Enhancing the SETA program with Mindfulness and Self-Efficacy

Jiri Vidgren [1]

[1] *University of Jyväskylä, Finland*

Abstract

The cyber threat landscape is constantly evolving. System vulnerabilities are identified and patched, digital defenses are strengthened, and policies are enforced. Still, the organization's most valuable resources, humans, are running their outdated operating systems without patching in sight. It is well proven that humans are the essential link in information security. With their humane feelings, emotions, thoughts, fears, hopes, and personal priorities, the users are more complicated to motivate, persuade, attract, and align with compliance than information systems. Mindfulness is a promising concept to assist users in pursuing more secure behavior and attitude, which proliferates in more secure organizations as a joint effort. Another promising strategy, developing self-efficacy, also appears to reinforce users' more secure behavior, thus complementing the benefits of mindfulness and contributing to the effectiveness of the security education, training, and awareness (SETA) program. However, incorporating the mentioned concepts with SETA programs needs to be researched further and with a broader scope. In this paper, future research is justified and motivated to discover and explore these promising approaches.

Keywords

SETA program, Information Systems Security, Mindfulness, Self-Efficacy

1. Introduction

From a highly abstract viewpoint, there are two types of cyber-attacks: (1) digital system vulnerability being exploited; or (2) a human being acting maliciously against themselves or their organization, intentionally or unintentionally, and probably influenced by some hoax or diversion. Technological advancements have benefited defenders and attackers regarding the recent history of information security. Moreover, even considering that artificial intelligence is assisting both sides to prosper in their campaigns, the number of successful attacks targeted at purely digital systems is decreasing [1]. The malicious actors have always tried to exploit "human firewalls" with phishing, social engineering, and such human-targeted attempts. Still, they are forced to expand and pivot more towards humans to fund their business since digital vulnerabilities are becoming scarce.

In a modern business environment, where information technology is ubiquitous [2], countering emerging threats and securing data and systems' confidentiality, integrity, and availability is critical. However, users and employees, primarily their actions, are secured with different measures. The SETA program is a well-known approach to enhancing users' information security awareness (ISA). Organizations have taken unique approaches to implementing such programs. While some organizations are putting significant effort into the SETA program, some are doing just the bare minimum in that segment. Still, information security is often absent from the top management's table. [3].

The foundation and anchoring point for information security management should be an appropriate information security policy [3, 4] (ISP), which underlines the commitment of the top management to information security. However, information security is treated in many organizations as a technical support function, and information security is often regarded in corporate strategy only by outsourcing the issue to IT management [4, 5, 6, 7].

TKTP 2023: Annual Symposium for Computer Science 2023, June 13-14, 2023, Oulu, Finland

ISPs have been described in various ways, with distinct meanings in different organizations [8]. From the top management's information security governance point of view, the function of ISP is to "provide management direction and support for information security in accordance with business requirements and relevant laws and regulations." [9, p. 96]. At the operational level, the ISP defines the "rules and guidelines for the proper use of organizational IS resources" [10].

No matter how comprehensive the ISP is, user compliance with the ISP is always under concern [11]. For example, according to the study by Siponen & Vance [12], the users could employ the "denial of the responsibility" [13, 14] of following the ISP by appealing to unclear or absent instructions. Regarding the same neutralization theory, with the "denial of injury" -technique, a user could argue that "no harm was caused" by non-compliant ISP behavior [14]. Siponen et al. [7, p. 217] claim, "A key threat to information security comes from employees who do not comply with information security policies." In a recent report by Verizon [15], the human element is involved in 82% of security breaches, proving the challenge is persistent.

One way to approach compliance is the "security theatre" [16], where organizations are just trying to write IS security procedures and guidelines to make auditors happy. The aim and motivation for these organizations are in the certification (i.e., ISO/IEC 27001) itself, and not in the holistic risk management, continuous improvement of their information security management system (ISMS), or focusing on the users' IS security behavior [17]. In summary, "compliance does not equal security." [17, p. 44].

