

A self-regulatory framework of security fatigue

Akanksha Malik
Guildhall School of Business and Law
London Metropolitan University
London, UK
a.jamwal@londonmet.ac.uk

Sanjay Goel
Information Security and Digital Forensics
University at Albany, SUNY
New York, United States
goel@albany.edu

Shuchi Sinha
Department of Management Studies
Indian Institute of Technology Delhi
New Delhi, India
shuchi@dms.iitd.ac.in

Abstract

As our networks get complex and cyber threats proliferate, organizations respond with more complex cyber security policies and greater restrictions on data access. This poses increasing demands on employees, wherein they have to adapt themselves to more complex procedures, frequent training and added restrictions on data access. These constantly evolving processes and procedures burden employees and over time may lead to security fatigue. The goal of this study is to advance the understanding of security fatigue by looking into the interactional influence of various antecedents of security fatigue. The results of this study would help to establish the criticality of security fatigue in maintaining security compliance by employees. It would further help in developing effective mechanisms for harmonizing security mandates in organizations with employee cognitive load and stress.

Keywords: cyber security, information security, job demand-resource model, security, security burnout, security fatigue, self-regulation

Introduction and Rationale for the Study

Organizations today are revising their security policies to make them more stringent and complex in order to adapt to the evolving cyber threat landscape and increasing risk of cyberattacks. With the increasing complexity of information security-related rules and policies, employees are getting more taxed with the burden of compliance – often leading to fatigue and intentional noncompliance (D’Arcy et al., 2014). When employees get security fatigued, that is, wearied from frequent engagement with security-mandates, such as updating operating systems, paying attention to phishing emails, or setting strong passwords (Stanton et al., 2016), they may disregard security policies and exhibit a reluctance to comply with them (Ogawa et al., 2021). This may further compel organizations to adopt sanctions for policy violation and subject employees to increased training demands on the policies, leading to more employee frustration and non-compliance (Ogawa et al., 2021).

There is a need to break this vicious cycle in the security domain and facilitate security compliance, especially since research in this area illustrates that a majority of security breaches are an outcome of the failure of well-meaning employees to follow security policies rather than employees with malicious intentions (Goel et al., 2021; Posey et al., 2014). It has been reported that non-malicious insiders were accountable for the loss of approximately sixty-seven percent of the compromised records over a year (IBM, 2018). However, it needs to be kept into consideration that although fatigue is not the only factor that will influence security policy compliance by employees, it is one of the critical factors to be investigated for effective cyber protection (Furnell and Thomson, 2009).

The present study aims to understand the complex phenomenon of security fatigue because of its severe implications for security behavior of employees in the organization. Individuals may disregard the security protocols and guidelines when they have to make decisions that are beyond their cognitive capacity (Choi and Jung, 2018) and as such we posit security fatigue as a failure to self-regulate in a situation. We pose that the constant decision-making based on mandated procedures required of employees has a negative influence on the self-regulatory capacity of the individual, such that it leads to a diminished sense of self control of the individual; we describe this as security fatigue.

The study aims to understand the interactional influence of security demands in the organization, impediment of work, organizational resources and individual characteristics on how fatigued individuals feel about the frequent advice and action requests related to security policies and procedures. The study integrates self-regulation with job demand resource (JD-R) theory to develop the causal model and facilitate the understanding of security fatigue. According to the JD-R theory, current job demands and resources to balance these demands, together, influence the productivity and well-being of the employees (Pham et al., 2019). The study positions itself such that security fatigue occurs or self-control depletes when the balance between the resources (organizational and individual) and security demands is disturbed.

A quantitative empirical study was designed after developing a conceptual self-regulatory model of security fatigue. The data collection survey instrument captures information on security demands and security culture of the organization, work impediments, resources available to employees in the organization (technological support and decision latitude), dispositional variables (self-regulatory capacity), how employees feel (exhaustion and cynicism) about the security protocols and procedures, and the security compliance behavior of the employees. The variables used in the study were measured with previously developed and validated scales. All the construct items were validated by a set of IS field experts to make the items better suited to the information security context. The effectiveness of the items in the survey was improved after taking insights from the pilot survey analysis. The first stage of data collection for the study comprised of employees (n=150) who have work experience, but are not limited to a particular industry to ensure the representativeness of the sample. Additional data of employees (n=148) was collected to strengthen and validate the insights from the initial findings. In the next stage of the study, we aim to collect data from employees working in a particular organization. This would be done to control the effect of the organizational culture and industry on security management.

