Winter 12-11-2022

Trading well-being for ISP compliance: An investigation of the positive and negative effects of SETA programs

Jalal Sarabadani
Washington State University, jalal.sarabadani@wsu.edu

Robert E. Crossler
Washington State University

John D'Arcy
University of Delaware

Trading Well-Being for ISP Compliance: An Investigation of the Positive and Negative Effects of SETA Programs

Jalal Sarabadani[1]
Carson College of Business,
Washington State University
Pullman, WA, USA

Robert E. Crossler
Carson College of Business,
Washington State University
Pullman, WA, USA

John D'Arcy
Lerner College of Business
and Economics,
University of Delaware
Newark, DE, USA

ABSTRACT

This paper attempts to challenge existing assumptions on SETA programs as positive interventions to promote ISP compliance behaviors. Drawing upon the conservation of resources theory, we posit SETA programs have resource enhancing and depleting effects, differentially influencing employees' ISP compliance. This paper aims to open new avenues of research by highlighting the positive and negative effects of SETA programs from a stress perspective.

Keywords: SETA programs, stress, resource gain, resource loss, ISP compliance

INTRODUCTION

Despite substantial investment and effort in protecting digital assets, data breaches are still on the rise (Statista 2022), with employees being the root cause (Cram et al. 2019). To address this issue, researchers and practitioners recommend security education, training, and awareness (SETA) programs. Estimates predict a $10 billion investment in SETA programs by 2027 (Shackleton 2021). Acknowledging their benefits, like other mandatory training endeavors, SETA programs may have the potential to place several demands such as taking over too much of employees' work/non-work time to meet SETA requirements, exposing them to excessive

[1] Corresponding author. jalal.sarabadani@wsu.edu

informational and instructional interruptions, and requiring them to process too much information, turning SETA programs into an additional source of strain for employees.

Prior research takes for granted that SETA programs promote employees' compliant behaviors, though we begin to observe employee fatigue from such corporate trainings (Pandey 2021). SETA programs are beneficial to help employees gain new personal resources such as higher confidence to protect digital assets. However, they can be detrimental to employees' well-being by contributing to employees' perception of work overload, interrupting their primary work, and feeding them too much information, causing resource loss. This raises the question of whether gains from SETA programs may come with costs. Thus, we aim to answer:

What are the resource enhancing and depleting effects of SETA programs?

We use the conservation of resources theory (COR) to answer our research question (Hobfoll 1989). From a COR perspective, employees invest resources in SETA programs to acquire new resources such as improved confidence in their ability to deal with information security threats. On the other hand, demanding excessive resources might lead to resource depletion, turning SETA programs into a workplace stressor with adverse consequences.

In the next section, we review SETA programs research and COR theory. Next, we develop the research model. As a work-in-progress paper, we present our initial thoughts on the research method, data analysis strategy, and expected research and practice contributions.

PRIOR RESEARCH ON SETA PROGRAMS

SETA programs are awareness and educational endeavors to enhance employees' compliance with information security policies (ISP). SETA programs are multi-dimensional and ongoing efforts that aim to accomplish objectives such as conveying knowledge about risks associated with organizational digital assets, informing employees of their responsibilities in

protecting digital assets, and making employees aware of sanctions against ISP violations (D'Arcy et al. 2009).

Existing research on SETA programs looks at this phenomenon from two major perspectives of (1) designing effective SETA programs and (2) using theoretical models to explain how SETA programs promote (deter) ISP compliance (violation). Regarding the former, research uses interpretive approaches to suggest pedagogical requirements to be incorporated in SETA programs to increase the likelihood of their success (Karjalainen and Siponen 2011). Relevant to the latter, extant research relies on psychology and criminal theories to study SETA programs. For instance, D'Arcy and colleagues (2009) find SETA programs increase the perception of severity and certainty of sanctions related to ISP violations, reducing the tendency to misuse IT. In addition, SETA programs provide opportunities to learn various techniques to protect digital assets, increasing the use of security tools (Crossler and Bélanger 2009).

