Computer Fraud and Security
ISSN (online): 1873-7056

Cybersecurity Training and Its Influence on Employee Behavior in Business Environments

Ahmed Shan-A-Alahi[1*], Md Mustafizur[2], Kazi Md Riaz Hossan[1], Abdullah Al Zaiem[1], Mohammed Mahmudur Rahman[3]

[1]Washington University of Science and Technology, Virginia, USA.
[2]University of the Potomac, USA.
[3]Southern University Bangladesh

Corresponding Author Email: aalahi.student@wust.edu

Abstract

The intent is to examine, as a petit question, how cybersecurity training programs affect employee behavior in the business workplace, as a possible measure to limit human factors that help to create structural vulnerabilities from within the organization. In many circumstances, negligent (or even noncompliant) human acts, overreliance on technology, and opposition to cybersecurity procedures result in cyber threats. Further, the research investigates how successful tailored training initiatives that utilize real world simulations and continued education can help employees become more aware and more engaged in helping to reduce risk through creating a proactive security culture. The study also identifies key elements of relevance, interactivity, and adaptability by which to integrate consideration of behavioral and cultural elements into training programs. The analysis shows the need for leadership involvement and continuous education to keep an attitude of security in place, covering the difference between technological measures and human behavior. The intent of these insights is to provide the needed guidance to organizations in shaping cybersecurity strategies that are effective in countering the advancing threats.

Keywords: Cybersecurity training, employee behavior, leadership

Introduction

People take a central place in the scenario of cybersecurity acting as the most dangerous link at the same time. In the current systems, technological measures of risk control and prevention of breaches are well applied but the major challenges which act as the root cause of breaches stem from human factors (Ifinedo, 2023). People at the workplace are often victims of cyber criminals' attacks via phishing, social engineering and other psychological tricks. Forgetting or worse choosing feeble passwords, getting tricked by phishing emails and not updating respective security programs provide the attackers with opportunities (Hong et al., 2023). Furthermore, behavioral factors including, over reliance, myopia, and resistance to change also form part of these vulnerabilities (Shaikh & Siponen, 2024). That one of the main reasons that the focus should be made on the people aspect as even the most developed information security systems are vulnerable to insufficient or even wrong employees' understanding or decision-making.

Delays in human behavior are facilitated by Cybersecurity training programs to reduce risks. Conferences are an essential aid to raising awareness, as well as arming people within an organization with information to identify and combat possible threats (Triplett, 2022). The best training normally focuses on the preventive measures which include recognizing phishing scams, reporting any suspicious activity or following organizational policies (Ertan et al., 2020). Real world scenarios and simulations enable employees to approach an attack situation calmly and with fewer mistakes (Kweon et al., 2021). In addition, ongoing training regarding cybersecurity means and ensures that everyone is on the same page about it. Through passing on information between the technical measures and the people, the training programs are important tools that help to eliminate risks and improve posture in an organization.

It is believed that in a world that is constantly getting more digital, risks are continually emerging in different forms with more sophistication and are very dangerous to organizational assets. Human factors remain one of the most significant threats when it comes to organizational cybersecurity measures solidification (Gillam & Foster, 2020). There is no doubt that most of the cyber-attacks are caused by accidental activities like falling for phishing scams, choosing bad passwords, or not being able to detect.

Social Engineering. This failure results in a chronic lack of understanding and readiness among the organisation's personnel, thus failing to close the gap between technological measures and practical threat management. This divergence shows the clear need for organizations to start focusing on the human element in security because no institution can ever fully protect itself from hackers.

In order to look into the effects of the cybersecurity training to the alteration of human behavior and minimization of the human factors in business environments. In order to review the focus of human interference in cybersecurity related issues at the organizational levels.

As for the goal of cybersecurity training programs, the studies carried out enable the assessment of the desirable level of vigilance and the minimisation of mistakes (Mashiane & Kritzinger, 2021). In this research, the various factors that will be sought after to establish the core aspects of the training programs that ensure improvement in the awareness and participation of the employees.

To investigate the dynamics of training and the improvement of proactive attitude towards cybersecurity. How human behavior does influences cybersecurity risks in organizations? To what extent does cybersecurity training increase employee awareness? What could be considered as key building blocks for the effective cybersecurity training program? What roles does training play in creating a security-oriented organizational culture?

