A Study of Employees’ Self-Reported Cybersecurity Behaviors

Wu He
Old Dominion University
Norfolk, VA, USA
whe@odu.edu

Mohd Anwar
North Carolina A&T State University,
Greensboro, NC, USA
manwar@ncat.edu

Ivan Ash
Old Dominion University
Norfolk, VA, USA
iash@odu.edu

Xiaohong Yuan
North Carolina A&T State University,
Greensboro, NC, USA
xhyuan@ncat.edu

Ling Li
Old Dominion University
Norfolk, VA, USA
lli@odu.edu

Li Xu
Old Dominion University
Norfolk, VA, USA
lxu@odu.edu

Abstract

The information security community has come to realize that the weakest link in a cybersecurity chain is human behavior. To develop effective cybersecurity training programs for employees in the workplace, it is necessary to identify factors that contribute to employees’ cybersecurity behaviors and then build a theoretical model to understand how these factors affect employees’ self-reported security behavior in the workplace. Supported by a grant from the National Science Foundation (NSF), we developed a model for studying employees’ self-reported cybersecurity behaviors, and conducted a survey study to investigate the cybersecurity behavior and beliefs of employees. Five-hundred-seventy-nine employees from various U.S. organizations and companies completed an online survey with 87 items carefully designed by six experts in cybersecurity, information technology, psychology, and decision science.

The results from statistical analysis of the cybersecurity behavior survey questionnaire will be presented in this TREO Talk. Some of the key findings include:

- Prior Experience was correlated with self-reported cyber security behavior. However, it was not identified as a unique predictor in our regression analysis. This suggests that the prior training may indirectly affect cybersecurity behavior through other variables.
- Peer Behavior was not a unique predictor of self-reported cybersecurity behavior. Perceptions of peer behavior may reflect people’s own self-efficacy with cybersecurity and their perceptions of the benefits from cybersecurity behaviors.
- The regression model revealed four unique predictors of self-reported cybersecurity behavior: Computer Skill, Perceived Benefits, Perceived Barriers, and Security Self-efficacy. These variables should be assessed to identify employees who are at risk of cyber attacks and could be the target of interventions.
- There are statistically significant gender-wise differences in terms of computer skills, prior experience, cues-to-action, security self-efficacy and self-reported cybersecurity behaviors. Since women’s self-efficacy is significantly lower than men, women’s self-efficacy may be a target for intervention.