Despite valuable research on the positive and negative effects of SETA programs, recent findings provide initial evidence of contradictory arguments. For instance, Han and colleagues (2017) and Hovav and Putri (2016) find that SETA increases the perception of cost, suggesting the existence of a potential dark side, yet there is no theoretical and empirical effort to test this assertion. These findings indicate that overt focus on SETA programs as positive interventions to promote ISP compliance may limit our understanding of this phenomenon. As a result, a more comprehensive view is needed to investigate both positive and negative effects of SETA programs.

CONSERVATION OF RESOURCES THEORY

Conversation of resources (COR) is a theory of understanding stress through resource dynamics (Hobfoll 1989). COR postulates that individuals have valued resources and strive to

protect, conserve, and build new resources. Resources can be perceptual or actual, and loss (gain) of resources indicates how individuals respond to certain events. Hobfoll (2001) identifies five broad categories of material (e.g., financial stability), energy (e.g., time and effort), work (e.g., reputation), personal (e.g., self-esteem), and interpersonal (e.g., relationships) resources.

According to the central tenets of COR, individuals with enough resources are willing to invest in certain conditions (e.g., work demands) to gain and accumulate new resources. Accordingly, successful investment of resources generates new resources and improves employees' sense of well-being, leading to positive outcomes (i.e., resource enhancing path). On the other hand, when a particular condition demands more resources that exceed individuals' capacity, it creates a sense of loss for individuals. Based on the COR, losing resources dampens one's motivation and can adversely influence subjective well-being, resulting in undesirable outcomes (i.e., resource depleting path).

The value of COR has been recognized in IS research as well. Previous studies on after-hours use of technology for work leveraged COR to pinpoint that although staying connected to work increases employees' sense of job control, such demands might make it hard for them to detach from work, thus having adverse effects on their well-being, work, and life outcomes (Chen and Karahanna 2018; Richardson and Benbunan-Fich 2011). COR is especially relevant to this research as it challenges existing assumptions around SETA programs. With time, energy, and personal resources relevant to this study, we postulate that SETA programs may produce various compliance behavior through resource enhancing and depletion paths.

RESEARCH MODEL AND HYPOTHESES

Our research model depicts that SETA programs can be differently associated with employees' ISP compliance through resource enhancing and depleting paths. Resource

enhancing path suggests that SETA programs improve employees' confidence in their ability to fulfill ISP requirements (i.e., information security self-efficacy (ISSE)) that subsequently increases their engagement with security practices, resulting in a higher likelihood of compliance with ISPs. Resource depleting path indicates that SETA programs contrast with employees' primary work, which puts excessive demand on them. As such, they cause a sense of overload that results in a feeling of strain, hampering their intentions to comply with ISPs.

