Cyber-complacency and the Security Downfall: An Empirical Analysis

Ensuring information security has become a strategic objective of modern organizations, especially those collecting and processing sensitive data. Organizations, therefore, employ information security policies and train employees to protect information assets and strengthen the human aspect or weakest link of information security. Prior information security studies have investigated different factors, such as fear appeals, habits, role values, neutralization, cyber-fatigue, and social influence, among others, as the antecedents of employee security behaviors. Nevertheless, mixed findings abound in this body of literature. One emerging factor that could resolve some of these inconsistent findings is the employees' perceptions of information security defense mechanisms used by their organizations. How do these perceptions affect employees' security behaviors? Can employees' overreliance on the organization's technical defense mechanisms lead to complacency and undesirable security behaviors? This research employs a two-study design (survey and experiment) to empirically examine the employee cyber-complacency phenomenon and its potential influence on two example security behaviors: compliance with information security policies and performance in detecting phishing messages. This research contributes to the information security literature in several important ways. First, it offers a validated measurement scale for cyber-complacency. Second, it integrates cyber-complacency in the unified model of information security policy compliance and extends the current nomological network. Third, it instigates future research to examine the different dimensions and instantiations of cyber-complacency and its critical role in shaping employee security behaviors.

Keywords: Cyber-complacency; employee compliance; information security; scale development; phishing attacks.