This research is valuable to organizations that want its healthcare industry to enhance its protection against cyber threats. Analyzing the contributions of training programs to the behaviour of employees, the study contributes to the practical knowledge in minimization of HR related risks. It emphasise on the development of cybersecurity cultural principles, where organisational staff is not only user of applications but also the protector of its resources. The research helps in identifying the key factors essential for designing the efficient training and addressing the risks allowing the businesses to prevent losses and reduce vulnerabilities to threats that can harm their financial and reputational position. Furthermore, the research also emphasizes the importance of perpetual programs in relation to maintaining overall coherence in adhering to contemporary threats while managing the employee's behavior to safeguard the organization's integrity in virtue of the long term.

Literature Review

Issues related to human behaviour leading to cybersecurity incidents within organizations

Organizations rely heavily on the cybersecurity frameworks effectiveness that is largely determined by human behavior. Cyber security studies indicate that the majority of Incidents are caused by human error, clearly showing employees can be critical in securing a company's networks (Pollini et al., 2022). Behaviors like neglecting to use security protocols, having been phishing, or mishandling of sensitive data lead to vulnerabilities attackers take advantage of (Nifakos et al., 2021). Especially social engineering attacks use techniques such as urgency, fear, authority to manipulate the human psychology in order to deceive the information of confidential nature. In addition, employees are inexperienced with cybersecurity risks or rely too much on automated systems, so they underestimate their ability to protect data and systems (Maalem et al., 2020). This can also be a product of organizational culture i.e. staff at tech companies may lack the appropriate discipline, for example, as many companies place the least amount of priority on cybersecurity. But in addressing these behavioral challenges requires a nuanced understanding of how human actions couple with the technological systems and how to introduce targeted interventions.

Effectiveness of Cybersecurity Training programs in increasing vigilance and error reduction.

Human error is the most commonly cited cause of breaches and is known to be the weakest link in your cybersecurity chain. Employees are trained to recognize potential threats, e.g. phishing attacks, malware, or unusual system activity and who to tell in the company, if something like that happens (Griffin, 2021). As research shows, employees who are trained regularly and recognize all the signs are more likely to detect and report suspicious activities, and therefore reduce the chances of successful attacks. Simulation exercise, like mock phishing campaigns, are also effective in learning because it offers the hands on learning experience in controlled environment (Abrahams et al., 2024). Moreover, organizations that do one time session for education instead of ongoing education get more benefit from it as long term education lets the employees aware of emerging threats and best practices. But good training is also about the appropriate mindset — making not just employees technical proficient but active participants in keeping the organization's digital infrastructure safe.

Cybersecurity Training Programs to increase Employee Awareness and Engagement

If companies can't keep workers interested in, and committed to, a cybersecurity training program, it will probably fail. Several key elements emerge clearly from research, separating effective programs from their less effective counterparts. First, relevance matters—training needs to be targeted to the roles and risks employees face, so that content is useful and relevant to your employees' on a regular basis (Reeves et al., 2021). Take for example IT staff; instead of general staff that will be trained on phishing and using secure passwords; we can have them trained on advanced threat detection (Sabillon, 2022).

Interactivity is another major factor; we engage students with the help of gamification, real life scenarios, role playing activities. Equivalent in importance is adaptability, as cyber threats are always changing and training programs must be reassessed regularly on an on-going basis to address new emerging risks and new technologies (Popoola et al., 2024). In addition, creating a culture of openness in which employees will feel safe to report mistakes or suspicious activity without fear of retribution, improves the efficacy of the program. Together, these elements guarantee that training programs not only transmit information employees need to know, but incentivize them to act proactively in the face of cybersecurity challenges (Nasir, 2023).

Past research has widely studied the significance of human behavior in cybersecurity and the training program's function in reducing threats; however, major voids still exist. Finally, most of the literature focuses on the technical aspects of cybersecurity without sufficient regard to psychological and behaviour factors affecting employee behaviour (Wray et al., 2020). Cognitive biases can lead to cybersecurity vulnerabilities. Second, training program effectiveness studies often assess short term outcomes, such as immediate improvements in awareness, but often fail to measure long term behavioral or sustainable change.

