8-9-2021

Incorporating Subjective Initiative Module into Security Education, Training, and Awareness Programs

Yuelin Zhu
University of Memphis, yzhu6@memphis.edu

Qiunan Zhang
University of Memphis, qzhang4@memphis.edu

Xihui Zhang
University of North Alabama, xihui.zhang@yahoo.com

Recommended Citation

Zhu, Yuelin; Zhang, Qiunan; and Zhang, Xihui, "Incorporating Subjective Initiative Module into Security Education, Training, and Awareness Programs" (2021). *AMCIS 2021 TREOs*. 20.
https://aisel.aisnet.org/treos_amcis2021/20

Incorporating Subjective Initiative Module into Security Education, Training, and Awareness Programs

TREO Talk Paper

Yuelin Zhu
University of Memphis
yzhu6@memphis.edu

Qiunan Zhang
University of Memphis
qzhang4@memphis.edu

Xihui Zhang
University of North Alabama
xzhang6@una.edu

Abstract

The COVID-19 pandemic has forced many companies to change their business processes. Global enterprises such as Google and Amazon are taking the lead in experimenting with “working from home” and considering the long-term implementation of such working mode. Without effective Security Education, Training and Awareness (SETA) programs on the individual side, this transformation of the working environment may create more complex and severe threats to an organization’s information security than that of “bring your own device to work.” It will cause more unpredictive security issues because employees may lose their defensive awareness when working in their comfortable zone – home. It is difficult for employees to prevent software attacks such as back door and packet sniffer in the operating environment without professional IT supervision/regulation, even they have been trained with the general SETA programs. It is a consensus that security awareness is the weakest link in the security systems, and it is also the most effective security method to protect a company’s information assets. Employees’ behaviors and actions have huge impacts on a company’s system security, even under the protection of professional tools and specialists. As such, it is necessary for CIOs and CISOs to adjust, develop, improve, and strengthen their SETA programs to emphasize the importance of employee behavior on the security of information assets and help employees establish the integrated and systematic organizational secure cognition.

The subjective initiative plays a critical role in one’s daily work. It includes a person’s cognition, perception, and confidence of one’s own abilities, the capability to plan flexible and effective actions in an independent situation, and the ability to think through the consequences and impacts of the actions. According to the subjective initiative concept, we developed the Subjective Initiative Module (SIM), which was based on employees’ understanding of the organization’s vision, mission, and strategy, enhanced by self-efficacy, sense of agency, and human agency, to construct and formulate the cybersecurity awareness of employees. Incorporating the “subjective initiative module” into the SETA programs will make the security awareness concept more concrete for employees from an independent individual view, help organizations integrate their structured cognition system, and avoid economic losses such as data breach due to unconscious human errors. With SIM, SETA programs foster employees’ engagement from “I can do it” and “I make it happen” to “I affect the life.” Consequently, employees step out of their comfortable zones and create a sense of responsibility when working at home. Adopting SIM in the SETA programs enables employees to normalize their behaviors intentionally, consciously, and actively when working independently, which in turn can enhance the effectiveness and efficiency of the SETA programs, leading to improved IT security performance.