Information Security Awareness: Identifying Gaps in Current Measurement Tools

*Corey Bolger, Brad Brummel, Sal Aurigemma, Tyler Moore, Meagan Baskin**
*The University of Tulsa, *Florida Gulf Coast University*
Corey-bolger@utulsa.edu, Bradley-brummel@utulsa.edu, sal-aurigemma@utulsa.edu, tyler-moore@utulsa.edu, mbaskin@fgcu.edu

Abstract

This paper describes the key role of information security awareness (ISA) in organizational attempts to comply with their information security policies and mandated frameworks and regulations. The design, implementation, and evaluation of Security Education Training, and Awareness (SETA) programs rely on the definition and measurement of ISA. Reviews of the research on SETA programs have shown robust effectiveness for the improvements of ISA and security-related behaviors as a result of these programs. However, this same research has shown little ability to differentiate between the wide variety of SETA programs for achieving the variety of possible knowledge, attitude, intention, and behavioral outcomes at the individual or the organizational level that could be the objectives of these programs. This lack of differentiation results from an approach to ISA measurement that was designed to be broad and heterogenous in an attempt to capture any and all changes in ISA. After reviewing these other approaches to awareness, we discuss how improved approaches to defining and measuring ISA have the potential to provide practitioners and scholars more guidance into which SETA approaches are most effective for which outcomes for which populations given the investment needed to implement the program.

Information Security Programs and Information Security Risk

Employees and end-users are recognized by security practitioners and academia as important components of the organizational cyber security ecosystem. Eighty-two percent of all industries analyzed in the Verizon 2021 Data Breach Investigations Report (DBIR) listed Social Engineering in the top three patterns for incidents and breaches. According to the IBM Cost of a Data Breach Report 2021 (CDBR), 20% of breaches have an initial attack vector of compromised employee credentials, while an additional 17% of breaches start with a phishing attack on employees. The most expensive breaches involve employees as well. Business email compromise (BEC), phishing, malicious insiders, social engineering, and compromised credentials make up the top five costliest breaches and all involve employees as a key piece of the compromise. Social engineering attacks have been on a continuously upward trend since 2017 (DBIR) and according to additional data found in the DBIR, phishing continues to rise in popularity among cyber criminals, being present in 36% of breaches in 2021, up 25% from 2020.

Preventing a potential data breach or avoiding being victimized in a BEC attack is motivation enough for some organizations to take action to improve employee cyber security behaviors. However, in many industries, there are laws, regulations, or other mandates that require organizations to formally address employee cyber security responsibilities and behaviors. The Computer Security Act (Public Law 100-238, 1988) requires all U.S. Federal Agencies to provide "mandatory periodic training in computers security awareness and accepted computer security practice of all employees" that use Federal information systems (Section 5.a, p6). The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to implement "security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of (A) information security risks associated with their activities; and (B) their responsibility in complying with agency policies and procedures designed to reduce these risks" (128 STAT. 3079 § 3554. Federal agency responsibilities (b)(4)). Outside of the U.S. Federal government, there are other mandates for organizations to implement similar security awareness programs. For example, the Payment Card Industry Data Security Standard (PCI-DSS), which applies to organizations that store, transmit, accepts or processes credit card data, requires that "a formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data" (PCI-DSS 12.6.1). Mandatory frameworks and regulations, like those described above, coupled with the risk appetite of the organization drive formalized, documented security behavior expectations in the form of Information Security Policies (ISPs). ISPs can be used to implement technical safeguards (such as mandating multi-factor authentication for account access) but can also be used to implement procedural safeguards such as a clean desk policy requiring employees to ensure no sensitive documents are left unprotected in their workspace.