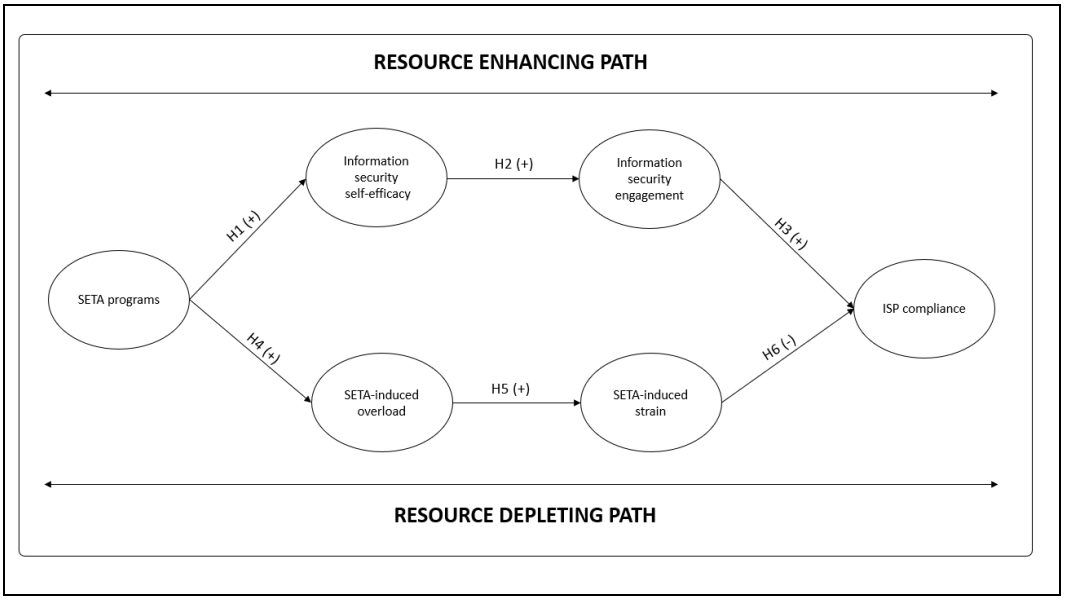

Figure 1. Research Model

Resource Enhancing Path Hypotheses

SETA programs essentially focus on improving employees' awareness of threats and improving their knowledge and skills to perform security-related precautions. Training employees about digital threats fulfills their knowledge gap (Kam et al. 2022). Previous findings show that individuals who receive such training programs feel more certain about their ability to have a safer cybersecurity behavior in their company (Hu et al. 2022). Thus, we propose that:

H1: SETA programs are positively associated with information security self-efficacy.

Information security self-efficacy (ISSE) refers to one's judgment of their ability to protect organizational IS assets from internal and external threats (Bulgurcu et al. 2010). Individuals with ISSE express positive feelings and are willing to put more energy into exploring the source of positive experiences (Burns et al. 2019). As such, they extend their effort to fulfill security-related tasks. A significant implication, thus, is that employees are more likely to use security tools (Crossler and Bélanger 2009). Furthermore, we argue that individuals with higher ISSE are more receptive to change, flexible to learn, and take precautions against threats. Therefore, involving in information security practices is joyful for them. Thus, we propose that:

H2: ISSE is positively associated with information security engagement.

Information security engagement can be described as one's expression of interest, enthusiasm, and enjoyment when performing information security-related tasks (Pham 2016). Highly engaged employees are intrinsically motivated and demonstrate positive attitudes (Bakker and Demerouti 2007). We posit that employees who engage with information security have the motivation to develop their skills, which is intrinsically and extrinsically rewarding for them. It is intrinsically rewarding because learning new security practices gives them a sense of accomplishment. It is also extrinsically rewarding because of receiving recognition from others for their ability to protect personal and organizational digital assets. Therefore, the rewards from their involvement motivate compliance behavior. Thus, we propose that:

H3: Information security engagement is positively related to compliance with ISPs.

Resource Depleting Path Hypotheses

SETA programs are mandatory (Puhakainen and Siponen 2010); thus, like other job training, they put additional demands, causing perception of overload (Cooper et al. 2001). Due to their multi-dimensional nature, SETA programs can cause overload in various ways. SETA

programs frequently present employees with updates about new policies, data breaches, and complex instructions to avoid threats (Hu et al. 2022), which takes their time away from work and requires substantial cognitive processing and adaptation from individuals (Cooper et al. 2001). Furthermore, organizations use e-mails, push notifications, and pop-ups to deliver informational and instructional materials. Exposure to interruptions forces psychological transition from one task to another (Addas and Pinsonneault 2018). Over exposure to such demands, thus, creates a sense of not having adequate resources left (e.g., time and energy) to attend to their primary work. Thus, we hypothesize that:

H4: SETA programs are positively associated with SETA-induced overload.

We define SETA-induced overload as the extent to which individuals receive and process more security-related informational and instructional materials than they can effectively handle. The relationship between overload and strain is well-established (Cooper et al., 2001). We posit that excessive demands from SETA force individuals to give up their free time at work and (or) outside work. The pressure to work faster and handle more information than capacity hinders employees from accomplishing their core tasks, producing anxiety and frustration. In addition, too many interruptions by SETA programs demand more cognitive effort and make it hard to resume interrupted tasks (Galluch et al. 2015; Mark et al. 2005). Such an overload deteriorates individuals' resources, including time and energy (Chen and Karahanna 2018), negatively influencing the ability to manage tasks and eventually resulting in exhaustion (Addas and Pinsonneault 2018). Therefore, we propose that:

H5: SETA-induced overload is positively associated with SETA-induced strain.

