8-10-2023

Cognitive Biases in Security, Education, Training, and Awareness: Good vs. Bad

Hwee-Joo Kam
University of Tampa, hkam@ut.edu

Matthew Jensen
University of Oklahoma, mjensen@ou.edu

Cognitive Biases in Security, Education, Training, and Awareness: Good vs. Bad

TREO Talk Paper

Hwee-Joo Kam
University of Tampa
hkam@ut.edu

Matthew Jensen
University of Oklahoma
mjensen@ou.edu

Abstract

This study argues that cognitive biases produce a complex set of outcomes in security, education, training, and awareness (SETA) programs. Mainly, cognitive bias *"produces representations that are systematically distorted compared to some aspect of objective reality"* (Haselton et al., 2015, p. 968). Several information systems (IS) studies examined cognitive biases (Fleischmann et al., 2014; Liedtka, 2015), proposing that cognitive biases negatively affect system design and development (Arnott, 2006; Kirs et al., 2001), incident response handling (Ceric & Holland, 2019), and information security (InfoSec) management (Jalali et al., 2019; Pfleeger & Caputo, 2012). Because cognitive biases also create a negative impact on training and education (Carpena et al., 2019; Payne, 2006), we argue that cognitive biases could adversely affect employees' learning about cyberattacks prevention presented in SETA programs. For example, employees in an organization may have witnessed few cyberattacks and even when they spotted one, they felt it was easily defused. Therefore, their perceptions about cyberattacks may dissuade them from taking SETA programs seriously. This example demonstrates representativeness or optimism biases (Arnott, 2006; Tversky & Kahneman, 1974). In this context, we examine how cognitive biases would deter employees from engaging in SETA programs related to cyberattack prevention. Our first research question is:

RQ1: How would cognitive biases deter employees from engaging in SETA programs?

Ironically, there can be some "goods" brought by cognitive biases (Schwenk, 1986). Rather than fighting them, organization leaders could create an environment in which cognitive biases would steer employees toward performing actions that benefit them and the organization (Schwenk, 1986). For example, leaders could present vivid examples (i.e., presentation bias) (Martin & Powers, 1983) of data breaches that occurred within the organization to emphasize the importance of SETA initiatives. Moreover, leaders could alter the illusion of management control (i.e., illusion bias) (Schwenk, 1986) by informing employees of existing monitoring tools or could alter perceptions of attack prevalence (i.e., representativeness bias) by conducting mock attacks or training exercises with employees. Altering the environment will likely change perceptions that feed cognitive biases. Rather than fight against biases, such interventions may bring cognitive biases to serve organizational security needs, propelling employees to engage in security behaviors. This notion is consistent with perceived mandatoriness (Boss et al., 2009) in that employees would take security seriously when organization leaders emphasized the criticality of security. However, unlike prior studies, we conceptualize cognitive biases in a context of management interventions primarily because organization leaders control information flow and dissemination. As a result, organization leaders could shape information flows during SETA campaigns (and their follow up) to foster cognitive biases that support positive organizational security outcomes. Based on the proposition that cognitive biases may engender some positive outcomes (Åstebro et al., 2007; Cristofaro et al., 2021; Levin et al., 1998; Martin & Powers, 1983; Schwenk, 1986; Simon et al., 2000), we form the second research question:

RQ2: How can organization leaders create an environment in which cognitive biases promote engagement with SETA programs and contribute to organizational security?

This study contributes to the IS literature by sharing how information flows could be altered to limit cognitive biases that exacerbate security weaknesses and foster cognitive biases that support organizational security. To the best of our knowledge, this is one of very few studies that adopts a nuanced view of cognitive biases in a SETA context. Using a longitudinal experiment, we plan to capture participants' perceptions and corresponding behaviors to mark any changes and the consequences of those changes.