Information Seeking Behavior in the Domain of Security Incident Detection: An Experimental Investigation

*TREO Talk Paper*

**Roozmehr Safi**
University of Missouri-Kansas City
safir@umkc.edu

**Glenn J. Browne**
Texas Tech University
glenn.browne@ttu.edu

**Abstract**

Prevention and detection & response are the two major approaches in countering information security threats. Traditionally, prevention-oriented measures were the preferred choice, since most security threats were known and were therefore preventable. However, the ability to effectively detect and respond to security threats is becoming even more important as intruders continue to further customize their attacks to evade traditional preventive security measures. Effective detection and response involves two major classes of behaviors: sensory vigilance (e.g., responding to an audio alert) and active information seeking (e.g., using diagnostic tools such as security scans or regularly reviewing security reports and logs). The focus of this research is on the latter type of behaviors. By conducting an experimental game which simulates real-world security scenarios, we investigate security-related information seeking behavior of users related to detecting threats. We also study the role of investment in security as a circumstantial factor that can adversely affect the quality of users’ threat-related information seeking behaviors. We argue that increased security investment can adversely affect users’ behavior, as users tend to adopt “risk-compensating behaviors” (a.k.a. Peltzman Effect) through which users relax their proactive security responsibilities when they perceive an increase in their level of safety. In our experiment, users are responsible for keeping a dataset safe over a given length of time, during which security incidents happen following a certain probability distribution. In the experimental game, undetected security incidents and checking for incidents both cost money. The goal in the game is to minimize the overall cost. By reducing the riskiness of the environment over several trials of the task, we investigate the effects of reduction in the perceived riskiness of the environment to examine whether users engage in risk compensating behaviors. Results from this study will better inform us about the monitoring behavior of decision makers and the adverse effects that any perceived increase in the level of safety and security can have on the quality of security-related behaviors.