In addition, little research exists in how to adapt training programs to particular organizational contexts, industries or employee roles, leading to generic approaches not adapted to specific context specific challenges (Abu-Amara et al., 2021). There is another gap in the experimentation with inventive training strategies like applications of gamification and AI propelled simulations which has not been very dependably explored in spite of their ability to support cooperation and efficiency (Alkhazi et al., 2022). Finally, there is inadequate emphasis placed on the feedback loop between organizational cybersecurity policies and employee behavior and how this loop can be used to update policies leveraging behavioral insights. As these gaps exist, it is imperative to tackle them so that we can improve our overall strategy for guiding human behavior into compliance with cybersecurity best practices.

Material and Methods

The current study uses a qualitative research design whose purpose is to comprehend the intricate and multi layered relationship between employee behavior, cybersecurity training programs and organizational practices. For this reason, this approach is justified in that it gives the depth and flexibility required for exploring subjective experiences, organizational contexts and behavioral changes, which cannot be adequately captured through quantitative methods (Campbell & Domene, 2024). The qualitative design is extremely useful to understand the motivations, the challenges,

and the people attitudes regarding cybersecurity training, driven by particular organizational dynamics as well as cultural factors.

In the study, a sample size of 10 purposive participants will be drawn from a mix of managers and employees that would guarantee answers from a diverse sample of participants drawn from different organization levels. The large sample size of this study is appropriate for qualitative research, as each participant is able to be explored in depth and neither the data collection nor analysis process are tedious. Managing is important, because they bring an insight into what is being implemented, and the proper manner that it is being done, and what are the strategic goals of the cybersecurity training programs (Kakar et al., 2023). They can also speak to the challenges and benefits of the firm for these initiatives. On the other hand, employees provide firsthand accounts of how the training affects their day to day behavior, awareness and their ability to respond to cybersecurity threats. Fusing these views, the study finds both systemic concerns and barriers and facilitators at the level of individuals to support a full account from the perspective of cybersecurity training effectiveness.

Semi structured interviews will be used for data collection as the main data gathering method to allow participants to speak freely about their experiences and opinions while ensuring the key areas of interest (training effectiveness, barriers to engagement and perceived impact) are addressed. This approach encourages open conversation and provides the researcher with the opportunity for deeper insights into insights into topics that are complex or sensitive and the like (such as resistance to change, the role of organizational culture).

Since thematic analysis enables systematic exploration of qualitative data for classification of patterns and themes, it has been chosen as the method for data analysis. The benefit of this method is it allows the researcher to distill large amounts of data into the 'meaningful themes' like 'Barriers to Effective Training', 'Engagement Strategies' or 'Cultural Influences on Cybersecurity Awareness.' The flexibility of thematic analysis allows the researcher to delve ‘deep’ into the data to capture both what people say, and what they mean, underneath the surface. For example, a manager may discuss missing resources for the training and employees implicitly may demonstrate the lack of trust in the organisational support system. Thematic analysis holds both layers of meaning thereby making an overall interpretation of the findings possible.

Also, thematic analysis is easy to apply because of its iterative nature, and this property is important to the study of dynamic and activity-context sensitive issues, for instance, cybersecurity training. The researcher can then narrow and extend themes as new insights come up throughout the research process (Braun & Clarke, 2023). For instance, if participants mention one of the challenges highlighted as unexpected, for example, language barriers with training materials, then such a comment can be placed into a new theme. With this adaptability the research stays relevant and responsive to the data.

This study is to combine a qualitative research design, thematic analysis and a purposive sample of 10 participants in order to have actionable insights that will assist with the improvement of cybersecurity training programs. In so doing, it will fill the gaps in existing literature but will also provide practical recommendations for doing so, with a view to enhancing organizational resilience to evolving threats by cultivating a cybersecurity conscious culture within organisations.

Results and discussion

Theme 1: Human behavior’s influence on cybersecurity risks

The second theme covers how individual actions and attitudes lead to cybersecurity vulnerabilities and will directly lead to the review of human interference impacting organizational cybersecurity. In this theme, the analysis exemplifies the psychological and behavioral points including fallacious dependency on technology, overlook, and lack of mindfulness that make them vulnerable to greater risks.

The IT department has everything well under control so I don't really worry too much of checking links and emails. It's hard to keep different passwords for different accounts, so sometimes I reuse one password among different platforms."