Previous research on stress presents ample evidence of the adverse effects of strain on individuals' work-related behaviors (Cooper et al. 2001). Research on technostress shows that

strain from technology can negatively influence employees' innovative use of technology (Maier et al. 2021), lower their performance (Maier et al. 2019), and even lead to quitting the use of IT (Beaudry and Pinsonneault 2010). Accordingly, we posit that experiencing strain from SETA disrupts employees' ability to manage workload. Under such circumstances, employees form dislike and distrust towards the source of strain (i.e., SETA programs) and hold it responsible for the issues they encounter at work. The resulting conclusion motivates them to avoid the source of strain or lower interaction with it (Liang et al. 2019). For instance, individuals may ignore security messages and reminders or engage with workaround activities (e.g., fast-forwarding training videos) to only meet the requirements. This lowers employees' attention to the latest threats and precautions they need to take to avoid threats, increases human errors, and degrades the value of ISPs, eventually decreasing their likelihood of compliance ISPs. Thus, we propose:

H6: SETA-induced strain is negatively associated with ISP compliance.

FUTURE OUTLOOK AND CONCLUSION

We will test our model using a longitudinal survey to capture resources and outcomes at two different points. We plan to collect data from full-time employees above 18, aware of ISPs, and receive SETA programs using online panels. We will measure SETA, ISSE, SETA-induced overload, and demographics in the first wave. In the second wave, we will capture information security engagement, SETA-induced strain, and ISP compliance. We take measures of SETA programs from D'Arcy et al. (2009), ISSE and ISP compliance from Bulgurcu et al. (2010), Information security engagement from Pham (2016), strain from Ayyagari et al. (2011). We will model SETA-induced overload as a reflective-formative second-order construct measured by SETA-induced work overload, interruption overload, and information overload. Measures will

be adapted from (D'Arcy et al. 2014), (Chen and Karahanna 2018) and (Zhang et al. 2016), respectively. We will use SmartPLS to evaluate the measurement and structural model.

We expect to contribute in several important ways. First, we highlight the positive and negative outcomes of SETA programs. Second, we echo the message that organizational training can potentially result in adverse consequences. Third, we inform practice by identifying the dual aspect of SETA programs. This helps organizations design SETA programs to enhance their positive effects while reducing employee overload.

REFERENCES

Addas, S., and Pinsonneault, A. 2018. "E-Mail Interruptions and Individual Performance: Is There a Silver Lining?," *MIS Quarterly* (42:2), pp. 381-406.

Ayyagari, R., Grover, V., and Purvis, R. 2011. "Technostress: Technological Antecedents and Implications," *MIS Quarterly* (35:4), pp. 831-858.

Bakker, A. B., and Demerouti, E. 2007. "The Job Demands-Resources Model: State of the Art," *Journal of managerial psychology*). (22:3), pp. 309-328.

Beaudry, A., and Pinsonneault, A. 2010. "The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use," *MIS Quarterly* (34:4), pp. 689-710.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS quarterly*, (34:3), pp. 523-548.

Burleson, J., Carter, M., and Sarabadani, J. 2019. "On the Importance of Data Quality in Information Systems Research and Ph. D. Curricula.," in: *SIG-ED Pre-International Conference on Information Systems (ICIS) Workshop*. San Francisco, USA: pp. 1-10.

Burns, A., Roberts, T. L., Posey, C., and Lowry, P. B. 2019. "The Adaptive Roles of Positive and Negative Emotions in Organizational Insiders' Security-Based Precaution Taking," *Information Systems Research* (30:4), pp. 1228-1247.

