Engaged Management ReView

Manuscript 1131

Optimizing Training to Effectively Mitigate the Human Risk of Cyberattacks: A Critically Appraised Topic

Christine Davis

EDBAC
ENGAGED SCHOLARSHIP•COLLABORATION•NETWORKING

ENGAGED MANAGEMENT ReView

CASE WESTERN RESERVE UNIVERSITY
EST. 1826

EDITORIAL NOTE

Appropriate for a critically appraised topic (CAT), this short paper examines the scientific literature in search of empirical evidence to support common practices. In this case, the very common practice in question regards the use of cybersecurity training (sometimes referred to as SETA, Security Education and Training Awareness) as a means of mitigating an organization's cybersecurity risks. There is research, including the works analyzed in this case, indicating such programs struggle to be effective. So, more specifically, the practice under examination is the use of "best practice" training management: tuning or optimizing the cybersecurity training for the best fit for individual employees. The CAT is motivated by the need to maximize organizational protections. However, these practices also hold promise for simultaneously maximizing employee productivity; minimizing unnecessary work or rework that is irrelevant: not contributing directly to an employee's value output for the organization. The results: the evidence in the literature supports the increased effectiveness from the individualization of cybersecurity training; and tailoring training programs to the needs and traits together with the job risks pertinent to a particular employee.

Optimizing Training to Effectively Mitigate the Human Risk of Cyberattacks: A Critically Appraised Topic

Christine Davis
Georgia State University

ABSTRACT

Employees are an organization's greatest defense against cyberattacks; however, traditional cybersecurity training falls short of developing this protection. Failing to properly train employees to prevent a cyberattack becomes a vulnerability that attackers exploit. Can organizations optimize employee cybersecurity training to effectively mitigate the human-related risks of cyberattacks? Findings indicate that optimized cybersecurity training can indeed mitigate this risk. In this topic paper, the author reviewed the research to recommend strategies for optimizing such training, highlighting the importance of embracing cybersecurity company-wide, at all levels. Furthermore, the lessons in the training must be reiterated, updated, and reinforced—thus promoting a culture of cybersecurity awareness—for the training to have ongoing value.

RESEARCH QUESTION

The purpose of this topic paper is to determine whether academic research supports the optimization of cybersecurity training as a means for organizations to protect against cyberattacks. As such, the research question is as follows: Can organizations optimize employee cybersecurity training to effectively mitigate the human-related risks of cyberattacks?

Table 1: PICOC

P = Problem	Cybersecurity has become an important consideration for many organizations. Socially engineered phishing emails increase the risk that humans may inadvertently enable successful cyberattacks, and cybercriminals continue to improve their persuasive tactics.
I = Intervention	Instituting personalized employee cybersecurity training programs.
C = Comparison	Compare organizations instituting personalized employee cybersecurity training programs with organizations that use traditional training programs.
O = Outcome	Mitigating the human risk of successful cyberattacks.
C = Context	Organizations that have employees conducting business through email or the Internet.

BACKGROUND

To enforce cybersecurity, an organization's employees are its greatest defense; but they also could be the organization's greatest vulnerability if they are not appropriately trained or informed on how to prevent a cyberattack (Fisher et al., 2021). With the rising trend toward remote work and telecommunication, the parameters for ensuring cybersecurity continue to grow in complexity (Hubbard et al., 2021). The COVID-19 pandemic substantially altered human behaviors, both personally and professionally, through increased virtual communication, cloud-based transactions, and e-commerce sales, thus inviting an increase in the number of attackers (Georgescu, 2021). Among the various types of cyberattacks, phishing campaigns pose a significant threat. Phishing is defined as the act of deceptively persuading a targeted online user to reveal personal information or to allow access to data (Back & Guerette, 2021). Socially engineered phishing attempts expose organizations and employees to greater risks of susceptibility because of the targeted, personable, time-sensitive nature of these attacks. Of course, cyberattacks are not limited to phishing; they can extend to malware, ransomware, web-skimming, remote desktop protocol attacks, data exfiltration, and other incidents (Georgescu, 2021; Fisher et al., 2021).

Cybercrime can have huge financial implications, can damage individual and organizational reputations, and can diminish customer loyalty, among other consequences (Fisher et al., 2021). Therefore, protecting organizational information and data should be an important objective for all companies. The purpose of this topic paper is to determine whether research indicates that employee cybersecurity training can be optimized to mitigate the risks of humans' susceptibility to cyberattacks by providing employees with the knowledge and tools needed to detect malicious correspondence before responding to or clicking on harmful links.