The theme focuses on how employees' small decisions each day including clicking on phishing emails, using weak passwords and breaking security protocols, creates entry points for cyber threats to work their way through their network. And second, organizational culture is also a factor in influencing these behaviors, as environments that do not prioritize accountability and cybersecurity awareness make high risk actions much worse.

"In the company, cybersecurity isn't really paid much attention to and most of us don't take it seriously. Then I thought that the antivirus would find some threat, and so I opened the email attachment without thinking twice."

The necessity of individual and systemic focused interventions to reduce behavior influencing human factors is underlined by this theme.

Theme 2: Cybersecurity training program's effectiveness

This area delves into how well a company's cybersecurity training programs prepare its people to detect and stop risks, consistent with the goal of measuring how training makes workers more self aware and less error prone as mentioned by the participant *"It wasn't consistent with follow up training sessions, so I missed most of the content within a few months. Examples in the training just didn't mirror the challenges I'm confronting with on the ground in my role."*. The analysis finds that many employees are trained, but the effect of training varies depending on frequency of training, training content relevance, and training delivery methods *They (the phishing simulation exercises) were very helpful in helping me learn what to be wary of in suspicious emails.*. As a general rule, training programs that actually include hands on simulations, practical exercises and real world scenarios are more successful at changing behavior than offering education only.

Additionally, the theme brings up challenges, like low retention rates for one time training sessions and the challenge of getting employees involved in generic, non interactive programs as stated by one of the participants i.e. *"After the training, I think I feel more comfortable about alerting IT for unusual activities."*

Theme 3: Foundation of effective cybersecurity training

This theme aligns with the research objective of identifying what makes a cybersecurity training program effective by identifying the key elements in facilitating an effective training program. The findings show that success is dependent on relevance, interactivity, adaptability and integration of culture.

"I feel the interactive role playing scenarios really helped me better understand how to respond in real life cyberattack situations. It didn't feel like the training material was specific to our realities and it was too generic."

Relevance means that the training is relevant to the people and specific roles they have. Interactivity, like gamification and role playing, keeps employees engaged in the eLearning module, and lets them have a controlled environment where they practice handling threats. Adaptability is because that the training adapts with the emerging cybersecurity risks and so on.

'I liked that the training included some real world examples of the latest in cybersecurity breaches and how to stop them.' It was made fun and easier to retain, the training was gamified."

As per this response, programs should educate employees and also allow them to express themselves in leveraging the achievements of organization assets. Both realistic and engaging methods coupled with constant updates makes the learning a sustainable one.

Theme 4: Positive training role

This theme studies how cybersecurity training, through specifc organizational interventions, contributes to building a culture where employees regard themselves as cyber security even at the organizational level, in line with the goal of studying the role of training in creating a security conscious culture of the organization.

"It was through the training that I was made to realize that cybersecurity not only the IT department has to think about but it is also my responsibility. We can be more efficient in learning from mistakes when we have this open communication culture about cybersecurity issues."

Analysis shows that training alone is not enough to cultivate such a culture, and requires constant leadership messaging, accountability policies and a workplace where it's safe to report mistakes.

"We have management that always brings up cybersecurity in every team meeting, which makes us more aware. There is a hesitance in my team to report mistakes because they'll be punished, which breaks down training."

Results from the survey show that a culture in which security plays a major role encourages a proactive, rather than reactive, attitude, including vigilance, cooperation and reduced probability of compromises. But it also demonstrates that strong cybersecurity cultures mean organizations will bake training into their broader values and priorities rather than treating it as a one time event.

Discussion

Critical insights into the interplay between human behavior, the organisation's culture and cybersecurity training in organisations are also discussed from the findings derived from the identified themes. These insights are important to improve cybersecurity training programs and to form a proactive security thinking among employees.

Human behaviour becomes a central element in understanding the cybersecurity risks in organizations. Over relying on the technological safeguards, forgetting to follow the security protocols or failing to take enough account of personal responsibility were mentioned by the participants as major vulnerabilities (Qusa & Tarazi, 2021). This indicates that employees are not conscious of how their actions drive down cyber threats. Cybersecurity was seen by many employees as an IT department problem, leaving people unprepared and guilty of careless actions like hitting phishing links or reusing passwords (Waddell, 2024). What this points to is the importance of targeted behavioral interventions to help close the gaps and (re)enforce that cybersecurity is everyone's responsibility. Organizations can incorporate behavioral psychology into their training programs to develop not only training that informs individuals but also motivates them to consistently practice secure behaviors.