To achieve ISP compliance *and* attain an adequate level of (IS) security, it is crucial to emphasize the users' behavioral dimensions and the socio-organizational aspects contributing to the information security resilience of the organization [18]. Precedent research has already established the importance of information security culture and its impact on the overall information security levels in the organization [19]. For organizations' information security to thrive, a security culture must be actively developed and nurtured by balancing socio-technological dimensions [19, 20]. In addition, there is evidence that mere technical and procedural measures are inadequate to engage with information security's human dimension [20]. Understanding the users' information security behavior (ISB) is a path toward more efficient SETA programs.

Mindfulness has been applied broadly throughout information systems (IS) research. Dernbecher and Beck [21] conducted an extensive literature review regarding using mindfulness concepts in IS research. As we advance, mindfulness in IS *security* research is still emerging and forming its shape. Mindfulness is a promising approach to improve SETA programs from an individual and organizational level. The characteristics of mindfulness, such as orientating in the present, giving attention to operational detail, and being willing to consider alternative perspectives [22], are rather practical approaches regarding IS security. (Organizational) Mindfulness has been suggested as a possible approach for efficient ISP management [23], and enhancing the SETA program with mindfulness has been pointed out as a future research direction [24].

Regarding ISP compliance, self-efficacy has been a promising dimension to assess the phenomena behind the users' behavior and motivation [25]. Self-efficacy, an essential construct of social cognitive theory, refers to an individual's belief in their ability to perform a specific task [26]. Self-efficacy in information security is developed through the ongoing acquisition of knowledge related to information security, possibly from the training that one receives. Previous studies have shown the link between self-efficacy and behavior; therefore, information security self-efficacy is expected to influence compliant behavior [26, 27].

This paper examines and justifies tailoring the SETA program by incorporating mindfulness and self-efficacy. This paper aims to guide scholars to empirically explore the validity and efficiency of such tailoring. Also, the paper intends to instruct the SETA program designers to modify their information security curriculum respectively.

2. Security Education, Training, and Awareness (SETA) Program

SETA is "a managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance for an organization's employees" [28, p. 211]. A SETA program is built on three elements: security education, security training, and security awareness. These elements are introduced in table 1.

Table 1
SETA Comparative Framework **[29, p. 145]**

	Awareness	Training	Education
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	Media • Videos • Newsletters • Posters, etc.	Practical Instruction • Lecture • Case study workshop • Hands-on practice	Theoretical Instruction • Discussion Seminar • Background Reading
Test Measure:	True / False Multiple Choice (Identify learning)	Problem-Solving (Apply learning)	Essay (Interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

ISA program is a sub-program of SETA. The role of the ISA program is typically designed to keep information security at the forefront of users' minds and provide *recognition* of possible threats, risks, and mitigations for those. Information Security Training (IST) builds on the foundation of ISA. The primary purpose of IST is to teach and train the *skills* needed to perform the user's duties securely. IST may also include security workshops and hands-on practice to engage with the users. The third level in SETA is Information Security Education (ISE) program, which is not on everybody's curriculum in the organization. Generally, the information security professionals are the users who are committed to ISE programs, championing information security and possibly pursuing also to certify their knowledge with third-party institutions. [29].

2.1. SETA and ISP

No matter what shape the SETA program assumes, it is fundamentally grounded in ISP [10]. Moreover, typically, SETA programs rely on the ISP as their primary means of instruction [30]. By raising awareness among the users about security issues, users better understand protecting themselves, which safeguards the company and the business. Eventually, it also fulfills the basic requirements of the ISP. Peltier [30] also argue that an adequate information security and cybersecurity program cannot be implemented without implementing an employee information security awareness and training program (SETA) as an underpinning foundation for information security. Scholl et al. [31] also suggest qualities like behavioral awareness and self-responsibility for all employees to be educated, trained, and measured aligned to the information security and cybersecurity awareness training.