SEARCH STRATEGY

The researcher conducted the literature search process on March 23, 2023, initiating a keyword search of the ABI/INFORM Collection, Business Source Complete, and Web of Science databases. The keywords used to find the most relevant articles on employee cybersecurity training included "cybersecurity," "training," "effectiveness," "employee," and "awareness" (see Figure 1). Searches using these keywords yielded 34,952 results. To manage the scope of the study, the researcher limited the results to articles from academic, peer-reviewed journals. In the third step, the researcher excluded articles either not published in the United States or not written in English. The fourth step limited the selection to articles published from 2020 to 2023 to ensure that the researcher included only the most recent research findings in this study. In step five, the researcher manually scanned titles and abstracts for relevance, narrowing the list to eight articles.

Critically assessing these remaining articles for their overall validity, the researcher found that one of the eight articles was a conceptual framework that was not empirically tested. Another article briefly mentioned that cybersecurity training was critical, but the research was based on a small, governmental sample, and training was not empirically examined. Based on these two assessments of low validity, the researcher eliminated these two articles.

Because cybersecurity is a vast and growing area of research interest, the researcher reviewed the remaining six articles for duplication in references and timespan. Although the researcher had narrowed the search to articles published after 2020, the remaining articles cover cybersecurity literature published between 1980 and 2022. Three of the studies are literature reviews covering research from 1980 through 2019, thus thoroughly representing cybersecurity literature published before 2020. See Table 2 for a list of the final search results and Table 3 for the validity assessment of the selected articles.

Table 2: Search Results

1	Back, S., & Guerette, R. T. 2021. Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. ***Journal of Contemporary Criminal Justice***, 37(3): 427–451.
2	Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. 2022. Response to a phishing attack: Persuasion and protection motivation in an organizational context. ***Information & Computer Security***, 30(1): 63–78.
3	Cross, C., & Gillett, R. 2020. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. ***Journal of Financial Crime***, 27(3): 871–884.
4	Fisher, R., Porod, C., & Peterson, S. 2021. Motivating employees and organizations to adopt a cybersecurity-focused culture. ***Journal of Organizational Psychology***, 21(1): 114–131.
5	Gillam, A. R., & Waite, A. M. 2021. Gender differences in predictors of technology threat avoidance. ***Information & Computer Security***, 29(3): 393–412.
6	Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. 2020. Review and insight on the behavioral aspects of cybersecurity. ***Cybersecurity***, 3(1): 1–18.

