Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2019 Proceedings | Midwest (MWAIS)

5-21-2019

Developing an Unintentional Information Security Misbehavior Scale (UISMS)

Forough Nasirpouri Shadbad
Oklahoma State University, nasirpo@okstate.edu

David Biros
Oklahoma State University, david.biros@okstate.edu

Developing an Unintentional Information Security Misbehavior Scale (UISMS)

Work-in-Progress

Forough Nasirpouri Shadbad
Oklahoma State University
nasirpo@okstate.edu

David Biros
Oklahoma State University
david.biros@okstate.edu

ABSTRACT

Although the number of security incidents and data breaches caused by humans increasing, no well-established scale exists to measure individuals' information security misbehaviors in interaction with the information systems. Knowing that individuals' misbehaviors differ in term of intentions, in this research, we identify important unintentional behaviors that users may threaten security through non-malicious actions and develop a unified information security misbehaviors scale aiming to exhibit acceptable psychometric properties. We believe such a measurement tool can help researchers to investigate various causes of human errors in system-user interactions and guide practitioners to make strategic decisions in organizations. Our goal is to build a set of Likert scale questions by exploring literature, security experts' advice, or adopting security policies implemented in organizations to find out what type of individuals' mistakes may lead to unintentional security misbehaviors.

Keywords

Unintentional behaviors, malicious intentions, psychometrics, security behavior

INTRODUCTION

In recent decades, our lives either personal or professional depend more upon information systems, computers, and advanced technologies; and the emergence of the Internet in the 21st century has increased tremendously the concerns regarding the protection of personal or organizational information from cyber attacks due to the risks associated with security incidents such as financial loss or loss of credibility (Cavusoglu, Cavusoglu, & Raghunathan, 2004). Scholars attempted to explore and investigate the technical, contextual, managerial, and behavioral aspects on information security (Zafar & Clark, 2009) to suggest possible solutions or provide feasible guidelines to reduce threats and security incidents; for example, improving system designs (Ravi, Raghunathan, Kocher, & Hattangady, 2004), training and increasing users' information security awareness (Puhakainen & Siponen, 2010) or motivating employees to comply with security policies (Bulgurcu, Cavusoglu, & Benbasat, 2010). Although all the aspects of security research are worth to exploring, the focus on technical issues has received more attention than behavioral information security research (Crossler et al., 2013); while studies have shown that the nature of security incidents are more due to human error than technical vulnerabilities (Ayyagari, 2012).

Behavioral information security seeks to investigate individuals' behaviors dealing with information systems in order to protect information (Crossler et al., 2013). According to the literature, humans violate security either intentionally (e.g., insiders with harmful and malicious intentions to hack or steal data for personal gains) or unintentionally without any harmful intentions (e.g., accidental disclosure of sensitive data via the internet) (Greitzer, Strozer, Cohen, Bergey, et al., 2014). Baker et al. (2010) reported that approximately half of the security violations occur within the organizations by insiders or internal employees. According to "Intelligent ID" (2017), 75% of insider threats are accidental or due to unintentional activities. Also, "Statista" (2018), the statistics portal, reported that the number of data breaches has been increasing in recent years and exposed records reached the highest number in the year 2017 which nearly was about 179 million records and negatively affected the business sectors. Wilshusen (2015) also acknowledged that the number of security incidents has been increasing each year since 2006 which corresponds to Statista's report. These huge number of data breaches prompt researchers to explore the root causes of such incidents.

Although information security has drawn the attention of many scholars, behavioral information security research suffers from a lack of potential studies, especially regards to unintentional insider threats (Crossler et al., 2013). For example, it is

not clear yet what human factors contribute to a rise in individuals' accidental misbehaviors. Particularly, because of the sensitivity of the security context, observing human behavior is not easily possible. One solution is to measure an individual's security-related behaviors indirectly using scales through self-reported study. Since the number of accidental security incidents by humans is increasing, having such a scale can be helpful to study potential factors causing security threats. To the best of our knowledge, no scales exist to measure computer-users' accidental behaviors (except for two scales which will be discussed in the next sections). To this end, our goal is to develop a scale to estimate unintentional information security misbehaviors following scale development instructions suggested by the literature.

