Security Analytics: Evaluating Antecedents to Non-Compliance Behaviors

Alexander McLeod
Texas State University
a_m919@txstate.edu

Diane Dolezel
Texas State University
dd30@txstate.edu

Abstract

Security analytics remain a challenge as researchers evaluate how and why users continue to violate security policies. Most data breaches happen because users engage in risky behaviors and do not follow organizational policies. Capitulation theory considers whether users are suffering data breach fatigue. Results from initial security analytics research using capitulation theory indicate low explanatory power from proposed antecedents. We consider additional antecedents and modifications in the crafting of our current research.

Security Analytics

Security analytics considers human factors related to security compliance. Security non-compliance contributes strongly to security incidents and data breaches (Diesch, Pfaff, & Krcmar, 2020; Furnell & Shah, 2020; Gillam & Foster, 2020; Vroom, 2004). Security policies are developed to control user behavior (Karjalainen, Siponen, & Sarker, 2020; McLeod & Dolezel, 2020). Data breaches have continued as users violate or ignore security policies (Kafali, Jones, Petruso, Williams, & Singh, 2017). These user behaviors cause problems for organizations trying to protect against cyberattacks and researchers studying this phenomenon wonder why users continue to break rules and violate policies (Johnston, Warkentin, McBride, & Carter, 2016). Some researchers have suggested that when users perceive a threat, they will take safeguarding actions or potentially act passively using emotion-focused coping (Liang & Xue, 2009; Xiao & Warkentin, 2021). It is these passive emotion focused coping mechanisms that are the core of this work. What emotions might be driving users towards their non-compliance behaviors?

While users "giving up" on security has been put forth as a reason for security policy failures, recent work has provided research models with low explanatory power (McLeod & Dolezel, 2022). Prior security analytics work on capitulation theory proposes distrust of security, rationalization, security self-efficacy, security threat, theft of privacy and vulnerability as antecedents to capitulation and compliance. Are there other more fitting constructs contributing to feelings of capitulation? Does the current model adequately reflect the constructs necessary to explain capitulation? This study evaluates emotion-based responses resulting from repeated data breaches to establish relationships and improve the explanatory value of the model. Results should inform those seeking to make clear how emotion-based reactions interact with feelings of capitulation, increasing non-compliance. Figure 1 shows the current research model associate with emotion-focused coping following breach fatigue.

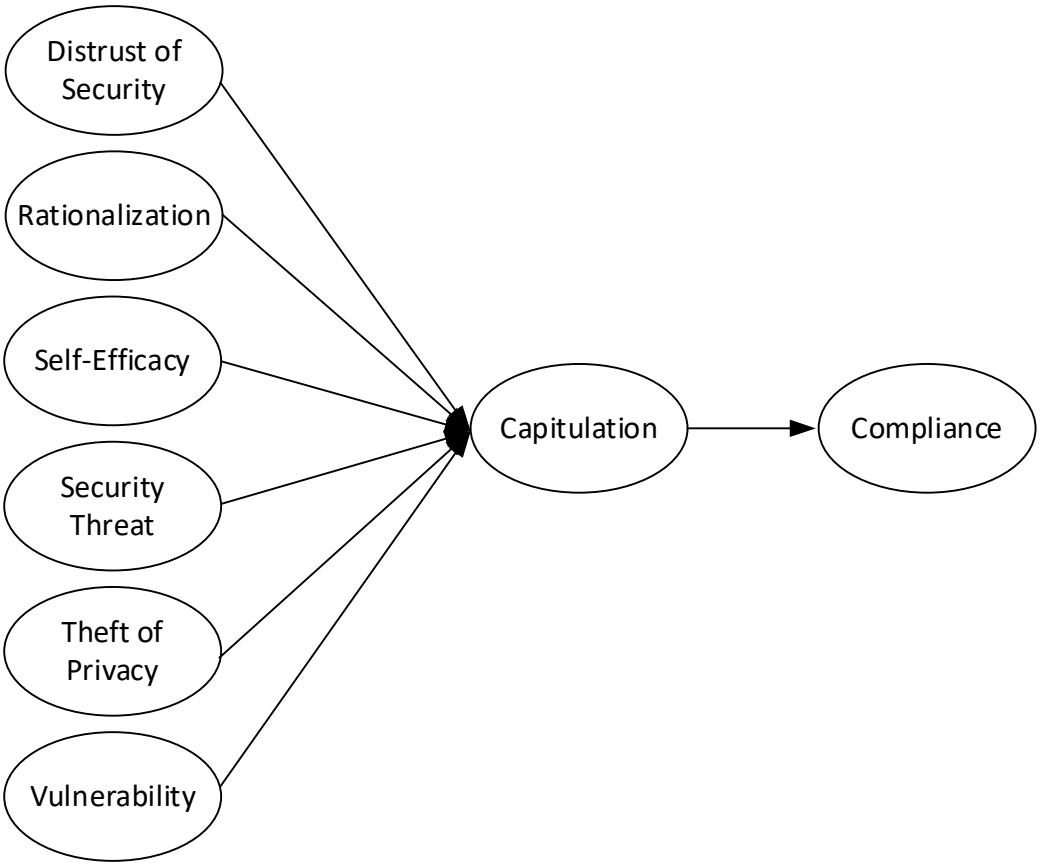

Figure 1: Emotion-Focused Coping

References

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security, 92*. doi:10.1016/j.cose.2020.101747

Furnell, S., & Shah, J. N. (2020). Home working and cyber security–an outbreak of unpreparedness? *Computer Fraud & Security, 2020*(8), 6-12.

Gillam, A., & Foster, W. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior, 108*. doi:10.1016/j.chb.2020.106319

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems, 25*(3), 231-251.

Kafali, Ö., Jones, J., Petruso, M., Williams, L., & Singh, M. P. (2017). *How good is a security policy against real breaches? A HIPAA case study.* Paper presented at the 2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE).

Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. *Computers & Security, 93*. doi:10.1016/j.cose.2020.101782

Liang, H., & Xue, Y. (2009). Avoidance Of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly, 33*(1), 71-90. doi:10.17705/1CAIS.04422

McLeod, A., & Dolezel, D. (2020). Toward Security Capitulation Theory.

McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security, 112*, 102526.

Vroom, C., von Solms, R. ,. (2004). Towards information security behavioral compliance. *Computers & Security, 23*(3), 191–198.

Xiao, S., & Warkentin, M. (2021). Too Bored to Engage: An Exploratory Study of Information Security-related Boredom.