Figure 1: Literature Search Diagram

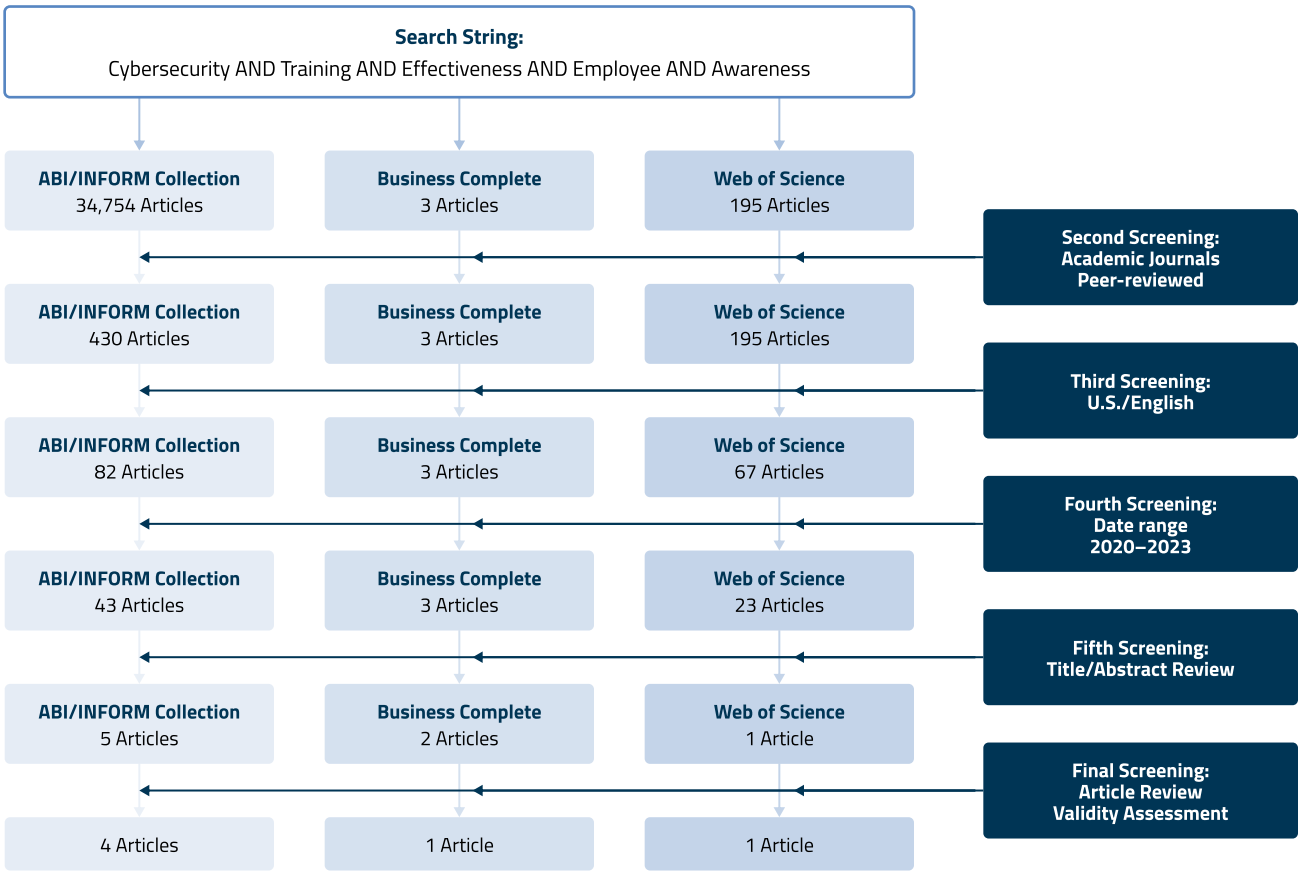

Table 3: Critical Evaluation of Overall Validity

Study	Research Approach	Empirical Basis	Analysis Method	Overall Validity
Study 1: Back & Guerette (2021)	Quasi-experimental design study	Simulated phishing attempt of 2,000 employees from the division of information technology of an urban public university located in the U.S.	Logistic regression analysis along with *t*-test and Mann-Whitney *U* test analyses	Moderate validity: Conclusion drawn from the comparison between the treatment group and the control group results. No initial baseline for the treatment group.
Study 2: Bayl-Smith et al. (2022)	Simulated field study	Online questionnaire of 2,918 financial institution employees located in Australia and New Zealand related to the persuasiveness of five variants of simulated phishing emails	Multinomial logistic regression analysis	High validity: Conclusions based on best persuasion strategies for phishing attack susceptibility analysis.
Study 3: Cross & Gillett (2020)	Literature review	Literature on business email compromise fraud	Literature synthesis	Moderate validity: The researchers did not detail the literature search and selection process. Academic and industry sources were used.
Study 4: Fisher et al. (2021)	Literature review	Literature on enhancing cybersecurity culture	Literature synthesis	Moderate validity: The researchers did not detail the literature search and selection process.
Study 5: Gillam & Waite (2021)	Exploratory design study	Online questionnaire of 206 U.S. adult workers selected through convenience and snowball sampling	Single-shot regression using ordinal regression, supported by K-means clustering	Moderate validity: Conclusions based on gender analysis. Respondents of this study may be different demographically than the population, indicating that the sample may not be truly representative of the whole population.
Study 6: Maalem Lahcen et al. (2020)	Comprehensive literature review	Literature on behavioral aspects of cybersecurity from 1980 through 2019 found using the EBSCO, IEEE, Xplore, JSTOR, Science Direct, and Google Scholar databases	Literature synthesis	High validity: Conclusions were drawn by combining the best results from behavioral literature.

RESEARCH AND ANALYSIS

Table 4 summarizes the findings and translations from the selected research articles. Each article addressed factors that influence the effectiveness of cybersecurity training programs and informed the recommendations related to training optimization.

