Association for Information Systems

AIS Electronic Library (AISeL)

SAIS 2020 Proceedings

Southern (SAIS)

Fall 9-11-2020

Roles of Social and Organizational Climate Factors in Discouraging Employee Engagement in Nonmalicious Counterproductive Computer Security Behaviors

Princely Ifinedo
Brock University, pifinedo@brocku.ca

ROLES OF SOCIAL AND ORGANIZATIONAL CLIMATE FACTORS IN DISCOURAGING EMPLOYEE ENGAGEMENT IN NONMALICIOUS COUNTERPRODUCTIVE COMPUTER SECURITY BEHAVIORS

Princely Ifinedo
Brock University
pifinedo@brocku.ca

ABSTRACT

The objective of this paper was to provide information on the influence of relevant social-related and organizational climate factors in discouraging employee engagement in nonmalicious counterproductive computer security behaviors (CCSB). To that end, this study adopts elements from the social cognitive theory and the organizational climate perspective to guide the research project. A research model is proposed to show that the factors of social support, observational learning/modeling and the sub-constructs of organizational climate (i.e., formalization, training, clarity of organizational goals, and involvement) have negative associations with employees' urge to participate in CCSB. Data collection took place in ten diverse countries and analysis of the data is in progress.

KEYWORDS

Information systems security, nonmalicious counterproductive computer security behaviors, social cognitive theory, organizational climate, employee, survey

EXTENDED ABSTRACT

Current information continues to point to the increasing danger posed by negligent insiders (Guo et al., 2011). It is worth noting that a negligent insider who engages in nonmalicious IS security practices is not the same as a malicious insider or outsider who engages in acts that harm organizational IS infrastructure (Loch et al., 1992). The focus of this study is on the former. This study maintains that nonmalicious acts (e.g., visiting non-work related web sites) and malicious behaviors (e.g., engaging in computer fraud, data leakages, and theft) are different issues requiring separate attention. While prior research has educated on insiders' malicious behaviors, nonmalicious IS security behaviors remain underexplored in the extant IS security literature (Guo et al., 2011; Ifinedo, 2019).

Prior studies have indicated that social-related and organizational climate factors are pertinent in shaping behaviors with regard to safe computing and IS security behaviors (Guo et al., 2011). To add to growing research in the area, this study adopts elements from the social cognitive theory and the organizational climate framework to guide the research project. A research model is proposed with hypotheses indicating that the factors of social support, observational learning/modeling and the sub-constructs of organizational climate have negative associations with employees' urge to engage in CCSB. To test the research model, a survey of employees knowledgeable about CCSB was used. The survey was administered in ten countries by a data research company. Data analysis will be carried out with structural equation modeling. Results from the pilot test confirmed that social support and organizational climate have negative associations with employees' intention to engage in CCSB. No support was found for the impact of observational learning/modeling on employees' intentions to engage in CCSB at work.

REFERENCES

1. Guo, K.H., Yufei, Y., Archer, N.P. & Connelly, C.E. (2011). Understanding nonmalicious security violations in the workplace: a composite behavior model. *JMIS*, 28(2), 203-236.
2. Loch, K.D., Carr, H.H., & Warkentin, M.E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, 16(2), 173-186.
3. Ifinedo, P. (2019). End user nonmalicious, counterproductive computer security behaviors: concept, development, and validation of an instrument. *Security & Privacy*, 2, 3, e66.