Unintentional Information Security Misbehaviors

According to the literature, humans violate security either intentionally (e.g., insiders with harmful and malicious intentions to hack or steal data for personal gains) or unintentionally without any harmful intentions (e.g., accidental disclosure of sensitive data via the internet) (Greitzer, Strozer, Cohen, Bergey, et al., 2014). Many scholars attempt to define unintentional security threats and provide evidence of negative consequences of accidental misbehaviors (Ayyagari, 2012; Collins, 2016; Crossler et al., 2013; Greitzer, Strozer, Cohen, Moore, et al., 2014; Kraemer & Carayon, 2007). Adopting the literature, we define unintentional information security misbehaviors as a person who has the authorization to access an organization's systems or data, and unwillingly (through accidental action and without any harmful intention) threaten information security. It is important to point out that we distinguish non-malicious misbehaviors from unintentional misbehaviors, although both groups are involved in non-harmful intentions. According to Guo, Yuan, Archer, and Connelly (2011) non-malicious security violations are non-harmful intentional end-user behaviors which are done voluntary and through conscious decisions. For example, employees may use colleagues' computers at work although they are aware of possible security risks, or they may ignore organizational security policies with their own will. However, unintentional misbehaviors are like forgetting locking computers or accidentally clicking on phishing links. Our main focus in this paper is to investigate individuals' unintentional misbehaviors.

Developing Unintentional Information Security Misbehaviors Scale (UISMS)

Ayyagari (2012) claimed that organizational factors and human factors are two types of possible causes that contribute to unintentional information security threats. Work setting, management systems, technical issues, and job stress impact employees' performance as organizational factors; and employees' health and psychological status, lack of security awareness or personality traits may influence their behavior to do unintentional behaviors. One of the best methodologies to study these potential factors and explore why employees exhibit such misbehaviors is to monitor employees and observe their actual behaviors (Crossler et al., 2013). However, because of the sensitivity of security-related data, access to the actual behavior of individuals is very difficult to acquire. For example, companies tend to avoid publicly announcing or reporting any negative security events. Therefore, as authors state "there is a dearth of actual behavior reporting in the current behavioral information security literature" (Crossler et al., 2013, p. 95). One of the suggested solutions by scholars is to use scales as a substitute for actual observation. When a phenomenon is hard to observe directly, a good way is to measure it through scales (DeVellis, 2016). Constructing a valid and reliable scale can be very helpful to study human behaviors as it has been implemented in the various discipline (e.g., psychology, social science) and assumed to be suitable for security context, too.

Since, unintentional information security misbehaviors are very hard to observe, having a scale for that can be very helpful to study human behaviors in the security domain. Behavioral information security researchers mainly focus on explaining different types of security threats, defining human behaviors (or misbehaviors) in various contexts, or providing multiple examples of such misbehaviors. Unfortunately, behavioral information security literature has been lacking such a measurement tool to assess individuals' unintentional misbehaviors. Previously, Egelman and Peer (2015) and Hadlington (2017) attempted to develop security-related scales known as "Security Behavior Intentions Scale (SeBIS)" and "Risky Cybersecurity Behaviors Scale," respectively.

Egelman and Peer (2015) developed a 16-item scale to measure intentions to comply with computer security advice consists of 4 subscales that measure attitudes towards password choosing, device securement, staying up-to-date, and proactive awareness. First, this scale does measure unintentional misbehaviors. Because in some of the items, users are assumed to already have knowledge about security actions and attempt to measure their intention to how they try to comply to these security behaviors (e.g., If I discover a security problem, I continue what I was doing because I assume someone else will fix it). Second, we believe this scale cannot reflect individuals' actual behaviors since it focuses on their intentions toward a behavior. They also acknowledge that "while SeBIS is reliable and stable over time, it is not clear how well it correlates with

actual security behaviors since it only measures intentions" (Egelman and Peer, 2015, p. 2881). Studies suggest that the measurement of actual behaviors are preferred rather than intentions since intentions do not always lead to behaviors (Mahmood, Siponen, Straub, Rao, & Raghu, 2010). So, we will strive to be careful in wording the items to possibly reflect their actual behavior.

Hadlington (2017) developed a 20-item online risky behavior scale. One limitation of this scale is that it is restricted only to the online environment. While there are some behaviors which deal with offline computer use like leaving the systems unlocked. The other drawback of this scale is that the items are mixed of personal and professional behaviors and they are not well categorized. This may limit validation of studies and theoretical models in information security contexts which are only observing employees' behavior at the workplace. Also, except for Cronbach's alpha, the reliability and validity of this construct were not reported which may bring doubts and concerns, and question further research using the scale.

