Journal of Database Management
Volume 31 • Issue 2 • April-June 2020

Experience Matters:
The Role of Vicarious Experience in Secure Actions

Leigh A. Mutchler, James Madison University, Harrisonburg, USA
Merrill Warkentin, Mississippi State University, Starkville, USA

ABSTRACT

Information systems security is a major organizational concern. This study examines the role of vicarious experience on an individual's behavioral intent to perform a secure recommended response. The protection motivation theory model is expanded to include vicarious experience, which was examined through the separate constructs of vicarious threat experience and vicarious response experience. This study closes a gap in the literature by including vicarious experience in the PMT model and confirming its role as a significant direct influence on the PMT threat and coping constructs, and thus on the PMT model's ability to explain the variance of an individual's intent to perform secure behaviors. Additionally, vicarious experience measures were multi-item reflective scales rather than the single item measures that are more typically used to measure experience. Implications for theory and practice are discussed.

KEYWORDS

Information Security, InfoSec, Moderation, PMT, Protection Motivation Theory

INTRODUCTION

The numbers of information system (IS) security incidents continue to rise as do the recovery costs (Ponemon, 2017; Vormetric, 2016). The employee is known to be the weakest link in the efforts to protect organizational data assets. Although practitioners and academic researchers are focusing their attention to strengthen that link (Kolkowska, Karlsson, & Hedström, 2017; Moody, Siponen, & Pahnila, 2018; Sharp, 2017; Sophos, 2017), employees continue to be the most commonly identified offender of security incidents (PwC, 2014). Ernst and Young (EY) reported that 73% of all organizations are concerned that their employees possess poor security awareness (EY, 2016), and that 57% of all attacks against an organization's data assets were perpetrated by employees. Interestingly, the underlying causes of 38% of those attacks were due to employee mistakes or poor understanding of protective behaviors (EY, 2014).

In the workplace, controls restrict employee behaviors, guiding them and at times forcing them to perform secure actions. However, as many as 43% of individuals working in the U.S. spend some of their time working remotely (Chokshi, 2017). During such times, individuals often have discretionary control regarding decisions about security. These individuals must make their own choices about

DOI: 10.4018/JDM.2020040101

whether or not to use antivirus software, whether or not to regularly back up data, which websites to visit, which emails to open, whether or not to patch (update) their software, and so on. Further, because work systems are often being accessed from an employee's home, using their personally owned and controlled devices, the choices they make may pose serious risks to the organization. Many organizations are implementing bring your own device (BYOD) programs, allowing employees to use their personal mobile devices for work purposes (Lee, Warkentin, Crossler, & Otondo, 2016). Those personal devices will likely hold organizational data but may be used anywhere and will be primarily managed by the employee. Last, as much as 20% of U.S. workforce is made of contract employees (Noguchi, 2018), and the perceptions held by these individuals about information security compliance may differ due to their non-full-time employee status (Sharma & Warkentin, 2018). Regardless, in all such cases – individuals engage in choices regarding workplace information security. For this reason, there is an important need for researchers and security professionals to examine and understand individual secure behaviors (Anderson & Agarwal, 2010; Hanus & Wu, 2016; Liang & Xue, 2010; Talib, Clarke, & Furnell, 2010; Tsai et al., 2016).

An individual's experiences are known to be strong influences on their decisions, attitudes, beliefs, and behavioral intent (Ajzen & Fishbein, 1969; Petter, DeLone, & McLean, 2013). For example, making the choice to perform a secure behavior such as regularly backing up personal data will likely be influenced by prior experiences with that behavior. Whereas direct experiences tend to make the greater impact on decision making (Ajzen & Fishbein, 1969), experiences gained vicariously can also be important and therefore should not be ignored. Vicarious experiences gained by observing others or through communications with friends, relatives, and peers in social settings and in the workplace can lead to a better understanding of security issues and or greater confidence to perform secure behaviors (Warkentin, Johnston, & Shropshire, 2011). Experience is an important construct within the IS field (Aguirre-Urreta & Marakas, 2008), but too few studies have examined the relationship between vicarious experience and secure behaviors. This leads to the research question: What role does an individual's vicarious experience with an information security threat and a secure response play in his or her intention to perform the recommended secure response to the threat?

To gain a better understanding of the role that vicarious experience plays in the behavioral intent to perform secure actions, an online survey was conducted, followed by the test of a research model supported by the protection motivation theory (PMT) (Maddux & Rogers, 1983). This study fills a gap in the literature and contributes to the stream of PMT research by testing the influence of vicarious experience within the PMT model. The presentation of this work continues with a discussion of the background, the model and method, the results, and the conclusions along with insights for future research.

BACKGROUND AND LITERATURE REVIEW

Protection Motivation Theory

The PMT (Maddux & Rogers, 1983) is a good theoretical fit for security research because it explains that when individuals are confronted with a threat, they will assess the threat (specifically the threat's severity and their susceptibility to it), seek out an available response to the threat, and make a behavior choice. A healthy stream of InfoSec research has applied PMT to IS security issues including, secure computing practices (Anderson & Agarwal, 2010; Crossler & Bélanger, 2014; Hanus & Wu, 2016), use of anti-malware software (Garung, Luo, & Liao, 2009; Johnston & Warkentin, 2010; Lee & Larsen, 2009), online safety (Banks, Onita, & Meservy, 2010; Marett, McNab, & Harris, 2011; Tsai et al., 2016), and data backup (Crossler, 2010; Malimage & Warkentin, 2010). The research models and the measures tested vary but most include the PMT constructs of threat severity, threat susceptibility, response efficacy, self-efficacy, and response cost (Boss, Galletta, Lowry, Moody, & Polak, 2015) as illustrated in the PMT schema in Figure 1.