ISPs are recommended by most compliance and security frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, ID.GV-1, PR.IP-5, PR.IP-6, PR.PT-1, PR.PT-2") and the International Organization for Standardization (ISO) 27000 (ISO/IEC 27000:2018, "Information technology – Security techniques – Information security management systems, Section 4.1"). In addition to these frameworks, certain industries are required by law to document IS practices via policies and procedures. These policies and procedures inform employees of the required actions to take during normal business operations as well as during and after an incident. By outlining these actions ahead of time, organizations can more readily identify and respond to information security incidents such as improper access or compromised employee credentials. While not all industries are required by law to develop formal information security policies, several industries must be able to verifiably demonstrate their adherence to these standards and frameworks to conduct business. The Health Insurance Portability and Accountability Act (HIPAA) requires organizations in the healthcare industry to implement specific controls to protect individuals' health information (U.S. Department of Health and Human Services Office for Civil Rights, "HIPAA Administrative Simplification", § 164.312 Technical safeguards, 2013), the Payment Card Industry Data Security Standards (PCI-DSS) requires any organization that accepts card payments to implement a different set of security controls to accept credit and debit card transactions ("Payment Card Industry Data Security Standard.", Requirement 12). These frameworks are critical to ensuring that organizations take appropriate care when utilizing sensitive information regardless of the nature of that information.

Well-formed ISPs tailored to meet organizations' governance, risk, and compliance (GRC) requirements are necessary. Information security policies (ISPs) are used as guidance by organizations to direct employees' actions in regards to information and cyber security actions (Aurigemma & Mattson, 2019). These policies are created in response to identified risk and compliance factors and are designed to satisfy these requirements or mitigate possible risk (Doherty & Fulford, 2006). Ensuring employees are cognizant of the ISPs and the responsibilities and expectations of employees contained within is equally necessary. The vehicle for exposing and educating employees on the ISPs falls on organizational Security Education Training and Awareness (SETA) programs. SETA programs can be defined as "ongoing efforts to focus employees' attention on information security–related issues, provide employees with crucial knowledge and skills, enable their deep understanding of why security protection is needed, and increase their awareness of security issues." (Hu, Hsu, Zhou, 2022, p1). Increased awareness of security issues and the contents and requirements of the ISPs is expected to lead to measurable and tangible improvements in employee security behaviors that, when sustained over time, decreases the security risk from employees to the organization, which in turn will feed back into the organization's risk calculus and GRC programs.

SETA Programs & ISA Measurement:

There is a diverse and growing corpus of academic research investigating different aspects of SETA programs. A comprehensive literature review of SETA program research (Hu Hsu, Zhou, 2022) identified one important finding: all the empirical research in this field showed that SETA programs have a positive impact on employee security compliance intentions, continuing compliance intentions, and both prescribed and extra-role security behaviors. Figure 1 outlines the overall flow of information security programs, SETA programs, and their interaction with internal and external organizational factors.

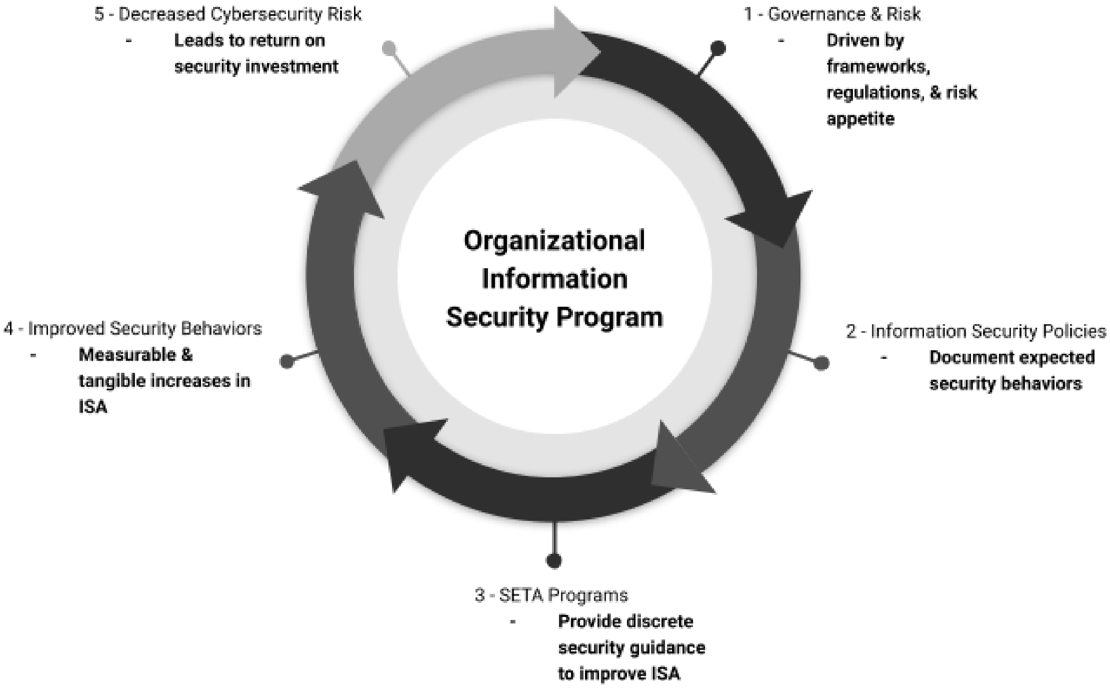
5 - Decreased Cybersecurity Risk
- Leads to return on security investment
1 - Governance & Risk
- Driven by frameworks, regulations, & risk appetite
Organizational Information Security Program
4 - Improved Security Behaviors
- Measurable & tangible increases in ISA
2 - Information Security Policies
- Document expected security behaviors
3 - SETA Programs
- Provide discrete security guidance to improve ISA