As the responses show, the design and delivery of cybersecurity training programs are key determinations to the effectiveness of them. Many of the participants felt that the interactive and scenario based training exercises were useful to better detect and respond to cyber threats; but some complained that generic or one off scenarios were lacking (Andronache, 2021). For example, simulation exercises such as a phishing test, improved their employees' ability to detect and avoid suspicious emails (Chowdhury et al., 2022). The knowledge was often forgotten over time, though, without reinforcement in follow up sessions or updates. Not only does that enable the apprehending of the role specific risk of the employees yet, it emphasizes the need of sustained training. Continuous education must be prioritized by organizations with additional focus on iterative training to adapt to the coming threats and regular refresher. This approach guarantees that staff are always attentive and ready to react quickly to changes in the ever changing world of cybersecurity (Triantafyllou & Georgiadis, 2022).

Moreover, the analysis reveals the key elements what makes good cybersecurity training programs, namely relevance, interactivity and adaptability. Participants appreciated training programs that included gamification, role playing, and practical simulations because through these ways they were engaged and had better retention of the information. Nonetheless another recurring concern was the limited role specific content in a lot of training sessions. Generic content was not helpful and therefore did not carry much practical applicability as it did not cover specific problems

of employee (Sharif & Ameen, 2021). In addition, the world of cybersecurity threats is always changing, and so the training programs need to evolve also to include the latest examples and techniques. It is imperative that training be both effective and pertinent and sensitive to the melting pot of needs that we know represents the array of unique jobs. These elements allow organizations to build programs that strengthen technical knowledge but also educate employees into active participants of these assets' protection (Ashley et al., 2022).

Moreover, they found that cybersecurity training can make a large contribution to supporting a security-oriented culture, but that on its own, it is not enough. Participants noted that a culture where cybersecurity is a shared priority requires a non-punitive environment as well as consistent leadership support (Arora & Mendhekar, 2021). The results revealed that employees engaged with and demonstrated high vigilance in organizations in which management underscored cybersecurity in meetings and led by example regarding security conscious behavior. In contrast, fear of punishment for mistakes led employees to avoid learning from the training and prevented them from reporting suspected threats (Zhang-Kennedy & Chiasson, 2021). These responses show the need for an organization to be embedded with cybersecurity principles deep in the cultural framework of the organization. If leadership instead regularly exhibits commitment to cybersecurity and an open environment that fosters trust and accountability, there is a higher chance that everyone else will rally around the effort. That, in turn, makes sure that the employees feel more empowered to act on their training and jointly defeat risk.

Taken together, these findings suggest that cybersecurity training programs are essential, but that their effectiveness is not a one dimensional issue, it is the culmination of multiple dimensions in behavioral, educational, and cultural elements. Both the technical and the psychological side of cybersecurity must be addressed in training so that employees not just get all the skills they need, but also are proactive and responsible about cybersecurity in general (Pham et al., 2021). Sustaining the behavioral and cultural changes required for effective cyber threat mitigation require leadership support, continuous education and openness and accountability culture. Through this holistic view, organizations can begin to close the divide between the technological safeguards and human engagement, improving their collective resilience in ever increasing complex and dynamic cyber threat environment.

Many cybersecurity training programs will help, but they aren’t guaranteed to protect you unless you put thought into how you plan, deliver and support them. Training must go deeper than surface level awareness initiatives. Good organizations start by building an ecosystem in which employees consider cybersecurity a shared responsibility embodied by leadership and sustained through ongoing, compelling, and relevant cybersecurity training programs (Klein & Zwilling, 2024).

Additionally, creating an open and accountable culture empowers employees to act on their training thus reducing risk and strengthening the organization’s cybersecurity posturing. Still, a large number of participants indicated that the content was not always appropriate to their respective jobs and responsibilities, making the content almost impossible to put into practice (Decusatis et al., 2022). The results indicate a flexible training structure will have to incorporate general cybersecurity principles as well as job related threats. And, not least, cybersecurity is a moving target and requires great adaptability (Angafor et al., 2020). The training has to be updated for the relevant and the effective scenarios and technologies. Organizations can create an environment in which employees are well prepared to recognize risks, but also motivated to do something about them by embedding interactive and personalized aspects into their programs.