Initial Findings

This study helps in conceptualizing security fatigue by understanding its components and functioning and thus facilitating a comprehensive understanding of the issue. It becomes essential to understand that information security is not just maintained by designing better technologies to keep the organizations safe but by ensuring the motivation and ability of the employees to comply with the security policies.

The findings of the study suggest that security fatigue has a negative impact on the security compliance behavior of employees. Every arduous act of self-regulation absorbs some amount of the limited cognitive resources of the individual. Thus, as the levels of security fatigue increase, the compliance of the individual decreases. Further, security demands increase work impediment of the employees which further increases fatigue with the security

policies. The study highlights the differential impact of various dimensions of security demands (uncertainty, complexity and overload of information) on work impediments.

Next, the study highlights that employee's control over the skills, time, decisions, and work in the organization moderates the relation between work impediment and security fatigue, such that when employee's control over the decisions in the organization is high, the impact of work impediment on security fatigue is reduced. Similarly, self-regulation capacity was shown to be an effective moderator in the relationship between work impediments and security fatigue. When the self-regulation capacity of the individual is high, the impact of work impediment on security fatigue is low. However, when the self-regulation capacity is low, self-control of the individual depletes, and work impediments leads to higher security fatigue. Thus, work impediment has a positive effect on security fatigue, however the impact is reduced when the employee has sufficient control over resources in the organization and has high self-regulatory capacity. We also find that organizational technological support has a negative effect on security fatigue of the individual, such that when employee's technological literacy is facilitated and technical support is provided to them, security fatigue is significantly reduced. The results of the study would help in conceptualizing security fatigue and developing strategies to achieve better cyber security outcomes.

Conclusion and Future Work

This study is a research-in-progress paper that presents a model to understand the interplay of antecedents influencing security fatigue. Security fatigue becomes an important area to explore and understand because of its significant influence on the security compliance behavior of employees. The failure to comply with the security policies can result in security breaches in the organization.

As the research on security fatigue is evolving, we conceptualize security fatigue through a self-regulation lens and understand the interactional influence of various antecedents through job-demand resource theory. We assert that security-related advice and actions in the organization pose a burden on the employees which impedes their regular work, productivity, and well-being. When the demands exceed the resources provided by the organization and the individual's capacity to self-regulate, it leads to depleted self-control, which can be described as security fatigue. The study provides direct evidence of the factors impacting the security fatigue of the employees, which can guide in forming timely mechanisms to minimize or resolve security fatigue in employees.

We hope to present the initial results at the conference and believe the feedback would help us to strengthen the idea and the paper.

References

- Choi, H. and Jung, Y. (2018) 'The role of privacy fatigue in online privacy behavior', *Computers in Human Behavior*, 81, pp.42–51.
- D'Arcy, J., Herath, T. and Shoss, M. K. (2014) 'Understanding employee responses to stressful information security requirements: A coping perspective', *Journal of Management Information Systems*, 31(2), pp.285–318.
- Furnell, S. and Thomson, K.-L. (2009) 'Recognising and addressing security fatigue', *Computer Fraud & Security*, 2009(11), pp.7–11.

- Goel, S., Williams, K.J., Huang, J. and Warkentin, M., (2021) 'Can financial incentives help with the struggle for security policy compliance?', *Information & Management*, 58(4), p.103447.
- IBM. (2018) 'X-Force Cyber Security Intelligent Index', Available at: <https://www.ibm.com/downloads/cas/XVWX6ZVZ> (Accessed: 10 February 2023)
- Ogawa, M., Tanimoto, S., Hatashima, T. and Kanai, A. (2021) 'Information Security Fatigue Countermeasures Using Cognitive Strategy Scale Based on Web Questionnaires', *International Journal of Networking and Computing*, 11(2), pp.412-425.
- Pham, H. C., Brennan, L. and Furnell, S. (2019) 'Information security burnout: Identification of sources and mitigating factors from security demands and resources', *Journal of Information Security and Applications*, 46, pp. 96-107.
- Posey, C., Roberts, T. L. and Lowry, P. B. (2015) 'The impact of organizational commitment on insiders' motivation to protect organizational information assets', *Journal of Management Information Systems*, 32(4), pp.179-214.
- Stanton, B., Theofanos, M. F., Prettyman, S. S. and Furman, S. (2016) 'Security fatigue', *IT Professional*, 18(5), pp.26-32.