Table 4: Findings and Translations

Study	Finding 1: Environmental Considerations	Finding 2: Employee Characteristics	Finding 3: Vulnerabilities	Finding 4: Training Considerations
Study 1: Back & Guerette (2021)	Cyber place managers are tasked with enforcing rules and acting as guardians of company data. Cybersecurity culture is a prerequisite to enhancing prevention strategies.	Age and race were predictors of phishing susceptibility. Older generations were more resilient to the deception of phishing attacks than younger generations.	Results indicate that individuals who had cybersecurity training were more susceptible to being victimized by phishing attacks than those who were not trained. However, a pretraining analysis was not conducted to conclude whether training improved the cybersecurity behaviors of the treated group.	Mixed results were reported for training effectiveness. The timeliness of training should be considered. Limited content and lack of interactivity contribute to training ineffectiveness.
Study 2: Bayl-Smith et al. (2022)	Mechanisms should be in place for employees to report suspected malicious emails. Cybersecurity culture could encourage the accountability of all employees to protect the organization's data.	Heuristics could explain why employees fail to detect phishing attempts.	Certain phishing persuasion strategies are more effective than others.	Training should include different persuasion techniques used by cybercriminals.
Study 3: Cross & Gillett (2020)	Employee support should be given before and after an attack. They are victims, too. Update software regularly, install anti-malware programs, and configure firewalls to detect and prevent attacks.	Cybercriminals take advantage of employees' inherent need to please managers and do their job well.	When organizational goals conflict with cybersecurity policies, training effectiveness decreases. Training by itself is not an exclusive solution.	Company-wide training is the most effective way to spread awareness and mitigate the risk related to phishing attacks. Simulated attack training provides hands-on experience with detecting phishing cues.
Study 4: Fisher et al. (2021)	Cyberattacks will become more sophisticated and frequent. A culture that fosters cybersecurity at all levels of the organization could mitigate these risks. Telecommuting policies and procedures need to be considered.	Employee willingness and motivation to change behavior are important. Management involvement in cybersecurity initiatives influences employee participation.	After an attack, security is ingrained in the culture, but time causes individuals to lose motivation.	Employees need to be properly trained and informed in an ongoing, proactive manner. Cybersecurity needs to be top of mind and offered more than once per year. Training should be customized to specific employee personality traits.

Study 5: Gillam & Waite (2021)	Organizational culture could influence threat avoidance behavior effectiveness.	Men are more likely to display threat avoidance behavior than women. Women are more likely to open phishing emails and click on embedded links.	In-house technology experts and programmed detection measures are not enough to ensure effective cybersecurity because human behavior can compromise cybersecurity.	Learner reception of training is higher when the learner is motivated and engaged with the training. Gender considerations should be included in the training to increase motivation but should not alienate learners.
Study 6: Maalem Lahcen et al. (2020)	Environmental workload, management, and communication practices could influence training effectiveness. Create cybercrime awareness advocacy groups.	Employee heuristics in decision-making related to cybersecurity could influence risk. Employee personality also plays a role in how employees respond to cyberattacks.	Cognitive load can lead to inattentiveness. Training does not prevent violations. Attacker strategy affects the effectiveness of the attempt. Cybersecurity spending is reactive rather than proactive, reducing efficiency.	Simulation can test the application of training. Heuristics should be included in the training to enhance awareness. Learning happens in a social context with shared experiences related to cybersecurity. Personality considerations should be included in the training. Continuous updates to the training are needed. Training should be personalized based on the employee's role and job duties.
Translation	**Creating an organizational culture that embraces and supports cybersecurity awareness is one of the most effective ways to mitigate the risk of a cyberattack.**	**Employee characteristics, such as gender, age, personality, and the heuristics they apply, can influence the effectiveness of cybersecurity initiatives and attacks.**	**The phishing strategy that is used affects the success of a cyberattack, and attackers target organizational vulnerabilities.**	**The delivery method of cybersecurity training influences effectiveness.**

Environmental Considerations

Overall, the articles reported mixed results from employee cybersecurity training programs. Mitigating the risk of cybersecurity attacks depends on multiple factors, including organizational culture, practices, and technology. The importance of a strong culture of cybersecurity awareness cannot be ignored in light of continuously evolving and sophisticated cyberattacks. Technology prevention software, human behavior, cybersecurity training, and organizational culture should be combined to mitigate risks through continuous and sustainable protection (Study 4). Study 6 mentioned the importance of aligning organizational goals and culture with security policies and procedures. Furthermore, individual cybersecurity behaviors influence training effectiveness, and these behaviors are influenced by the organization's management style, employee workload, and communication practices (Study 6). By instilling cybersecurity awareness into everyday work habits, organizations can develop employees' heuristics—those intrinsic rules of thumb individuals use to make quick decisions—aimed at identifying and preventing malicious cyberattacks.

