TREO
Technology, Research, Education, Opinion

Are Threats driving Security Measures in Organizations?

A Mixed-Method Study of Employee Behavior Post Security Breach Incidents

Abhipsa Pal, Indian Institute of Management Bangalore, abhipsa.pal14@iimb.ac.in;
Rahul De', Indian Institute of Management Bangalore, rahul@iimb.ac.in

Firms and their employees are frequent victims of security breaches. Cybercriminals target individuals to create a breach and harm the reputation of their firms (Safa, Von Solms, & Furnell, 2016). While such attacks cause disruptions in work and loss of business, they also create high levels of threat that result in a push towards the implementation of new security measures in the organization. Such measures are a form of reactive physical coping mechanism. Several prior studies explored cases of security violations (Zafar, Ko, & Osei-Bryson, 2016), including discussion on the seriousness of losses for people and firms. However, since the perception of severe threats impacts security policy attitude (Herath & Rao, 2009), we suggest how breaches will trigger severe levels of threat, directly leading to policy changes.

To validate our claims, we propose a mixed-method approach. We collected qualitative data on security breach incidents from 14 organizations, as reported by employees who were either, a victim of the attack, or had direct involvement with the incidents. The data consisted of in-depth reports containing the details of the attack, the immediate reactions of the victim and the organization's support team, the details of the damage, and the policy changes implemented after the incident. The analysis of the data gave rise to concepts like severity and susceptibility of threat, preventive awareness, and the procedural measures for policy changes. These concepts are closely related to technology threat avoidance theory (TTAT) (Liang & Xue, 2009) and Protection Motivation Theory (PMT) for IT threats (Herath & Rao, 2009; Rogers & Prentice-Dunn, 1997). Borrowing from these theories, and combining with the findings from our qualitative data analysis, we develop a research model to explain how security measure implementations are driven by IT security threats. We plan to validate the model using a survey with hypothetical breach scenario to trigger the threat perception of the respondent. This study contributes significantly to IT security literature. It has practical implications for organizations in the era of cybercrimes and malware attacks.

References

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, *33*(1), 71–90.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. *Handbook of health behavior research 1: Personal and social determinants* (pp. 113–132). New York, NY, US: Plenum Press.

Safa, S. N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82.

Zafar, H., Ko, M. S., & Osei-Bryson, K.-M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, *18*(6), 1205–1215.