3. Mindfulness and SETA

Mindfulness is a psychological construct conceptualized on an individual level by Ellen J. Langer, who presents mindfulness as a cognitive process of alertness and dynamic awareness [32]. Based on Langer [33], the concept of mindfulness revolves around certain psychological states that are different versions of the same thing: (1) openness to novelty; (2) alertness to distinction; (3) sensitivity to different contexts; (4) implicit, if not explicit, awareness of multiple perspectives; and (5) orientation in the present. These characteristics predominantly concern the (individual) *trait mindfulness*, which is often discriminated from more specific mindfulness concepts, like IT mindfulness [34] and Eastern/Western approaches to mindfulness [35, 21].

3.1. Mindfulness in IS Security Research

In addition to the eastern, even religious (e.g., Buddhism) approaches, mindfulness is divided and branched into many different sub-concepts, broadly identified by current research. The most notable differences, in general, are between the Eastern and Western mindfulness traditions, whereas the Eastern tradition is rarely integrated with IS research [21]. Ray et al. [36] have characterized more of these Western approaches and highlighted primarily *organizational* mindfulness. Organizational mindfulness has been studied mainly from high-reliability organizations (HROs) perspective [37, 35, 38]. HROs focus on a minimum level of variance in performance, therefore aiming for reliability and safety but also *security* as a priority [37]. Some common examples of HROs are air traffic control teams, nuclear power plants, law enforcement special units (e.g., SWAT teams), and emergency room staff.

The most apparent counterpart for organizational mindfulness is *individual* mindfulness, the most interesting one regarding IS security research from an individual's information security awareness point of view. This paper follows Langer's perception of mindfulness [33]. It represents the Western tradition from an individual perspective and focuses on external factors like information categorization for solving active and goal-oriented tasks [21].

Motivating future research about incorporating mindfulness in IS research, Dernbecher and Beck [21, p. 138] encourage scholars by stating: "As a result, we recommend that IS research endeavors to extend the mindfulness concept by combining it with existing theories from the IS discipline as well as from other related disciplines."

4. Enhancing SETA Program with Mindfulness

The human factor of individual members is an essential aspect of cybersecurity research. With the users' humane approach and "outdated operating system," individual members are the crucial link between business and technology in the converged world ahead, where technology is embedded in everything [2]. Embedded technology will emerge new challenges related to IS security, which eventually be coped with on an individual level.

SETA programs must be developed and tailored to improve the perceived information security level and protect the IS operating environment of the organization [30]. However, tailoring the awareness program "to fit" does not end with tailoring by role and level of the user. This paper argues that tailoring should also include elements from mindfulness.

Langer [33, 22] indicates that when individuals feel elevated involvement and wakefulness in the present, they are more likely to detect changes in their setting and consequent opportunities for action [39]. In addition, findings by Jensen et al. [40] suggest that mindfulness techniques can be successfully taught to individuals and that the results of the training rise above mere awareness of the level of behavior.

4.1. Avoiding Mindless SETA Program

Organizations often use *rule-based* information security awareness programs to train their users, where regular repetition leads to *mindless* behavior [40]. Also, the chosen delivery mediums might be incapable of delivering the actual training content effectively, i.e., a tedious video or an irrelevant web-based application is not adequate to change the behavior of the users [41].

Based on recent research results, Jensen et al. discovered that rule-based training might be less effective than other training approaches. They noted the discrepancy between the training participants' self-estimated skills and actual behavior considering targeted phishing attacks. Jensen et al. conclude that the training may affect attitudes and behavior differently [40]. Rule-based activity may spark confidence and perceived expertise in the users' intentions, but improvements in protective behavior may not be achieved.

To avoid mindless SETA programs, Nwachukwu et al. [41] have provided six tentative design recommendations for SETA programs: (1) Engaging participants through interaction and active participation via different training delivery methods [42, 43, 44, 45]; (2) ensuring contextual relevance [46]; (3) taking the particular susceptibility to threats in account to ensure personal relevance [46, 47]; (4) using concrete and strong fear appeal messages [48, 49, 12]; (5) running training programs periodically [50], and

finally; (6) developing essential skills required to the compliant behavior, rather than just facilitating unidirectional messaging about the desired outcome [51].

