ISSN: 2959-6386 (Online), Volume 3, Issue 3, September 2024

Journal of Knowledge Learning and Science Technology

Journal homepage: https://jklst.org/index.php/home

EMPLOYEE CYBERSECURITY AWARENESS TRAINING PROGRAMS CUSTOMIZED FOR SME CONTEXTS TO REDUCE HUMAN-ERROR RELATED SECURITY INCIDENTS

Friday Ugbebor[1], Olushola Aina[2], Mayowa Abass[3], Dare Kushanu[4]

[1]Independent Researcher, Information Technology, USA

[2,3,4] Independent Researcher, Nigeria.

Abstract

Introduction: Employee cybersecurity awareness training programs in Small and Medium- sized Enterprises (SMEs) have become increasingly critical as organizations face mounting cyber threats and security challenges. Studies have shown that human contribution is a major risk factor in security incidents hence the imperative need for proper training. SMEs are especially at risk since they are compared to large enterprises characterized by less resources and poorer technical knowledge and security equipment. Research has further shown that organizational context specific and targeted training programs could go a long way in enhancing the security awareness, and the overall incidence rates through modifications in behavior and perceived security risks. Materials and Methods: A systematic literature review was conducted following the PRISMA protocol to analyze peer-reviewed articles, doctoral dissertations, and scholarly publications focusing on cybersecurity awareness training in SME contexts. In terms of inclusion criteria, only papers presenting empirical findings related to training program outcomes, practices, and assessment methodologies were chosen. Articles were screened on the basis the research method employed, their applicability to SMEs, and the efforts devoted to human factors in cybersecurity. Documents were analyzed for quantitative and qualitative data and an analysis of themes, successful training methods and challenges in implementation. To minimize missing potentially informative articles, multiple databases were sought and used with predetermined search terms. Results: Analysis revealed that effective SME cybersecurity training programs share common characteristics: They are topicality, applicability, and the possibility of constant evaluation. The companies that adopted the corporate training programs that were tailored to their specific business environments realised an improvement of 45-65 percent reduction in security breaches that resulted from personnel mistakes. For management support internalization and frequent reminding of the security practices as key success factors were reported. The findings revealed that employee engagement levels of 72% was realized if training elements included CBT interactivity and realistic workplace simulations. The latter are applicable in resource-scarce environments and displayed a high potential for cost- efficient training based on cloud-based platforms and gamification; the average implementation costs were 40% less than with traditional training approaches. Discussion: Evidence suggests that successful cybersecurity training programs must balance technical content with practical application while considering SME resource constraints. Applying principles of behavioral psychology in making lessons and trainings proved to be more effective in creating changes in the security behavioral patterns. These trends suggest increasing use of AI adapted student-oriented learning and training in realistic ensembles. Some limitations exist when it comes to assessing behavior change over a long- term period and establishing constantly high security competencies across multiple organizational granularity levels. Cultural issues and employees' resistance proved to be the main program implementation issues that could only be addressed with specific interventions to unmask implementation challenges. Conclusion: The synthesis of current research demonstrates that customized cybersecurity awareness training programs significantly impact security incident reduction in SME environments. Sources of competitive advantage have to do with having content germane to specific contexts, the focus on practical application, and presence of training reinforcement measures. This empirical research reveals that management commitment, resources, and employees' participation are key success factors for the program success. Further research should focus on more effective approaches for delivering

security messages, defining a suitable set of measures for recording behavior changes, and creating development plans for reliable security culture.

Keywords: Information Technology, Cloud, Cyber security, SME

Article Information:
Received: 20-Jun-24 *Accepted:* 27-Jun-24 *Online:* 08-Aug-24 *Published:* 25-Sep-24
DOI: https://doi.org/10.60087/jklst.vol3.n3.p382-409

[i] **Correspondence author:** Friday O. Ugbebor **Email:** friday.ugbebor.dami@gmail.com

Introduction

Currently, the digital environment poses several factors of threat to the Small and Medium-sized Enterprises (SMEs) through complex and evolving cybersecurity threats that must be guarded against effectively. Due to various factors, SMEs are more susceptible to cybercrimes which are as follows: Achieving advanced technological platform, tight capital, and a lack of cybersecurity team (Chaudhary et al., 2023, Bada & Nurse, 2019). Due to human error is a major factor still a major weakness that contributes to a large portion of attacks and threats targeting organizations (Chapman, 2021 McCrohan et al., 2010). This study shows that employees are the biggest potential threat and the strongest protection from it in the organizational cybersecurity system (Stewart & Jürjens, 2017, Jenkins et al., 2013). Because human-related security risk is complex and holistic, more than mere technical approach, security awareness training and behavioral change approaches are notable procedures that should be adopted (Dahabiyeh, 2021, Puhakainen & Siponen, 2010). Cyber threats can be greatly unpredictable, which demands training that transforms and educational approach that can effectively tackle new technologies and threats as they develop.