Employee Characteristics

Study 5 found a relationship between gender and cybersecurity threat avoidance: Men were more likely to display threat avoidance behavior, and women were more likely to open phishing emails and click on embedded links. Older generations are less trusting of electronic communications, making them more resilient to becoming a victim of a phishing attack than younger generations (Study 1). Moreover, Study 6 concentrated on behavioral aspects of cybersecurity, finding that employee personality was a crucial factor in determining whether a cybersecurity training program was effective. Finally, relying on certain heuristics may increase employees' likelihood of responding to a phishing email (Study 2). These studies show that the effectiveness of cybersecurity training is influenced by employee characteristics; thus, individual characteristics are an important consideration when designing training programs.

Vulnerabilities

Study 3 found that the human aspect of managing cybersecurity cannot be replaced with technological solutions. In addition, and contrary to expectations, Study 1 found that individuals who completed a cybersecurity awareness training program were more likely to fall victim to a phishing attack than employees who had not completed the cybersecurity training. Note that these findings would be more reliable if cybersecurity susceptibility had been measured for each group in the study before the intervention. Because of how the research was conducted, determining whether those in the treated group improved their ability to detect and avoid a phishing attack after completing the training would be difficult.

Study 2 used five different variants of a phishing email to determine which

persuasion strategy would be the most successful in convincing participants to respond to an attack. The researchers found that socially engineered phishing attacks, using social proof and scarcity tactics, were more likely to succeed. Social proof is a psychological tendency to conform to the behaviors of individuals believed to be more knowledgeable about a situation, and scarcity tactics are used to create a sense of urgency around the situation. Correspondingly, attackers exploit organizational vulnerabilities using different tactics to persuade employees to create openings for cyberattacks.

Training Considerations

Understanding that gender differences exist could help organizations maximize training effects without alienating learners based on gender (Study 5). Timeliness of training and lack of interactive lessons lead to ineffective cybersecurity training (Studies 1 and 5), while delivering company-wide training and simulating attacks increased training effectiveness (Studies 3 and 6). Furthermore, individuals are more likely to retain what they learn when training is geared toward their preferred learning style (Study 6). Ultimately, the delivery method of the training influences effectiveness.

CONCLUSION

Based on the review of and translations derived from the selected articles, the researcher found evidence that traditional employee cybersecurity training does not provide much support in mitigating the human-related risks of successful cyberattacks. Organizations tend to introduce cybersecurity training during onboarding as a one-and-done, one-size-fits-all solution or immediately following a successful cyberattack. The value of this training is short-lived if the lessons are not reiterated, updated, or reinforced by a culture of cybersecurity awareness.

Organizational culture can be used to create an environment of employee accountability by rewarding detection and prevention behaviors while motivating employees to participate in cybersecurity training initiatives (Gillam & Waite, 2021). The importance of cybersecurity must be embraced across the company and at all levels to sustain effectiveness (Fisher et al., 2021), and training should be customized to fit different learning styles and personality traits (Maalem Lahcen et al., 2020). The conclusions from Maalem Lahcen et al. (2020) were further validated by a group of Australian researchers who found empirical support for aligning training with individual learning style preferences to improve security awareness (Pattinson et al., 2020).

RECOMMENDATIONS

Organizations that have the most effective cybersecurity programs foster a culture of cybersecurity awareness and align organizational goals with cybersecurity policies and procedures. Therefore, cybersecurity training can be effective in mitigating the human-related risks of cyberattacks if the training is geared toward various employee characteristics, addresses different attacker strategies, incorporates hands-on learning, and is paired with a supportive culture. Effective training addresses individual differences, accounts for interactions between diverse factors, and personalizes the training for the trainees (Fisher et al., 2021). The objective is to make cybersecurity an ingrained aspect of every employee's job, thus, allowing employee heuristics or intuition to drive the decision-making process related to avoiding cyberattacks. Moreover, software and technology can help to detect and prevent cyberattacks by flagging or blocking potentially harmful emails. However, reliance on technology also can create complacency among employees if workers assume the technology will catch all attacks (Cross & Gillett, 2020).