Figure 1: Information Security Program Cycle

In this paper, the focus is on the path between SETA programs and measurably improved security behaviors via increasing information security awareness (ISA). While there is a broad research base exploring various aspects of SETA programs, substantially less attention has been given to measuring the effectiveness of SETA programs to produce improved and sustained employee security awareness. Specifically, the design, implementation, and evaluation of SETA programs rely on the definition and measurement of ISA. Reviews of the research on SETA programs have shown robust effectiveness for the improvements of ISA and security-related behaviors as a result of these programs. However, this same research has shown very little ability to differentiate between the wide variety of SETA programs for achieving the variety of possible knowledge, attitude, intention, and behavioral outcomes at the individual or the organizational level that could be the objectives of these programs. This lack of differentiation results from an approach to ISA measurement that was designed to be broad and heterogenous in an attempt to capture any and all changes in ISA. We argue that a refined approach to ISA measurement has the potential to improve the outcomes of SETA programs. After reviewing current ISA measures and definitions, we discuss how improved approaches to defining and measuring ISA have the potential to unleash a new generation of research studies into which SETA approaches are most effective for which outcomes for which populations given the investment needed to implement the program.

Current Definitions and Measurement of ISA:

Within the information security literature, no single accepted standard of information security awareness exists. Many behavioral models include security awareness as an overall concept; however, there is lack of consistency around how information security awareness is operationalized and measured. While no uniformly accepted definition of ISA exists, most definitions tend to conceptualize awareness within the context of the knowledge-attitude-behavioral intention (KAB) model. Parsons et al., (2014) define ISA as the "extent to which an organization's employees understand the importance and implications of information security, and the extent to which they behave in accordance with the organization's information security policies and procedures" (p. 41). This definition includes both understanding the importance and implications of information security and behaving accordingly, namely knowledge and action. Despite this lack of clear understanding of the definition of ISA, scholars and practitioners alike have developed and employed a variety of measures of ISA, but only few have been empirically evaluated outside of the original researchers' context. Some measures are general and broad while some are specific and narrow. The instruments in the ISA literature can be summarized into three general categories: measures with a limited ISA construct, a quasi-ISA construct, and a global ISA construct. Measures with a limited ISA construct measure only a specific construct space of ISA, such as the Secure development of applications (SDA) attitude and behavioral intention measure. Some instruments are quasi-ISA models which are related to ISA but not actually measuring an individual's understanding and behavior as it relates to information security outcomes, such as the Compliance with InfoSec Policies measure. Some instruments attempt to provide a holistic or global measure of information security awareness but do not provide enough granularity to target specific training needs, such as the Risky cybersecurity behaviors scale (RScB) & Attitudes towards cybersecurity and cybercrime in business (ATC-IB) measures.

A compilation of ISA measures, their content areas, a general overview, and a set of example items can be found in table 1 below.

