. Utica College.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," in *Proceedings of the 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*: IEEE, pp. 156b-156b.

Paliszkiewicz, J. 2019. "Information Security Policy Compliance: Leadership and Trust," *Journal of Computer Information Systems*).

Reeder, R.W., Felt, A.P., Consolvo, S., Malkin, N., Thompson, C., and Egelman, S. 2018. "An Experience Sampling Study of User Reactions to Browser Warnings in the Field," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pp. 1-13.

Saariluoma, P., and Jokinen, J.P. 2014. "Emotional Dimensions of User Experience: A User Psychological Analysis," *International Journal of Human-Computer Interaction* (30:4), pp. 303-320.

Schlienger, T., and Teufel, S. 2002. *Information Security Culture*.

Straub, K.R. 2003. *Information Security Managing Risk with Defense in Depth*, SANS Institute.

Zink, C. 2008, Jun 10. "Why the Brain Follows the Rules.", 1/8/2022, from https://www.scientificamerican.com/article/why-the-brain-follows-the.