4.2. Towards Mindful SETA Program

It is predominant for any SETA or ISA program to aim to change the actual behavior rather than just intentions. Jensen et al. have indicated that incorporating mindfulness techniques aids the transition from awareness to real behavioral change [40]. According to Jensen et al., the program content should be delivered using engaging delivery methods with corresponding audience portions and supplementing such rule-based training with mindfulness approaches [40, 46].

The research by Jensen et al. [40] focuses on mitigating phishing attacks with mindfulness techniques. However, ENISA [52] has identified multiple additional human-related emerging threats, which cannot be mitigated without changing the behavior of users. These threats include advanced disinformation campaigns, human errors, and skills shortages, which catalyze challenges such as lack of knowledge, training, and understanding [52]. Social engineering, including the physical dimension, and threats against data are also listed as human-related emerging "prime threats" [1].

Regarding the sustainable development of security-aware culture, Bulgurcu et al. [25] suggest that organizations should organize security training to ensure users' self-efficacy, which correlates strongly with users' positive information security behavior [53, 54, 49]. As the results of Rhee et al. [54, p. 822] confirm: "self-efficacy in information security (SEIS) is a meaningful construct in explaining users' security practice behavior."

5. Discussion

While technical countermeasures advance, threat actors and cybercriminals are pivoting to easier targets, like humans, which are relatively more susceptible to security breaches. This emerging trend will challenge organizations with constantly evolving threats and strategies by malicious actors. Users in different organizations, roles, and levels need to be trained adequately to support the individuals' awareness and skills in information security. The security culture in organizations builds on active discussion, interaction, involvement, participation, and user cooperation. The positive development of the security culture will depend on the organizations' management decisions on whether to invest (more) in SETA programs or not. For this culture to thrive, organizations must take a humane approach in their SETA programs and empower the users to behave securely, sustain compliance with ISP, and perform as the most vital link of information security.

Mindfulness should be integrated into SETA in various formats and approaches to habilitate the users from encountering unforeseen threats. Current empirical research on mindfulness and information security is narrowed to specific interventions, such as phishing and identifying fake news. However, mindfulness should be studied empirically with other emerging, extensive human-related information security topics, like social engineering. A more comprehensive approach would allow us also to examine the physical dimension of security, in which mindfulness could prove helpful.

This paper is intended to bridge publication between two articles related to a dissertation. Therefore, the traditional IMRaD is not followed precisely; for example, the methods and results are absent. The primary purpose of this paper is to motivate further research regarding the topic and predispose the research recommendations for critique and review.

5.1. Recommendations for Future Research

I suggest that mindfulness techniques should be implemented in any SETA program, especially in those which are more generic, awareness-focused, and therefore targeted to every user in the organization. I assume it would naturally position mindfulness as the foundation of information security awareness training. Organizations should also develop users' self-efficacy and enhance the information security-aware culture organizations. All in all, I allege that the humane approach could result in more secure behavior, which is the root of information security, as discussed. However, this needs to be researched further. In addition, it must be ensured that the behavior is measured, not just the intention to behave or the self-estimated level of awareness, perceived expertise, or confidence about protecting the organization's

assets. Therefore, a sheer survey would not be adequate to measure the sustaining effect of SETA programs. Instead, empirical research is needed to validate how mindfulness could be incorporated into the SETA program with suitable interventions and corresponding training with a mindfulness angle. In addition, the possible benefits of such an approach should be measured and evaluated. Finally, introducing self-efficacy development with the SETA program to pursue secure behavior should also be considered a substantial research opportunity.

6. References

[1] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2022," European Union Agency for Cybersecurity (ENISA), Athens, Greece, 2022.

[2] M. Dufva, "Megatrendit 2020," Sitra, Vantaa, 2020.

[3] B. von Solms and R. von Solms, "The 10 deadly sins of information security management," *Computers & Security,* vol. 23, no. 5, pp. 371-376, 2004.

[4] R. A. Rothrock, J. Kaplan and F. Van Der Oord, "The Board's Role in Managing Cybersecurity Risks," *MIT Sloan Management Review,* vol. 59, no. 2, pp. 12-15, 2018.