The discussion contributes to actionable insights that closely match up with the research objectives and questions. Addressing the human behavior aspect, enhancing training methodologies and creating a security oriented culture is the way for the organizations to bridge the gap between the technological measures and the humans in doing cybersecurity practices.

Conclusion

These findings suggest that the human behavior, training effectiveness, and organizational culture will be the critical factors to address when working to mitigate cybersecurity risks. The weakest link in organizational cybersecurity still remains human factors such as negligence, over reliance on technology, lack of personal accountability and other kindred ills. Training programs have been seen to be a useful tool for generating awareness and providing employees with the tools to recognise and react to threats, but only if they are interactive, relevant to the individual's context, and updated regularly. In addition, fostering a security oriented organizational culture by carrying out its impact via leadership and creating an environment of trust and accountability is key to long term sustained behavioral change and embedding of cybersecurity principles into the core of the organization.

This research has future implications to show that cybersecurity training and risk management will require a more holistic approach. Organizations need to be investing in continuous and adaptive training programs that deal with both general cybersecurity principles and the particular challenges of particular roles within the organization. Innovation like gamification, real world simulations and AI driven personalized training modules can take into account be applied to elevate engagement and retention. Beyond that, extraverts could be integrated with training design as they can reduce psychological barriers and encourage proactive employee behavior. Training is more than merely instruction, teaching people how to spot and report issues, but organizations also have to foster a culture of openness where telling a supervisor of a mistake or maybe even a potential threat is seen as an opportunity to learn and grow, and not something that is going to come back and damage the organisation.

Leadership must stand up and be proactive in demonstrating the commitment to cybersecurity, making it an organization wide item everyone is responsible for at all levels. Future research may address the long term impact of such tailored training programs, probe how emerging technologies can make training more effective, and suggest means through which cybersecurity practice can be embedded smoothly into organizational culture. These steps are paramount to creating robust organizations better able to traverse an increasingly artificial and volatile cyberspace threat landscape.

This research provides additional confirmation that cybersecurity is as much a people problem as it is a technological problem. These behaviors, attitudes, and decisions of employees either strengthen or compromise an organization's cybersecurity posture. Although we continue making technological advancements to face increasingly sophisticated cyber threats, the human part is usually the weakest link. In this sense, it highlights the importance of giving employees not only technical knowledge but, what is even more important, understanding in what your important role in preserving the organizational assets is. An effective training program that is relevant, interesting and regularly updated can fill the gap of technological measures versus human behavior. However, training is not enough without the organizational culture to support a cybersecurity mindset that is shared, championed by leadership, and backed by trusting and open communication.

In the future, companies must shift to a multi-pronged strategy that includes training, as part of a wider strategy of behavioral and cultural change. This covers work like embedding cybersecurity principles into day to day workflows, encouraging active employee participation, and ensuring cyber security aligned with the organization's strategic objectives. Improvement of training methodologies, the application of adaptive technologies and personalized learning paths will be important means of overcoming emerging threats and keeping employee engagement. Furthermore, all these stake outlined above can also provide a platform for cross functional collaboration to take place across technical and non-technical teams, forming a more coherent and holistic cybersecurity framework. Future research should further long term behavioral impacts of different training methods as well as the role of leadership in defining a resilient cybersecurity culture. Addressing these areas allows organizations to build a more resilient and ready stance against the ever changing threat landscape. Based on the findings of this study, there are avenues to empowering actionable strategies that put humanity at the heart of cybersecurity resilience.

