Improving Security Behavior of Employees in Cyberspace through Evidence-based Malware Reports and E-Learning Materials

Wu He, Ling Li, Li Xu, & Ivan Ash, Old Dominion University
Mohd Anwar & Xiaohong Yuan, North Carolina A&T State University
http://securitybehavior.com

The objectives of this project are: 1) to identify factors that contribute to employees' cyber security behavior and then build a theoretical model to understand how these factors affect employees' self-reported security behavior; 2) to develop new, evidence-based e-learning materials in order to improve employees' security awareness and capabilities; 3) to compare different evidence-based training methods and find out the most effective training method through a controlled experimental study; 4) to disseminate knowledge, research methodologies, and training materials to companies & educational institutions.

Approach

We conducted a thorough literature review on articles related to behavioral information security and designed a survey as the instrument for data collection. This survey instrument has gone through several rounds of internal revisions and refinement. The survey includes 87 Likert items collecting data to measure an individual's computer skills, self-efficacy, prior experience with computer security practice, and other constructs depicted in the proposed model (see Fig. 1).

We conducted an online survey to 481 employees from various organizations. Detailed data analysis was conducted to validate the proposed model afterwards. Furthermore, we developed new evidence-based e-learning materials in order to improve employees' security awareness and capabilities. An experimental study to compare different evidence-based training methods and measure their effectiveness is under way.

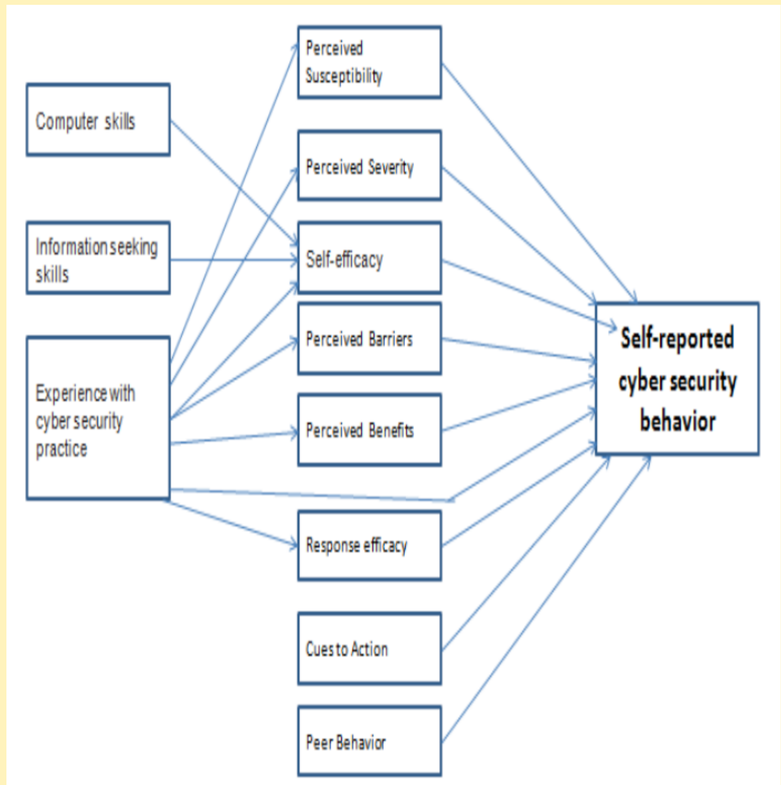

Fig. 1. Cybersecurity behavior model

Employment Status and Cybersecurity Behaviors

There was a negative correlation between perceived vulnerability (PV) and Employment status, which was statistically significant (rpb = -.24, n = 482, p = .0). There was also a statistically significant negative correlation between prior experience with cyber security practice (PE) and employment status, (rpb = -.27, n = 482, p = .0) as well as between computer skills (CS) and employment status (rpb = -0.17, n = 482, p = .0).

Gender Difference and Employees' Cybersecurity Behaviors

Our results show that gender has some effect in security selfefficacy (r=-.435, p< .001), prior experience (r=-.235, p< .001) and computer skills (r=-.198, p< .001) and little effect in cues to action (r=-.152, p< .001) and self-reported cybersecurity behaviors (r=-.152, p< .001).

Peer behavior's Impact on Employees' Cybersecurity Behaviors

Our results show that the influence from peer behavior and employees action experience of cyber security is an important factor for improving cyber security behavior in organizations. Peer behavior positively affects cue to action, which positively impacts employees' action experience. Employees' action experience then would have positive impacts on their threat perception and response perception. As a result, employees' threat perception and response perception are positively related to their cyber security behavior. This process is a chain reaction.

Developing and Using Evidence-based E-learning Videos for Cybersecurity Education

To help people improve their knowledge and security self-efficacy in dealing with malware attacks that are relevant and meaningful to their organizations, we recently developed over 30 e-learning videos based on the major types of malware attacks we captured using the state-of-the-art anti-malware solution. Specially, we deployed leading anti-malware tools provided by FireEye and the Wedge Networks to detect a variety of malware that were attacking the network of our campuses in the past two years. Both anti-malware tools detected and captured a variety of malware during the research period. As the result, we identified the popular malware that affectour employees' computers and then created some elearning videos along with relevant materials for the selected malware such as Trojan.Generic, Trojan.Zbot, malicious URL, SQL injection attack, ransomware and Win Adware Agent.

The preliminary evaluation results of the videos are quite positive and indicate that these evidence-based e-learning videos have great potential to increase users' security self-efficacy.

Comparing different evidence-based training methods (ongoing; so far we collected data from over 50 subjects)

Malware Report	E-learning Materials/Instruction	
	Yes	No
Yes	Increased perceived susceptibility Increased self-efficacy Largest increase in security intentions Largest decrease in malware attacks	Increased perceived susceptibility Small or no change in security intentions Small or no change in malware attacks
No	Increased self-efficacy Small or no change in security intentions Small or no change in malware attacks	No changes in susceptibility, self-efficacy, security intentions, or malware attacks.

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Jan. 9 -11th 2017, Arlington, Virginia