Aug 10th, 12:00 AM

Designing a Messaging Strategy to Improve Information Security Policy Compliance

Federico Giovannetti
University of South Florida, fgiovannetti@usf.edu

Alan Hevner
University of South Florida, ahevner@usf.edu

Gert-Jan de Vreede
University of South Florida, gdevreede@usf.edu

Designing a Messaging Strategy to Improve Information Security Policy Compliance

Emergent Research Forum (ERF)

Federico Giovannetti
University of South Florida
fgiovannetti@usf.edu

Alan Hevner
University of South Florida
ahevner@usf.edu

Gert-Jan de Vreede
University of South Florida
gdevreede@usf.edu

Abstract

Lack of employee compliance with information security policies is a key factor driving security incidents. Information security practitioners struggle to enforce policy compliance while employees try to curtail controls in favor of expediency and other perceived business and personal goals. This research-in-progress project utilizes the Design Science Research framework to develop an intervention based on a novel messaging strategy that aims to help information security practitioners improve employees' behaviors through intrinsic motivation, thus increasing compliance with information security policies.

Keywords

Employee compliance, target groups, tailored messaging, leadership, ambassadors, intrinsic motivation.

Introduction

Organizations looking to safeguard the confidentiality, integrity and availability of their information assets commonly implement a rigorous Information Security Program for their employees. A crucial component of such programs is the creation of information security policies, procedures, standards and guidelines that clearly state expected behaviors (Da Veiga and Eloff 2007). Lack of employee compliance with such policies represents a significant challenge to information security practitioners (PricewaterhouseCoopers 2016). However, employees can also help the information security department implement, maintain, and enforce appropriate security controls in a significant way if appropriately informed and motivated. In other words, employees' behaviors can directly affect the information security safeguards of an organization in both negative and positive ways (Da Veiga and Eloff 2010). The objective of this research-in-progress project is to utilize the Design Science Research framework (Hevner et al. 2004) to create a management level intervention to support information security practitioners improve policy compliance across their organization via a novel messaging strategy.

Background

Employee behaviors, specifically their lack of compliance with information security policies, weaken the security posture of organizations (Merhi and Ahluwalia 2019). Over the last decade, there has been substantial research seeking to understand the causes underlying such noncompliance behaviors, but not as much in way of designing management level interventions to be applied by information security practitioners. Influential factors towards compliance are linked to psychological theories that explain individual behavior, such as the Theory of Planned Behavior (Ajzen 1991), the Protection Motivation Theory (Rogers 1975), and the Deterrence Theory (D'arcy and Herath 2011). The challenge is that interventions at the individual level are neither practical to implement nor impactful in a large organizational context. We propose an innovative messaging strategy that includes management-level actions that empower practitioners to improve information security policy compliance.

Research Objectives

As research-in-progress, RO1 and RO2 have been completed, while RO3 is the next phase of this research.

- RO1: Determine key concepts to include in a management level intervention that can help practitioners improve employee behaviors towards compliance with information security policies.
- RO2: Design the intervention based on the key concepts found and validate it by exposing it to subject matter experts and analyzing their feedback.
- RO3: Evaluate the effectiveness of the resulting intervention through a field experiment.

Understanding the security compliance problem space

An extensive literature review was performed to highlight the most common factors that influence employee behaviors towards information security compliance. The complete list of individual and organizational factors, along with their corresponding references, can be found in Giovannetti (2021). Table 1 summarizes these factors. Individual factors are those that originate within the individual's own cognitive system, whereas organizational factors, though they influence individual behavior, have an origin that is external to the individual.

Individual factors	Organizational factors
Self-Efficacy: the belief of the individual about his/her own skills to execute a certain task.	Normative beliefs and group norms (subjective and descriptive). What one perceives from others that must be done, and what others actually do.
Lack of knowledge regarding general information security concepts.	
Lack of knowledge regarding the information security policy.	Leadership support of information security governance. Employees tend to trust leaders with respect to policy security controls.
Inertia: the manifestation of an employee's reluctance to change their current behavior.	
Perception of cost vs. benefit of compliance.	Conflicting goals. Productivity vs. information security compliance. Compliance seen as impediment of business goals.
Perception of the severity and certainty of monitoring and sanctions.	
Perception of the severity, vulnerability, and probability of security incidents.	Organizational commitment. How committed is the employee to the organization?
Unintentional: stress, mood and other affects, operator error.	