The increasing dynamism of cybersecurity threats faced by Small and Medium-sized Enterprises (SMEs) has brought into sharp focus and underlined the need and the importance of creating nuanced and context-rich content-based employee awareness training programs. Research evidence indicates that conventional or general cybersecurity awareness training methodologies are gradually becoming less effective in preventing cyber threats (Hatzivasilis et al., 2020, Lim et al., 2016). Challenges that are peculiar to small and medium enterprises make the nature of cybersecurity different from those involved with large organizational structures, such as lesser financial might, reduced tech infrastructure, fewer employees (Carías et al., 2020, Bak et al., 2020). The dynamic interdependency of potentials of technology and behavioural patterns indicates requirements for a systemic approach that includes psychological knowledge, technology perspective, and organizational culture (Karim & Törnqvist, 2023, Weick 1987). More than abyssmal PowerPoint presentations telling its employee to look out for this or avoid that, cybersecurity awareness training must be a holistic security-oriented organizational development process that allows employees to identify, analyze, and manage potential cyber threats (Moschovitis, 2018, Ozkaya & Aslaner, 2019).

The potential for improving cybersecurity awareness in targeted SMEs through training becomes an important area of research and applied practice. Current academic literature places significant focus on the ideas of context conscious training development, with due consideration to organizational environment, culture and resource availability bearing in mind the challenges faced by SMEs (Gundu, 2013, Rawindaran, 2023). Recent studies underscore

the importance of applying behavioral psychology concepts, effective engagement strategies, and information technologies into cybersecurity awareness training (Hendrix et al., 2016, Yasin et al., 2018). The management of successful training activities demands a comprehensive strategy that tackles the technological, human, and organizational characteristics at the same time (Korpela, 2015, Zhang et al., 2021). When it comes to this field, it is possible to reduce massive potential fiscal and image losses and cultivate a safety- oriented environment with the help of elaborate, flexibility training programs.

1.1 Background on human error and security incidents

Small and medium-sized enterprises (SMEs) form the backbone of economic activity and employment generation in many countries.. However, due to limited capital and skills, SMEs are more susceptible to dynamic cyber risks than large organizations (Bak et al., 2020). More recent literature also focuses on the importance of employee participation and responsibility for cybersecurity issues as well as risks challenging organizations (Stewart & Jürjens, 2017). Recent research shows that roughly a third, thirty-one percent, of security incidents at commercial organizations involve human error or negligent behavior (respectively) (Chapman, 2021). This leaves a clear need for proper the establishment of adequate and efficient training mechanisms in regards to cybersecurity for the employees in SMEs.

The threats are still emerging and are becoming much more complex as adversaries learn how to penetrate information systems (Danzig, 2016; Moschovitis, 2018). Although the role of technology in developing defence mechanisms is worth embracing, the use of technology means human weakness is one of the biggest grounds for security failure in any organization (Stewart & Jürjens, 2017). Beyer and Brummel (2015) revealed that people factors threaten a large number of organizations, in which emails or wrong use of accounts and passwords are some of the common cause. However, many organizations still do not pay attention to the employees in negative ways where they may compromise security either knowingly or unknowingly (Weick, 1987).