According to the research, best practices for optimizing cybersecurity training programs to mitigate the risk of phishing attacks include the following:

1. Ensuring that employees understand they are accountable for protecting personal and organizational information (Bayl-Smith et al., 2022) and rewarding employees who exhibit the correct phishing detection and reporting behaviors (Fisher et al., 2021).
2. Personalizing the training to address various employee personalities, learning styles, and job duties (Maalem Lahcen et al., 2020).
3. Conducting cyberattack simulations regularly to continuously evaluate the effectiveness of the training (Cross & Gillett, 2020) and to assess the areas that future training programs need to address (Maalem Lahcen et al., 2020).
4. Updating the training regularly to ensure relevance (Fisher et al., 2021) and also gamifying the training and making it interactive (Back & Guerette, 2021).

Traditional employee cybersecurity training is not effective in mitigating the human-related risks of cyberattacks. Nevertheless, creating a culture of cybersecurity is more effective when it combines employee training that is continuous, interactive, hands-on, and relevant with technological detection aids and reinforcement and reward strategies. Such training also must be updated regularly and adapted to various learning style preferences, gender differences, and personality considerations. Thus, a strong cybersecurity awareness culture paired with a personalized cybersecurity training program allows organizational leaders and managers to transform their workforce from their greatest cybersecurity weakness into their strongest defense against cyberattacks.

LIMITATIONS AND FUTURE RESEARCH

This topic paper is limited by the small sample of articles used to draw conclusions on cybersecurity training effectiveness, some of which were literature reviews. The literature on cybersecurity awareness and training is vast, and the author's search inadvertently might have omitted important articles that using various synonyms—such as electronic information security or cyber safety—might

have found. Additional insights could be discovered if these keywords had been included in the search. Although the author did not include these keywords in her search, her subsequent search efforts that included different terms did not provide new insights, indicating theoretical saturation. In addition, research on the effectiveness of cybersecurity training is affected by researchers' limited access to proprietary information. Many organizational leaders fear legal or reputational ramifications if cybersecurity weaknesses are exposed to the public, creating data access challenges for researchers.

The selected articles briefly addressed the concept of targeting specific job duties through cyberattacks; however, they included no details of the training strategies that might mitigate this risk. Future research should empirically examine how cybersecurity training might be tailored to address cyber concerns related to different job functions, such as finance, human resources, and product development.

REFERENCES

Back, S., & Guerette, R. T. 2021. Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. ***Journal of Contemporary Criminal Justice***, 37(3): 427–451.

Bayl-Smith, P., Taib, R., Yu, K., & Wiggins, M. 2022. Response to a phishing attack: Persuasion and protection motivation in an organizational context. ***Information & Computer Security***, 30(1): 63–78.

Cross, C., & Gillett, R. 2020. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. ***Journal of Financial Crime***, 27(3): 871–884.

Fisher, R., Porod, C., & Peterson, S. 2021. Motivating employees and organizations to adopt a cybersecurity-focused culture. ***Journal of Organizational Psychology***, 21(1): 114–131.

Georgescu, T. M. 2021. A study on how the pandemic changed the cybersecurity landscape. ***Informatica Economica***, 25(1): 42–60.

Gillam, A. R., & Waite, A. M. 2021. Gender differences in predictors of technology threat avoidance. ***Information & Computer Security***, 29(3): 393–412.

Hubbard, T., Klimavicz, J. F., Wong, S., & Steinhoff, J. C. 2021. Zero trust in a virtual cybersecurity world. ***The Journal of Government Financial Management***, 70(2): 12–19.

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. 2020. Review and insight on the behavioral aspects of cybersecurity. ***Cybersecurity***, 3(1): 1–18.

Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D., & McCormac, A. 2020. Matching training to individual learning styles improves information security awareness. ***Information & Computer Security***, 28(1): 1–14.

ABOUT THE AUTHOR

Christine Davis is a certified public accountant licensed in Florida and Michigan with over 20 years of experience in her field. She obtained a Bachelor of Arts in Mathematics and a Bachelor of Science in Accounting from Oakland University, a Master of Business Administration from the University of Michigan – Dearborn, and a Doctor of Business Administration from Georgia State University. She currently serves as the controller for The National Center for Construction Education and Research, Ltd. (NCCER). Before joining NCCER, she worked in controllership roles for a drone manufacturer and petroleum wholesaler/retailer. Preceding her transition to industry, the first half of her career was spent working in public accounting. With a passion for utilizing technology to create accurate, efficient, and transparent processes, her research interests include worker recruitment, retention, and training.