Table 1: Factors influencing employee behaviors

The design of the intervention

The intervention consists of a novel messaging strategy for integration into an organizational security awareness program. Its design seeks to address most of the factors listed above and is informed by scientific theories and models considered relevant to the effectiveness of the intervention, namely:

a) The message utility concept from the Single Client Resonance Model (Gill 2015), which claims that for a message to be useful to a receiver, it must pass two important bias filters: the information filter (is this new to me?), and the motivation filter (does it matter to me?).

b) The Fogg Behavior Model (Fogg 2009), which claims that a behavior occurs when three separate factors converge at the same time: motivation, ability, and trigger. In our case, the ability factor is driven by education, not only of information security concepts, but also of the information security policies themselves. That part is considered a separate component of the security awareness program and this research assumes its effectiveness. Triggers to activate the right compliance behavior always exist, whether it is a notification of a new software patch being available or receiving a potential phishing email. Therefore, if the ability is provided through education and the triggers are a constant occurrence, making sure the motivation is there to put that ability into action upon a trigger is an important contributing outcome of this research.

c) The Self-Determination Theory (Ryan and Deci 2000) provides insights on how to increase individual motivation at an organizational level. It claims that there are three basic human needs that trigger

intrinsic motivation: autonomy, competence, and relatedness. Autonomy is the ability and free will to take actions and make decisions, competence is the need to control task outcomes and develop mastery, and relatedness is the need for relationships with others.

Therefore, the messaging strategy consists of delivering a message with sufficient utility to register with the receiver, in a way that stimulates autonomy, competence, and relatedness so that intrinsic motivation is promoted when the triggers appear. Thus, the right behaviors will occur. We propose to design and implement this messaging strategy by following three well-defined steps:

1. Segment the organization into target functional groups with common business activities and goals. For example: Sales & Marketing, Operations, R&D, Finances, and Customer Support.
2. Craft security awareness messaging tailored to each target group, considering their business goals and activities. The message content focus is on understanding "why information security is important to you" at the functional group level.
3. Recruit individuals from both upper management (a.k.a. leadership) and peers (a.k.a. ambassadors) within target groups, as influencers to help deliver the message.

Step #1 addresses the normative beliefs (group norms) factor and aligns with relatedness. Step #2 addresses perceptions-related factors, inertia, and self-efficacy, and aligns with message utility and competence. Step #3 addresses normative beliefs for both types of influencers. For leadership influencers, it also addresses the conflicting goals factor. In the case of peers, it addresses self-efficacy and aligns with autonomy, competence, and relatedness. As an example, consider the targeted functional group being software developers. The tailored message would concentrate on the importance of writing secure code and the personal benefit of acquiring that marketable skill. This messaging should increase awareness in a way that intrinsic motivation is there when positive behaviors are needed upon a trigger, even beyond the software development environment.

The conceptual model that represents this messaging strategy design is in Figure 1. The relationships between constructs in this diagram are considered positive (increases or improves) as shown left to right.

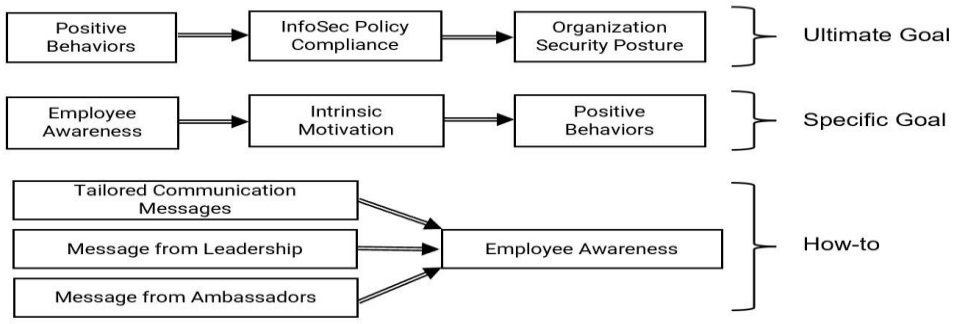

Figure 1: Conceptual Model

Focus Group Study

We validated the theoretical foundation of the messaging strategy through a qualitative Focus Group Study (Eriksson and Kovalainen 2015). It consisted of a one-hour structured discussion with the participation of four multidisciplinary subject matter experts. The discussion was moderated by a professional via video conference. One of the researchers observed the discussion but did not participate. A 10-minute recorded summary of the research was presented to the participants at the start of the session, followed by pre-established discussion topics prompted by the moderator, such as "What methods have you found most effective to increase employees' intrinsic motivation in the workplace?". The complete list of topics is available upon request from the first author. Participants from different disciplines were included in order to elicit discussion that presented different angles and points of view:

- A Chief Learning Officer, experienced in corporate training.
- A Marketing Director for a media company, experienced in messaging.
- An Organizational Psychology Academic Researcher, experienced in organizational climate.

- A Chief Information Security Officer, experienced in running an information security department.

The data generated from the discussion consisted of a video recording and a transcript. The data were analyzed using a Thematic Analysis approach (Clarke and Braun 2017). This analysis included open and selective coding of the transcript to select common themes, complemented by an ethnographic analysis based on observing the video recording several times, looking for the topics that prompted the most engaging exchanges among participants.

Thematic Analysis

Two main themes were extracted from the data, with the second theme containing sub-themes.

Theme #1: Participants favored intrinsic motivation over extrinsic motivation and rewards as more effective than punishment.

Most participants agreed that punitive and reactive approaches to a lack of compliance were not effective. Rewards can play a role, but they are more effective in the form of recognition for "being the hero." Avoiding the shame of being the person who is blamed for a cybersecurity attack is an important motivation factor. All four participants endorsed intrinsic motivation and two endorsed extrinsic motivation, but in the form of rewards. No one endorsed extrinsic motivation in the form of penalties, except in extreme cases of blatantly recurring violations.