References

1. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1-25.
2. Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M., & Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. International Journal of Information Technology, 13(6), 2371-2380.
3. Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior. IEEE access, 10, 132132-132143.
4. Andronache, A. (2021). INCREASING SECURITY AWARENESS THROUGH LENSES OF CYBERSECURITY CULTURE. Journal of Information Systems & Operations Management, 15(1).
5. Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. Security and privacy, 3(6), e126.
6. Arora, A., & Mendhekar, A. (2021). Innovative techniques for student engagement in cybersecurity education. In Data Management, Analytics and Innovation: Proceedings of ICDMAI 2020, Volume 1 (pp. 395-406). Springer Singapore.
7. Ashley, T. D., Kwon, R., Gourisetti, S. N. G., Katsis, C., Bonebrake, C. A., & Boyd, P. A. (2022). Gamification of cybersecurity for workforce development in critical infrastructure. Ieee Access, 10, 112487-112501.
8. Braun, V., & Clarke, V. (2023). Toward good practice in thematic analysis: Avoiding common problems and be (com) ing a knowing researcher. International journal of transgender health, 24(1), 1-6.
9. Campbell, A. K., & Domene, J. F. (2024). Zooming into qualitative research: online adaptation of the action-project method research design. Qualitative Research in Psychology, 21(3), 307-327.
10. Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies.
11. Decusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., ... & Mah, B. (2022, January). A cybersecurity awareness escape room using gamification design principles. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0765-0770). IEEE.
12. Ertan, A., Crossland, G., Heath, C., Denny, D., & Jensen, R. (2020). Cyber security behaviour in organisations. arXiv preprint arXiv:2004.11768.
13. Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. Computers in Human Behavior, 108, 106319.
14. Griffin, L. (2021). The Effectiveness of Cybersecurity Awareness Training in Reducing Employee Negligence Within Department of Defense (DoD) Affiliated Organizations-Qualitative Exploratory Case Study (Doctoral dissertation, Capella University).
15. Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N. L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. Education and Information Technologies, 28(1), 439-470.
16. Ifinedo, P. (2023). Effects of security knowledge, self-control, and countermeasures on cybersecurity behaviors. Journal of Computer Information Systems, 63(2), 380-396.
17. Kakar, Z. U. H., Rasheed, R., Rashid, A., & Akhter, S. (2023). Criteria for assessing and ensuring the trustworthiness in qualitative research.
18. Klein, G., & Zwilling, M. (2024). The weakest link: employee cyber-defense behaviors while working from home. Journal of Computer Information Systems, 64(3), 408-422.
19. Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. Information Systems Frontiers, 23, 361-373.
20. Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3, 1-18.

21. Mashiane, T., & Kritzinger, E. (2021). Identifying behavioral constructs in relation to user cybersecurity behavior. Eurasian Journal of Social Sciences, 9(2), 98-122.
22. Nasir, S. (2023, July). Exploring the effectiveness of cybersecurity training programs: factors, best practices, and future directions. In Proceedings of the Cyber Secure Nigeria Conference.
23. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119.
24. Pham, H. C., Ulhaq, I., Nguyen, M., & Nkhoma, M. (2021). An exploratory study of the effects of knowledge sharing methods on cyber security practice. Australasian Journal of Information Systems, 25.
25. Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work, 24(2), 371-390.
26. Popoola, O. A., Akinsanya, M. O., Nzeako, G., Chukwurah, E. G., & Okeke, C. D. (2024). Exploring theoretical constructs of cybersecurity awareness and training programs: comparative analysis of African and US Initiatives. International Journal of Applied Research in Social Sciences, 6(5), 819-827.
27. Qusa, H., & Tarazi, J. (2021, January). Cyber-hero: A gamification framework for cyber security awareness for high schools students. In 2021 IEEE 11th annual computing and communication workshop and conference (CCWC) (pp. 0677-0682). IEEE.
28. Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. SAGE open, 11(1), 21582440211000049.
29. Sabillon, R. (2022). The cybersecurity awareness training model (CATRAM). In Research Anthology on Advancements in Cybersecurity Education (pp. 501-520). IGI global.
30. Shaikh, F. A., & Siponen, M. (2024). Organizational learning from cybersecurity performance: Effects on cybersecurity investment decisions. Information Systems Frontiers, 26(3), 1109-1120.
31. Sharif, K. H., & Ameen, S. Y. (2021, December). A review on gamification for information security training. In 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI) (pp. 1-8). IEEE.
32. Triantafyllou, S., & Georgiadis, C. (2022). Gamification of MOOCs and security awareness in corporate training.
33. Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. Journal of Cybersecurity and Privacy, 2(3), 573-586.
34. Waddell, M. (2024, January). Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. In Healthcare Management Forum (Vol. 37, No. 1, pp. 13-16). Sage CA: Los Angeles, CA: SAGE Publications.
35. Wray, R., Massey, L., Medina, J., & Bolton, A. (2020). Increasing engagement in a cyber-awareness training game. In Augmented Cognition. Human Cognition and Behavior: 14th International Conference, AC 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part II 22 (pp. 147-158). Springer International Publishing.
36. Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys (CSUR), 54(1), 1-39.