[5] M. T. Siponen and H. Oinas-Kukkonen, "A review of information security issues and respective research contributions," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems,* vol. 38, no. 1, pp. 60-80, 2007.

[6] B. von Solms, "Corporate Governance and Information Security," *Computers & Security,* vol. 20, no. 3, pp. 215-218, 2001.

[7] M. Siponen, M. A. Mahmood and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Information & Management,* vol. 51, no. 2, pp. 217-224, 2014.

[8] R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations," *Logistics Information Management,* vol. 15, no. 5/6, pp. 337-346, 2002.

[9] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security,* vol. 4, no. 2, pp. 92-100, 2013.

[10] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research,* vol. 20, no. 1, pp. 79-98, 2009.

[11] M. Karjalainen, M. Siponen and S. Sarker, "Toward a stage theory of the development of employees' information security behavior," *Computers & Security,* vol. 93, 2020.

[12] M. Siponen and A. Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly,* vol. 34, no. 3, pp. 487-502, 2010.

[13] J. W. Rogers and M. D. Buffalo, "Neutralization Techniques: Toward a Simplified Measurement Scale," *The Pacific Sociological Review,* vol. 17, no. 3, pp. 313-331, 1974.

[14] G. M. Sykes and D. Matza, "Techniques of Neutralization: A Theory of Delinquency," *American Sociological Review,* vol. 22, no. 6, pp. 664-670, 1957.

[15] Verizon, "Data Breach Investigations Report (DBIR)," Verizon, New York City, NY, USA, 2022.

[16] B. Schneier, Beyond Fear, Berlin: Springer, 2006.

[17] L. Zinatullin, The Psychology of Information Security: Resolving conflicts between security compliance and human behaviour, Cambridgeshire: IT Governance Publishing, 2016.

[18] S. E. Choi, J. T. Martins and I. Bernik, "Information security: Listening to the perspective of organisational insiders," *Journal of Information Science,* vol. 44, no. 6, pp. 752-767, 2018.

[19] J. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Computers & Security,* vol. 29, no. 4, pp. 476-486, 2010.

[20] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: An action research study," *MIS Quarterly:*

Management Information Systems, vol. 34, no. 4, pp. 757-778, 2010.

[21] S. Dernbecher and R. Beck, "The concept of mindfulness in information systems research: a multi-dimensional analysis," *European Journal of Information Systems,* vol. 26, no. 2, pp. 121-142, 2017.

[22] E. J. Langer, The Power of Mindful Learning, Reading, MA: Addison-Wesley, 1997.

[23] J. L. Parrish, J. R. Kuhn and J. F. Courtney, "Mindful administration of IS security policies," in *14th Americas Conference on Information Systems, AMCIS 2008*, Toronto, ON, Canada, 2008.

[24] A. D. Landress, J. Parrish and S. Terrell, "Resiliency as an Outcome of SETA Programs," in *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation*, Boston, MA, USA, 2017.

[25] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly,* vol. 34, no. 3, pp. 523-548, 2010.

[26] A. Bandura, "Self-efficacy: Toward a unifying theory of behavioral change.," *Psychological Review,* vol. 84, no. 2, pp. 191-215, 1977.

[27] C. A. Chambliss and E. J. Murray, "Efficacy attribution, locus of control, and weight loss," *Cognitive Therapy and Research,* vol. 3, no. 4, pp. 349-353, 1979.

[28] M. E. Whitman and H. J. Mattord, Principles of Information Security, 6th edition, Boston, MA, USA: Cengage Learning, 2017.

[29] National Institute of Standards and Technology (NIST), "An Introduction to Computer Security: the NIST Handbook," National Institute of Standards and Technology, Gaithersburg, MD, USA, 1995.

[30] T. R. Peltier, "Implementing an Information Security Awareness Program," *Information Systems Security,* vol. 14, no. 2, pp. 37-49, 2005.

[31] M. Scholl, K. B. Leiner and F. Fuhrmann, "Blind Spot: Do You Know the Effectiveness of Your Information Security Awareness-Raising Program?," *Journal of systemics, cybernetics and informatics,* vol. 15, no. 4, pp. 58-62, 2017.