Hence, our goal is to develop a self-reported scale to capture all possible misbehaviors which individuals do in interaction with computers or information systems either in an online or offline environment. We endeavor to construct a new scale (UISMS) to assess individuals' actual behaviors which are done totally unintentionally or by honest mistakes but may increase the risk of security threats. For this purpose, we will follow construct development procedures suggested by Netemeyer, Bearden, and Sharma (2003).

Methodology

According to Netemeyer et al. (2003), scale development consists of four steps: (1) construct definition and explaining the content in details ; (2) generating all possible measurement items; (3) performing appropriate analysis to refine the scale; and (4) finalizing the scale by testing the reliability and validity. In the following, we briefly explain how we are going to apply each of these steps.

Construct definition. We will explore behavioral information security literature to distinguish intentional and unintentional security behaviors to explain the construct in details and provide a unique definition for unintentional information security misbehaviors and identify possible antecedents of those actions.

Item generation. In order to generate an initial set of items, as a starting point, we plan to review behavioral information security literature or security policies offered in organizations to identify security-related activities. These documents can guide us to understand what security actions are considered accepted behaviors or violations and how they relate to intentional or unintentional behaviors. Also, we may follow it with qualitative research by interviewing security experts or computer users. We believe real world examples (or any possible security incidents occurred at workplaces by users) can help us to achieve our goal to best determine users' misbehaviors.

Scale refining. To test how initial items work, we need to conduct a pilot study. Using the collected data, we will check for reliability, the applicability of items, acceptable variance, and the correlation between items to decide accordingly to change or refine the items.

Finalizing the scale. We will continue to recollect data as much as needed to perform required analysis like Exploratory Factor Analysis, Confirmatory Factor Analysis, and other required analysis in order to test the reliability and validity of our scale. Ultimately, we will finalize UISMS consists of appropriate questions reflecting unintentional misbehaviors.

CONCLUSION

In order to study individuals' information security misbehaviors and explain why and how security incidents occur in organizations (e.g., what personal or environmental factors cause such misbehaviors), having a scale to measure unintentional or accidental behaviors can be very beneficial. Understanding the reasons of human errors is a far-reaching action to protect systems from security threats. Therefore, in this study, we aim to develop UISMS to measure end-users' unintentional misbehaviors regarding security activities. We hope such this scale help researchers to investigate various factors of human errors in system-user interactions and also guide practitioners to make strategic decisions in organizations.

REFERENCES

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security, 8*(2), 33-56.

Baker, W., Goudie, M., Hutton, A., Hylender, C., Niemantsverdriet, J., Novak, C., . . . Sartin, B. (2010). Verizon 2010 Data Breach Investigations Report. Verizon Business. In.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *Mis Quarterly, 34*(3), 523-548.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. J. C. o. t. A. f. I. S. (2004). Economics of ITSecurity Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems, 14*(1), 3.

Collins, M. (2016). *Common sense guide to mitigating insider threats (No. CMU/SEI-2016-TR-015).* Retrieved from

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security, 32*, 90-101.

DeVellis, R. F. (2016). *Scale development: Theory and applications* (Vol. 26): Sage publications.

Egelman, S., & Peer, E. (2015). *Scaling the security wall: Developing a security behavior intentions scale (sebis).* Paper presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.

Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A., & Mundie, D. (2014). *Unintentional insider threat: contributing factors, observables, and mitigation strategies.* Paper presented at the 2014 47th Hawaii International Conference on System Sciences (HICSS).

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). *Analysis of unintentional insider threats deriving from social engineering exploits.* Paper presented at the Security and Privacy Workshops (SPW), 2014 IEEE.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. J. J. o. m. i. s. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems, 28*(2), 203-236.

Hadlington, L. J. H. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346.

IntelligenID (2017). 75% of Insider threats are accidental. Retrieved frorm https://intelligentid.com/75-insider-threats-accidental/

Kraemer, S., & Carayon, P. J. A. e. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics, 38*(2), 143-154.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. J. M. q. (2010). Moving toward black hat research in information systems security: an editorial introduction to the special issue. *Mis Quarterly, 34*(3), 431-433.

Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). *Scaling procedures: Issues and applications*: Sage Publications.

Puhakainen, P., & Siponen, M. J. M. Q. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, 757-778.

Ravi, S., Raghunathan, A., Kocher, P., & Hattangady, S. J. A. T. o. E. C. S. (2004). Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems (TECS), 3*(3), 461-491.

Statista (2018). Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions). Retreived from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Wilshusen, G. J. G. H. (2015). Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems, 24*(1), 34.