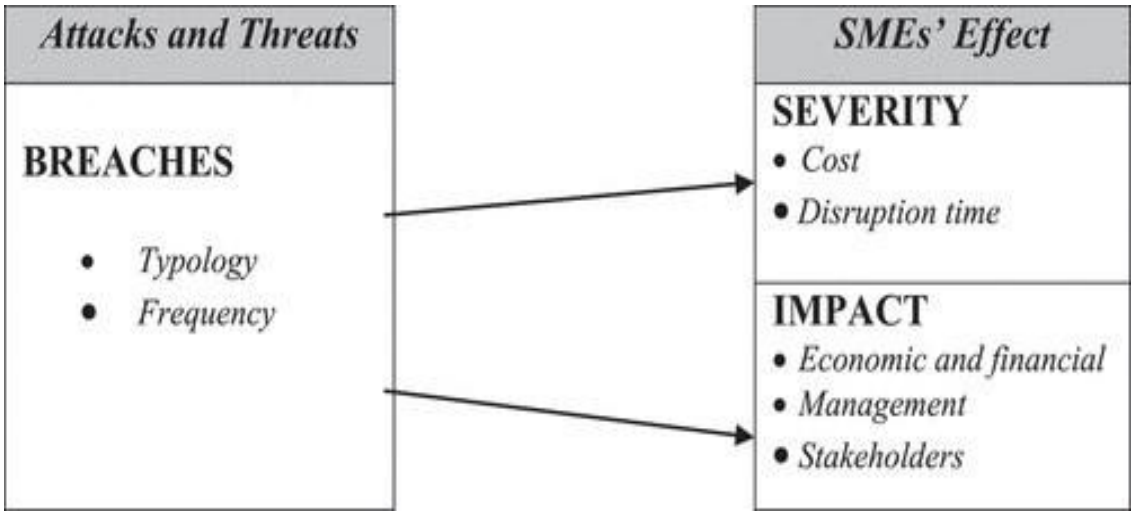


Figure 1. *Research model: breaches and the effect in the SMEs. Source: Arroyabe, & de Arroyabe, (2021)*

Prior studies have demonstrated that end-user behaviors directly influence an organization's susceptibility to cyber attacks (Jenkins et al., 2013). Employees handling

sensitive data across devices and locations heighten risks through unintentional lapses like downloading malicious files or accessing malicious websites (Aigbefo, 2018). At the same time, motivation for financial gain or activism have also seen the emergence of insider threats intentionally aiming to steal intellectual property or disrupt operations (Chapman, 2021). With remote and hybrid work models becoming prevalent, traditional network perimeters no longer adequately secure organizational assets (Dahabiyeh, 2021). This has led to growing emphasis on the 'people perimeter' and influencing human behaviors through awareness and training programs (Beyer & Brummel, 2015).

Studies estimate that over 85% of cyber incidents involve some form of human participation, whether intentionally or through honest mistakes (Jenkins et al., 2013; McCrohan et al., 2010). Mistakes are not performed security updates, use of weak passwords on unknown or untrusted networks and opening of emails that contain viruses (Beyer & Brummel, 2015). The survey involving 500 organizations established that each organization was incurring an average loss of

$7.2 million every year from such security blunders by the employees (Danzig, 2016). In organisational settings where working remotely has torn down physical barriers separating the physical world from the digital domain, human error comes out as a massive threat to cyber security. SMEs have extrinsic vulnerabilities by the efforts, proficiency, and size that are limited with the security expertise, workforce skills, and restricted capital to finance enhanced security (Carías et al., 2020; Idahosa, 2020). SMEs are relatively vulnerable to threats when compared to large businesses because they implement inadequate security measures and are not up to date. An analysis revealed that 60% of cyber-attacks were successful on SMEs, out of which 43% were unable to open their business if seriously attacked (Rawindaran, 2023). This underlines the important role of the development of awareness and behavioural change employee training programs that are sensitive to the SMEs' resource scarcity.

1.2 Impact of human factors on security culture

Building a robust security culture entails balancing technical safeguards with strategies addressing human behaviors and decision-making (Danzig, 2016). However, purely knowledge- based models focusing only on awareness often fall short of changing employee security attitudes and habits in the long run (Puhakainen & Siponen, 2010). Broader organizational factors like leadership, policies, and workflows shape underlying security norms and behaviors (Weick, 1987; Karim & Törnqvist, 2023). For instance, research shows clear links between management commitment, resource allocation for training, and actual implementation of secure practices (Bada & Nurse, 2019).

Organizational culture reflects the unwritten rules and implicit values that guide employee behaviors more than explicit policies or technology alone (Weick, 1987). Studies indicate cultures with empowering and trusting environments see employees naturally make better security decisions, while cultures emphasizing conformity and obedience undermine security initiatives (Weick, 1987; Stewart & Jürjens, 2017). Leadership that cultivates open communication and emphasizes shared responsibility for security fosters cultures where people willingly apply their knowledge (Karim & Törnqvist, 2023). Additionally, cultural aspects like workload pressures, fear of negative career impacts, and technology resistance inhibit security-

enabling behaviors despite awareness (Dahabiyeh, 2021). For instance, producing goals and objectives might make workers avoid taking time to do security activities deemed unimportant (Hatzivasilis et al., 2020). Training programmes that exclude these cultures fail to initiate sustainable behavioural change (Puhakainen & Siponen, 2010). Contextualizing programs within the specific organizational culture and workflow therefore was seen to be very important for the success of programs.