Chen, A., and Karahanna, E. 2018. "Life Interrupted: The Effects of Technology-Mediated Work Interruptions on Work and Nonwork Outcomes," *MIS Quarterly* (42:4), pp. 1023-1042.

Cooper, C. L., Cooper, C. P., Dewe, P. J., O'Driscoll, M. P., and O'Driscoll, M. P. 2001. *Organizational Stress: A Review and Critique of Theory, Research, and Applications*. Sage.

Cram, W. A., D'Arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly* (43:2), pp. 525-554.

Crossler, R. E., and Bélanger, F. 2009. "The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage," *Journal of Information System Security* (5:3), p3-22. 20.

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.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information systems research* (20:1), pp. 79-98.

Galluch, P. S., Grover, V., and Thatcher, J. B. 2015. "Interrupting the Workplace: Examining Stressors in an Information Technology Context," *Journal of the Association for Information Systems* (16:1), pp. 1-47.

Hobfoll, S. E. 1989. "Conservation of Resources: A New Attempt at Conceptualizing Stress," *American psychologist* (44:3), p. 513.

Hobfoll, S. E. 2001. "The Influence of Culture, Community, and the Nested-Self in the Stress Process: Advancing Conservation of Resources Theory," *Applied psychology* (50:3), pp. 337-421.

Hu, S., Hsu, C., and Zhou, Z. 2022. "Security Education, Training, and Awareness Programs: Literature Review," *Journal of Computer Information Systems* (62:4), pp. 752-764.

Kam, H. J., Ormond, D. K., Menard, P., and Crossler, R. E. 2022. "That's Interesting: An Examination of Interest Theory and Self-Determination in Organisational Cybersecurity Training," *Information Systems Journal* (32:4), pp. 888-926.

Karjalainen, M., and Siponen, M. 2011. "Toward a New Meta-Theory for Designing Information Systems (Is) Security Training Approaches," *Journal of the Association for Information Systems* (12:8), p. 3.

Liang, H., Xue, Y., Pinsonneault, A., and Wu, Y. 2019. "What Users Do Besides Problem-Focused Coping When Facing It Security Threats: An Emotion-Focused Coping Perspective," *MIS Quarterly* (43:2), pp. 373-394.

Maier, C., Laumer, S., Tarafdar, M., Mattke, J., Reis, L., and Weitzel, T. 2021. "Challenge and Hindrance Is Use Stressors and Appraisals: Explaining Contrarian Associations in Post-Acceptance Is Use Behavior," *Journal of the Association for Information Systems* (22:6), pp. 1-60.

Maier, C., Laumer, S., Wirth, J., and Weitzel, T. 2019. "Technostress and the Hierarchical Levels of Personality: A Two-Wave Study with Multiple Data Samples," *European Journal of Information Systems* (28:5), pp. 1-27.

Mark, G., Gonzalez, V. M., and Harris, J. 2005. "No Task Left Behind? Examining the Nature of Fragmented Work," in: *Proceedings of the SIGCHI conference on Human factors in computing systems*. pp. 321-330.

Pandey, A. 2021. "How to Overcome Learning Fatigue in Your Remote Employee Training Programs." from https://www.eidesign.net/how-to-overcome-learning-fatigue-in-your-remote-employee-training-programs/

Pham, H. 2016. "Security Demands, Organisational and Personal Resources: A Stress-Based Security Compliance Model." RMIT University.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS quarterly* (34:4), pp. 757-778.

Richardson, K., and Benbunan-Fich, R. 2011. "Examining the Antecedents of Work Connectivity Behavior During Non-Work Time," *Information and Organization* (21:3), pp. 142-160.

Shackleton, T. 2021. "Cyber Security Budget Trends in 2022." from https://www.6dg.co.uk/blog/cyber-security-budget-trends/

Statista. 2022. "Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to First Half 2022." from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Zhang, S., Zhao, L., Lu, Y., and Yang, J. 2016. "Do You Get Tired of Socializing? An Empirical Explanation of Discontinuous Usage Behaviour in Social Network Services," *Information & Management* (53:7), pp. 904-914.