Table 1: ISA Measures

Name: Human Aspects of Information Security Questionnaire (HAIS-Q) **Author(s):** Parsons, McCormac, Butavicius, Pattinson, & Jerram **Year of Publication:** 2014
Content Area(s): Password management, email use, internet use, social media use, mobile devices, information handling, incident reporting
ISA Construct: Global measure
General Review: Uses the Knowledge-Attitude-Behavior model from I-O psychology which is a good foundation. Many items reference past best practices which have since been invalidated. Covers a wide base of general security knowledge. Results only provide a "Total InfoSec awareness" measurement, with no extrapolating information. Items correlate heavily and may not measure distinct aspects of "InfoSec awareness".
Example Items: "It's acceptable to use my social media passwords on my work accounts.", "I am allowed to share my work passwords with colleagues.", "A mixture of letters, numbers, and symbols is necessary for work passwords."

Name: Security Behavior Intentions Scale (SeBIS) **Author(s):** Egelman & Peer **Year of Publication:** 2015
Content Area(s): Device securement, password generation, proactive awareness, updating
ISA Construct: Global measure
General Review: Limited in use. Covers behaviors that are widely known. Items were developed based upon behavioral recommendations from security experts but were not tested for validity.
Example Items: "I set my computer screen to automatically lock if I don't use it for a prolonged period of time.", "I use different passwords for different accounts that I have.", "I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon)."

Name: Conservative Behavior Scale (CBS) **Author(s):** Ogutcu, G., Testik, O. M., & Chouseinoglou, O. **Year of Publication:** 2016
Content Area(s): Passwords, updating, internet use, email use, securement
ISA Construct: Quasi measure
General Review: Targeted at identifying the "direction of relationship between the individuals' awareness toward information security and their behaviors of using information and communication technologies…". This measure aims to identify whether individuals risk perception has any impact on their behaviors and to understand the impact of security awareness on their behaviors. While this measure does strive towards similar goals, simply measuring whether there is an effect or not is insufficient to adequately develop new training methods.
Example Items: "I am concerned about having my identity stolen while shopping online.", "How likely is it for one's privacy to be invaded while shopping online?", "In the past year, have you asked an online business to remove your name and address from any lists they use for marketing purposes?"

Name: Users' Information Security Awareness Questionnaire (UISAQ) **Author(s):** Velki, T., Solic, K., & Ocevcic, H. **Year of Publication:** 2014
Content Area(s): Potentially risky behavior, security awareness, beliefs about infosec, quality and security of passwords
ISA Construct: Global measure
General Review: Developed with the intention of being a general measure of information security awareness. Because of the broad nature of the items, only a very broad sense of ISA can be obtained using this measure. No items were provided making it difficult for others to utilize this measure.
Example Items: N/A

Name: Compliance with InfoSec Policies **Author(s):** Siponen, M. T., Pahnila, S., & Mahmood, M. A. **Year of Publication:** 2010
Content Area(s): Actual compliance (*I comply with information security policies*; 3 items), Intention to comply (*I intend to comply with information security policies*; 3 items), Normative Beliefs (*Top Management thinks I should comply with information security policies*; 4 items)
ISA Construct: Quasi measure
General Review: Generally showed a strong correlation between intent to comply with actual compliance, but it is unclear whether it would be possible to obtain accurate information from employees given the nature of the survey items such as those listed in the example items.
Example Items: "I intend to comply with information security policies.", "An information security breach in my organization would be a serious problem for me.", "Having information security policies in our organization keeps information security breaches down."

Name: Information Security Culture Assessment (ISCA) questionnaire. **Author(s):** Martins, A. & Eloff, J. H. P. (2002); da Veiga, Martins & Eloff (2007) **Year of Publication:** 2002; 2007
Content Area(s): Management of information security, performance management, performance accountability, communication, governance, capability development
ISA Construct: Quasi measure
General Review: No explicit definition of information security awareness was provided by the authors. Based upon the survey items the definition of ISA used is simply "any knowledge of the existence of information security policy." This definition is too broad to be useful in a nuanced measure of ISA at the individual or organizational level.
Example Items: "It is important to understand the threats to the information assets (for example, systems and information) in my department.", "I know where to get a copy of the information security policy.",

"I believe that the information I work with is adequately protected."