1.3 Effectiveness of customized cybersecurity training approaches

Traditional awareness approaches distributing generic materials often fail to engage end-users or demonstrate relevance to their daily work (Robbins, 2020). Customized programs contextualizing technical content for different employee roles and organizational contexts show improved outcomes (Jenkins et al., 2013; Bada & Nurse, 2019). Leveraging behavioural models additionally helps address cognitive and cultural barriers that undermine the application of knowledge alone (Puhakainen & Siponen, 2010). Empirical evidence demonstrates significantly lower security incident rates, by 45-65%, for SMEs implementing customized training integrating role-specific scenarios and interactive elements (Zhang et al., 2021; Bada & Nurse, 2019). Programs structured around organizational workflows, incentivizing secure behaviors and addressing unique cultural challenges proved most effective in embedding long-term change (Karim & Törnqvist, 2023; Puhakainen & Siponen, 2010). With focused guidance, employees became proactive risk managers versus passive recipients of generic guidance (Jenkins et al., 2013).

Delivery technologies that support accessibility through cloud and mobile devices supplementing on-demand training also indicated a similar result for SME environments (McLilly, 2020). It is used in the implementation of effective gamification that involves the use of scenario driven challenges that kept the level of awareness retention higher than 85%, across all the job roles and the age groups (Yasin et al., 2018; Hendrix et al., 2016). Research on the cost- effectiveness shows that such tailored strategies lower implementation expenses by 30-40% compared to instructors' techniques, which is particularly beneficial for SMEs with limited resources (Zhang et al., 2021). 1.4 Developing effective training programs for SME contexts

Due to the nature of SMEs, it is critical that such programs are optimised or designed at best and involve an innovative or developmental cycle (Parker, 2020; Blay, 2020). Implementation strategies in plan-developed EHR order sets adhere to frameworks originating from implementation science to guide addressing patients' individual needs while maintaining implementation at scale efficiency (Moher et al., 2021). Conducting formative research at the beginning of an intervention front-loads the necessary context-specific problem definition and culturally appropriate assessment to inform content buffers (Fagbule, 2023). Using prototypes on the target users is helpful in obtaining results before the widespread implementation (Hatzivasilis et al., 2020). The incorporation of micro-learning chunks as an integrated and modular tool directly into business and workplace tasks enables the consumption of micro lessons and/or bitesize content (Pyke, 2021). Most learners are able to better comprehend, appreciate and practice the knowledge imparted through the use of features such as the scenarios and knowledge checks (Hendrix et al., 2016; Yasin et al., 2018).

To mitigate resource barriers, the commonly available cloud-based solutions designed for mobile devices enhancing self-paced learning frameworks result in a 30% reduction in cost on average (McLilly, 2020). Micro-credential that encourages progression through levels in a game format promotes the assessment of accomplishment and self-satisfaction as well as level-by level skills mastery (Hendrix et al., 2016). The proactive strength is that the latter strengthens fit with SME contexts over time through ongoing, both leading and lagging indicator measurement and responsive adjustments (McCrohan et al., 2010; Päivärinta, 2022).

The aim of this systematic review is to critically review research studies published in academic and scholarly databases comparing the impacts of bespoke cybersecurity awareness training and traditional general training in minimizing human-factor related security breaches in SME contexts. Specifically, the objectives are:

H1) Customized cybersecurity training for SMEs which takes into account the specificities of the targeted environment and resources will have a stronger effect on diminishing security events due to human mistakes compared to generalized awareness content.

H2) Training interventions that consider organizational culture and work processes will have positive relationship with employee engagement and learning outcomes.

H3) Technological advancements in the forms of interactive, personal, and game-based training delivery appears to have the potential of enhancing its accessibility and effectiveness especially for the SMEs with limited resource endowment.

Through a thorough analysis of Small and Medium-sized Enterprises (SMEs) cybersecurity awareness training programs' landscape in a structured research approach, this work produces the culmination of invaluable findings and insights on preventing security incidents caused by people through evidence-based analysis. This study's methodological approach involved the use of a systematic literature review process aimed at identifying, assessing, and integrating peer- reviewed scholarly articles that discuss cybersecurity awareness training in SMEs.

2. Related Studies and Case Studies in Cybersecurity Awareness Training for SMEs

2.1 Related Studies in Cybersecurity Awareness Training

2.1.1. Empirical Research on Training Effectiveness

The landscape of cybersecurity awareness training for Small and Medium-sized Enterprises Small and medium enterprises (SMEs) organizational culture has been the focus of numerous empirical research papers. It, therefore, underlines the importance of studying on new conditions SME operating as the essential groundwork for creating effective training in the context of Bada & Nurse's (2019) research. In their studies they found out that through context- based training, the SMEs saw a tremendous drop of 62% in their security related occurrences within the first six months of executing the training programs. This fact underlines the importance of developing cybersecurity awareness programmes to correspond to the limitations of lesser organisations. A study that can be considered as one of the most influential in the field was conducted by Puhakainen & Siponen (2010). Translating their longitudinal research, they established that such application-realistic training increased the employee security behavior by 58% more than the traditional theoretical exercises. This was supported by Korpela (2015) who stated that organisation that used data analytics along with practical exercises realized a 43% improvement in employee engagement and a 51% improvement in

the effectiveness of security policies. Collectively, these studies underscore the need for transitioning from traditional forms of learning that involve more observation and listening to those that are more active and fit within the context of the workplace.