Theme #2: Content and Actions are both important to influence the increase of intrinsic motivation among employees.

Relevancy of *content* is extremely important. Security policies, training, and messaging must be relevant. Information security goals should be relevant to corporate goals. Even teaching employees how to be "safe-at-home" should be relevant content that helps with motivation. Consequences are also important. Participants recommended providing real examples of cyber-attacks from other companies to emphasize the importance of strong information security. Several *actions* were listed as important to influence intrinsic motivation, such as:

1. Recruit Influencers: Find champions/ambassadors who can influence their peers.
2. Genuine Leadership Buy-in. Employees can detect when a message is not genuine.
3. Build Morale: A strong and healthy work culture is a necessary foundation before trying to influence motivation towards information security compliance.
4. Manage Repeat Offenders: Individuals that simply refuse to comply, must be swiftly managed.

Results

Based on the themes extracted from the data analysis, the Focus Group study validated our theoretical foundations. It also provided important baseline assumptions that this research must consider before studying its effectiveness in an intervention. One assumption is that the information security policies should be relevant to the organization, as opposed to boilerplate templates. The second assumption is that a strong organizational/work culture is a pre-requisite for an intervention to have a chance to work. In addition, the discussion generated specific messaging ideas such as "safe-at-home" that can be used in future experimental phases of this research.

Experimental Phase

We are designing a field experiment to evaluate the effectiveness of the intervention. We will recruit a host organization and target a specific functional business group for the study. This group will be divided into four treatment groups. Each treatment group will receive a different intervention where two independent variables will be manipulated as a 2x2 field experiment as shown in Table 2. The tailored messaging used during the field experiment, crafted after the functional business group is selected, will be the discussion topic of a second focus group with the same participants. This will ensure that such an important component of the experiment is also validated by subject matter experts.

Using a validated scale (Laycock et al. 2019), the information security culture score (dependent variable) of each treatment group will be measured before and after the intervention. The expectation is that

treatment group #1 will have the highest delta score improvement. The scale uses seven dimensions of information security culture, including attitudes, behaviors, norms, and communication. The score can be calculated per dimension as well as overall. Both calculations will be used in the analysis. Additional conclusions will be driven by statistical analysis within and across treatment groups.

#1: Tailored messaging content including leadership in the delivery	#2: Generic messaging content including leadership in the delivery
#3: Tailored messaging content not including leadership in the delivery	#4: Generic messaging content not including leadership in the delivery

Table 2: Treatment Groups

Conclusion

The novel security compliance messaging strategy has great potential for significant contributions to both research and practice. If the analysis of the field experiment demonstrates an improvement in the information security culture score, practitioners should be able to deploy this prescriptive program to obtain similar benefits. Even if mixed, marginal, or inconclusive results are obtained in the experimental phase, the theoretical foundation of the intervention, as validated through the Focus Group study, can be used to build nascent design theories to create customized security messaging strategies for specific organizations. The use of influencers can also be enhanced using other forms of social control as described in Hsu et al. (2015).

REFERENCES

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.

Clarke, V., and Braun, V. 2017. "Thematic Analysis," *Journal of Positive Psychology* (12:3), pp. 297-298.

D'arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the Is Security Literature: Making Sense of the Disparate Findings," *European Journal of IS* (20:6), pp. 643-658.

Da Veiga, A., and Eloff, J. H. P. 2007. "An Information Security Governance Framework," *Information Systems Management* (24:4), pp. 361-372.

Da Veiga, A., and Eloff, J. H. P. 2010. "A Framework and Assessment Instrument for Information Security Culture," *Computers & Security* (29:2), pp. 196-207.

Eriksson, P., and Kovalainen, A. 2015. *Qualitative Methods in Business Research: A Practical Guide to Social Research*. Sage.

Fogg, B. J. 2009. "A Behavior Model for Persuasive Design," *Proceedings of the 4th international Conference on Persuasive Technology*, pp. 1-7.

Gill, T. G. 2015. "Informing Science: Concepts and Systems." Informing Science Press, pp. 263-301.

Giovannetti, F. 2021. "People-Centric Security Awareness Program," *Proceedings of the International Conference on Information Technologies. IEEE Conference, Rec. #52438*, pp. 51-63.

Hevner, A., March, S. T., Park, J., and Ram, S. 2004. "Design Science Research in Information Systems," *MIS quarterly* (28:1), pp. 75-105.

Hsu, J. S.-C., 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.

Laycock, A., Petrič, G., and Roer, K. 2019. "The Seven Dimensions of Security Culture." KnowBe4 Research Paper.

Merhi, M. I., and Ahluwalia, P. 2019. "Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security," *Computers in Human Behavior* (92), pp. 37-46.

PricewaterhouseCoopers. 2016. "Key Findings from the Global State of Information Security Survey," PricewaterhouseCoopers Report.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology* (91:1), pp. 93-114.

Ryan, R. M., and Deci, E. L. 2000. "Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being," *American psychologist* (55:1), p. 68.