Name: Security features **Author(s):** Furnell, S. M., Jusoh, A., & Katsabas, D. **Year of Publication:** 2006
Content Area(s): Awareness of threat, security features within Win XP and 3 popular applications
ISA Construct: Limited measure
General Review: No items provided. Based on very outdated technology.
Example Items: N/A

Name: Policy compliance intention **Author(s):** Herath, T., & Rao, H. R. **Year of Publication:** 2009
Content Area(s): Policy compliance intentions
ISA Construct: Quasi measure
General Review: This is not necessarily a measure of ISA but rather a measure of policy compliance intentions. We do not believe this measure would be useful for identifying target areas for additional security training based upon the focus on policy rather than behavior.
Example Items: Items were sourced from multiple previously validated studies. No individual list of items was provided.

Name: Risky cybersecurity behaviors scale (RScB) & Attitudes towards cybersecurity and cybercrime in business (ATC-IB) **Author(s):** Hadlington, L. **Year of Publication:** 2017
Content Area(s): Device securement, password generation, proactive awareness, updating
ISA Construct: Quasi measure
General Review: The two instruments used in this study are interesting because they attempt to identify specific traits tied to risky cybersecurity behavior. This concept should be extrapolated to more behaviors outside of just attitudes towards cybersecurity. This study did not attempt to build a measure of ISA, but rather a measure of risky cybersecurity behaviors. We believe an instrument similar to this could be useful in identifying specific behaviors that are desirable or undesirable in relation to ISA.
Example Items: (RScB) "Entering payment information on websites that have no clear security information/certification", (RScB) "Bringing in my own USB to work in order to transfer data onto it.", (RScB) "Clicking on links contained in unsolicited emails from an unknown source." (ATC-IB) "I believe everyone in the company has a role to play in protecting against threats from cybercriminals.", (ATC-IB) "I do not feel that IT security is a priority within my organization", (ATC-IB) "I would not know how to report a cyberattack if one happened."

Name: Naïve mistakes and basic hygiene **Author(s):** Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. **Year of Publication:** 2005
Content Area(s): Password management, password sharing behaviors, organizational support of security related behaviors
ISA Construct: Quasi measure
General Review: The methods used in this research may prove to be useful for building a more broad measure of ISA that still allows for measurement of individual roles within an organization. The behaviors targeted for measurement were sourced from IT professionals and managers specifically discussing detrimental and beneficial behaviors related to information technology and security. This focus is too narrow to itself provide a general measure of ISA that is useful for comparing SETA programs, but it lays a firm foundation to be built upon.
Example Items: "He did a training program to learn about the sensitivity and criticality of special company files so that he could apply appropriate protective measures when handling the information.", "She forged routing information to make it seem like someone else had sent some packets."

Name: Omission of security **Author(s):** Workman, M., Bommer, W. H., & Straub, D. **Year of Publication:** 2008
Content Area(s): Subjective omission of security (intentions)
ISA Construct: Global measure
General Review: This study, like many others reviewed, utilizes pre-existing scales for "their validation characteristics and for efficiency". While we understand the appeal of using pre-existing scales, we believe that a new measure must be created to accurately measure ISA.
Example Items: "Threats to the security of my confidential information are: Harmless ... Severe", "I believe that trying to protect my confidential information will reduce illegal access to it: Unlikely ... likely" "The primary responsibility for protecting my confidential information belongs to: My employer ... Myself"

Name: Secure development of applications (SDA) attitude and behavioral intention **Author(s):** Woon, I. M. Y., & Kankanhalli, A. **Year of Publication:** 2007
Content Area(s): SDA attitude (3 items), SDA behavioral intention (2 items)
ISA Construct: Limited measure
General Review: This measure is designed to measure the intentions of software developers as it relates to information security. We believe this approach should be generalized to apply to all members of a department or organization to better identify shortcomings in ISA.
Example Items: "Practising secure development of applications (SDA) would make my applications more robust (better withstand attacks or misuse).", "Almost all my co-workers think that practising SDA is a good idea.", "I would be able to carry out SDA without the help of others."

