12-12-2021

Examining information systems security behavior of employees

JOTI KAUR
The University of North Carolina at Greensboro, j_kaur2@uncg.edu

Gurpreet Dhillon
IT and Decision Sciences, gurpreet.dhillon@unt.edu

Winnie Picoto
w.picoto@iseg.ulisboa.pt

TREO
Technology, Research, Education, Opinion

Examining information systems security behavior of employees

A mixed-methods research

Joti Kaur (j_kaur2@uncg.edu); Gurpreet Dhillon (gurpreet.dhillon@unt.edu); Winnie Ng Picoto (w.picoto@iseg.ulisboa.pt)

Majority of organizations are continuously under threat because of employees' mishandling of sensitive information. While information systems (IS) security is an integral part of employee responsibility, failure to follow security procedures and other employee psychological capabilities results in sub-par security behaviors. There are also numerous instances where regular employees have inadvertently and without malicious intent caused a data breach or a security incident (for example, the Federal Deposit Insurance Corp. data breach in March 2016, Home Depot data breach in October 2020). Therefore, it is crucial to examine the factors that can enhance the IS security behavior of employees. Researchers in IS have extensively studied IS security intention of employees, but the behavioral aspect of employees has not received much attention. Both theoretical and empirical studies in the past have focused on technical, individual, and social factors that could provide additional information on how to improve intentions to keep sensitive information secure. Studies have also explored practices that keep employees away from risky security behaviors by better user awareness and training (e.g., see Siponen et al. 2014). However, scholars in IS are beginning to recognize that although organizational IS security is increasingly dependent on the employees, we need deeper understanding on the factors that influence the behavior of employees towards IS security. In this research, we develop and empirically test a theory-based model that examines the IS security behaviors using the conceptualization of IS security performance and IS security competence. We argue that employees' IS security behavioral outcomes are a function of their *thriving* in their work environment. *Thriving* is an important domain of inquiry as it is the subjective experience that allows employees to develop in a positive manner. We also examine how work context (keeping sensitive information secure) is facilitated by *agentic work behaviors*. Using a mixed-methods design, we develop our theory-based model followed by a quantitative survey-based study to validate our model. This research provides deeper theoretical understanding for information systems security behavioral outcomes. We theoretically combine the knowledge based on two prominent organizational studies aspects – namely *thriving at work* and *agentic work behaviors* – and examine them in the context of IS security. At a practical level, this research would help managerial functions formulate better organizational security policies that would result in improved IS security behaviors among employees.

References

Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp. 217-224.