[32] E. J. Langer, "Minding Matters: The Consequences of Mindlessness–Mindfulness," *Advances in Experimental Social Psychology,* vol. 22, pp. 137-173, 1989.

[33] E. J. Langer, Mindfulness, Reading, MA: Perseus Books, cop., 1989.

[34] J. B. Thatcher, R. T. Wright, H. Sun, T. J. Zagenczyk and R. Klein, "Mindfulness in information technology use: Definitions, distinctions, and a new measure," *MIS Quarterly: Management Information Systems,* vol. 42, no. 3, pp. 831-847, 2018.

[35] K. E. Weick and K. M. Sutcliffe, "Mindfulness and the Quality of Organizational Attention," *Organization Science,* vol. 17, no. 4, pp. 514-524, 2006.

[36] J. L. Ray, L. T. Baker and D. A. Plowman, "Organizational Mindfulness in Business Schools," *Academy of Management Learning & Education,* vol. 10, no. 2, pp. 188-203, 2011.

[37] A. J. Burns, "Security organizing: A framework for organizational information security mindfulness," *Data Base for Advances in Information Systems,* vol. 50, no. 4, pp. 14-27, 2019.

[38] T. J. Vogus and K. M. Sutcliffe, "Organizational mindfulness and mindful organizing: A reconciliation and path forward," *Academy of Management Learning and Education,* vol. 11, no. 4, pp. 722-735, 2012.

[39] E. J. Langer and M. Moldoveanu, "The Construct of Mindfulness," *Journal of Social Issues,* vol. 56, no. 1, pp. 1-9, 2000.

[40] M. L. Jensen, M. Dinger, R. T. Wright and J. B. Thatcher, "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems,* vol. 34, no. 2, pp. 597-626, 2017.

[41] U. Nwachukwu, J. Vidgren, M. Niemimaa and J. Järveläinen, "Do SETA Interventions Change Security Behavior? – A Literature Review," in *56th Hawaii International Conference on System Sciences*, Lahaina, HI, Usa, 2023.

[42] M. Karjalainen and M. Siponen, "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches," *Journal of the Association for Information Systems,* vol. 12, no. 8, pp. 518-555, 2011.

[43] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Computers and Security,* vol. 29, no. 4, pp. 432-445, 2010.

[44] E. Dincelli and I. Chengalur-Smith, "Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling," *European Journal of Information Systems,* vol. 29, no. 6, pp. 669-687, 2020.

[45] S. Abraham and I. Chengalur-Smith, "Evaluating the effectiveness of learner controlled information security training," *Computers & Security,* vol. 87, 2019.

[46] L. Jaeger and A. Eckhardt, "Eyes wide open: The role of situational information security awareness for security-related behaviour," *Information Systems Journal,* vol. 31, no. 3, pp. 429-471, 2021.

[47] R. Wright and K. T. Marett, "The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived," *Journal of Management Information Systems,* vol. 27, no. 1, pp. 273-303, 2010.

[48] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody and P. Polak, "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly,* vol. 39, no. 4, pp. 837-864, 2015.

[49] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly,* vol. 34, no. 3, pp. 549-566, 2010.

[50] P. J. Steinbart, M. J. Keith and J. Babb, "Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication," *Information Systems Research,* vol. 27, no. 2, pp. 219-239, 2016.

[51] M. Wolf, D. Haworth and L. Pietron, "Measuring An Information Security Awareness Program," *Review of Business Information Systems (RBIS),* vol. 15, no. 3, pp. 9-22, 2011.

[52] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!," ENISA, 11 November 2022. [Online]. Available: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030. [Accessed 29 March 2023].

[53] B. Xue, M. Warkentin, L. A. Mutchler and P. Balozian, "Self-efficacy in Information Security: A Replication Study," *Journal of Computer Information Systems,* vol. 63, no. 1, pp. 1-10, 2023.

[54] H.-S. Rhee, C. Kim and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers & Security,* vol. 28, no. 8, pp. 816-826, 2009.