Name: Attitude & behavioral intentions towards information security organizational policies and procedures (ISOP) **Author(s):** Safa, Von Solms, & Furnell **Year of Publication:** 2016
Content Area(s): ISOP attitude (4 items), ISOP behavioral intentions (5 items)
ISA Construct: Quasi measure
General Review: This measure provides a useful analysis of individuals' attitudes regarding information security policy compliance. While these outcomes may not be directly tied to information security awareness, the attitude of employees towards the organizational security program is an important aspect to capture as part of a holistic measure of organizational information security awareness.
Example Items: "I think information security knowledge sharing helps me to understand the usefulness of information security policies in my organization.", "I gain new information security knowledge in collaboration with experts", "Different information security training methods affected my attitude towards compliance with information security policies"

As previously discussed, the measures identified range from broad (ISCA) to specific (SDA), but there is a large gap between the two which no measures currently fill. The global measures identified are capable of measuring ISA at a broad level but do not provide enough detail for a targeted training program to be developed. The limited measures identified do provide enough detail for targeted training but are very limited in scope or targeted at a single profession. The quasi measures that were analyzed do provide the ability to tie behaviors to security awareness, but none do so in a way that is targeted at practical use in an organization. Furthermore, while these instruments have been validated as part of the study, validity is typically a measure of the use of an instrument, not the instrument itself. For the purposes of identifying groups of users for targeted information security awareness training, the existing measures fall short. We argue that the existing methods of applying a single awareness training across an organization is less effective than targeted training would be, but without a measure to assess training results, it is difficult to test this hypothesis. The measures we have now can easily demonstrate that some training leads to some increase in awareness, but further nuance is not currently possible. Because of this, organizations are unable to make the relative choice of investment in training because no indication of training effectiveness is available. If a training that costs $1,000 per trainee and takes 10 hours to complete is compared with a training that costs $100 per trainee and takes 15 minutes to complete using today's measures it is difficult to differentiate between the level of impact between the two trainings. This results in the obvious choice of organizations choosing the cheaper training option which has led to the development of training that is designed to be cheap, easy, and quick, instead of training that has the greatest impact on user awareness. While these training options are certainly better than nothing, we argue that a stronger emphasis on quantifying awareness training results will lead to the development of new and more effective training programs and methodology.

Conclusion & Future Research:

To improve the outcomes of SETA programs a broader measure of ISA designed to capture both general and nuanced areas of awareness must be developed. The end user is widely regarded as one of the weakest points in any system, yet the research surrounding how to best target this weakness has fallen behind other areas of information security. Future research could include identifying the knowledge, skills, and abilities (KSAs) most used by the typical end user when conducting day-to-day work activities relating to information security, developing a new instrument designed to measure these KSAs, and designing training to target these KSAs. A measure that is designed to identify target areas for training could lead to the development of the next generation of SETA programs.

References

Aurigemma, S., Mattson, T. (2019). Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. *Journal of the Association for Information Systems*, 1700–1742. https://doi.org/10.17705/1jais.00583

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, *25*(1), 55–63. https://doi.org/10.1016/j.cose.2005.09.009

Egelman, S., & Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2873–2882. https://doi.org/10.1145/2702123.2702249

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27–35. https://doi.org/10.1016/j.cose.2005.12.004

H.R.145 - 100th Congress (1987-1988): Computer Security Act of 1987. (1988, January 8). https://www.congress.gov/bill/100th-congress/house-bill/145

H.R.3103 - 104th Congress (1995-1996): Health Insurance Portability and Accountability Act of 1996. (1996, August 21). https://www.congress.gov/bill/104th-congress/house-bill/3103

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

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. https://doi.org/10.1057/ejis.2009.6

Hu, S., Hsu, C., & Zhou, Z. (2022). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, *62*(4), 752–764. https://doi.org/10.1080/08874417.2021.1913671

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

PCI Security Standards Council (2022). Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0. https://www.pcisecuritystandards.org/document_library/

Ponemon Institute (2021). Cost of a Data Breach Report 2021. https://ibm.com/reports/data-breach

S.2521 - 113th Congress (2013-2014): Federal Information Security Modernization Act of 2014. (2014, December 18). https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, *43*(2), 64–71. https://doi.org/10.1109/MC.2010.35

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Velki, T., Solic, K., & Ocevcic, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ) &#x2014; Ongoing work. *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1417–1421. https://doi.org/10.1109/MIPRO.2014.6859789

Verizon (2021). Data Breach Investigations Report. https://verizon.com/dbir/

Woon, I. M. Y., & Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications. *International Journal of Human-Computer Studies*, *65*(1), 29–41. https://doi.org/10.1016/j.ijhcs.2006.08.003

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005