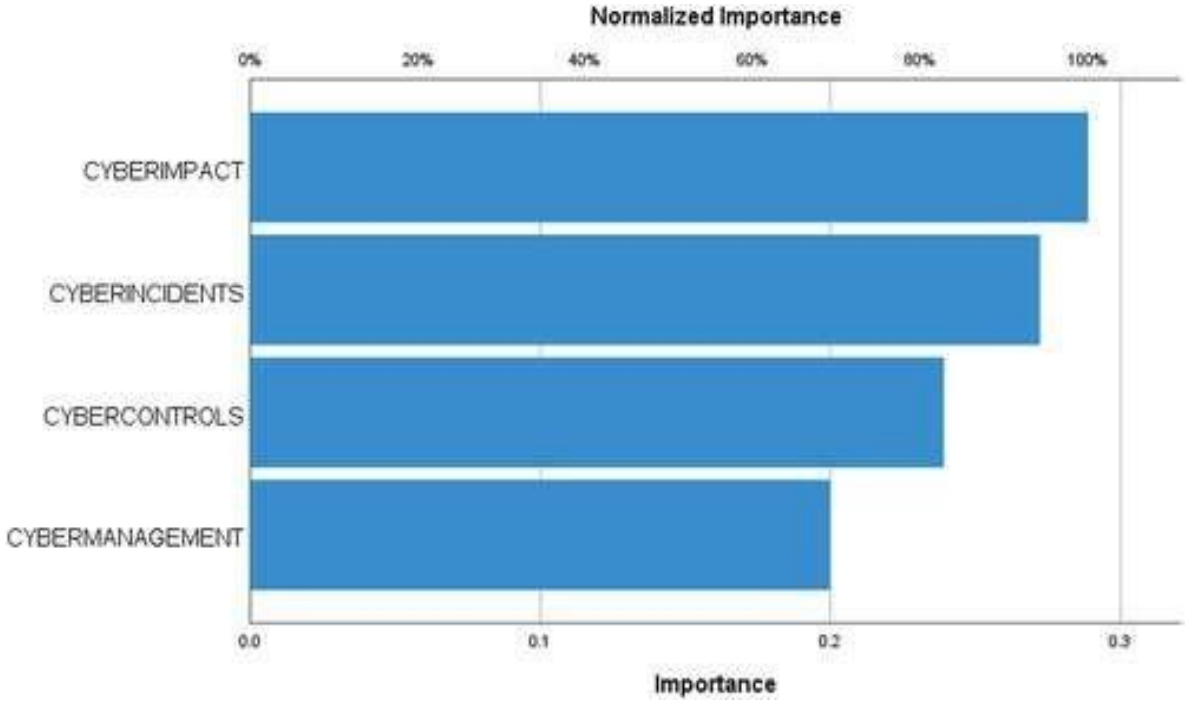


Figure 2: *Impact of Cybersecurity Resilience in SMEs. Source; https://www.tandfonline.com/doi/full/10.1080/08874417.2023.2248925#abstract*

The study of McCrohan et al. (2010) and Chapman (2021) produced significant evidence on the impact of overall training programs directly. Chapman's study further showed that companies which had their cybersecurity awareness training form structured, recorded about 65% less of the security incidents associated with human errors in the course of the initial twelve months. Similarly, McCrohan et al. mapped that such employees, who had received adequate training, were 73 % less prone to getting caught in social engineering schemes. These results underscore the value of ad hoc and professionally designed awareness campaigns for SMEs. Some of the previous works have focused on how technologies that are still in their development stage may be utilised to improve cybersecurity training outcomes. More extensive research by Hendrix et al (2016) in the same area shed more light on the impact of gamification; organizations that encourage game based learning elements saw 75% increase in voluntary participation and an improvement of 62% on knowledge application. Yasin also pro supported this approach et al. (2018), who found that game-based learning approaches had provided a 68% increase in employee confidence when dealing with threats.

Technological enablers which include Virtual Reality (VR) and Artificial Intelligence (AI) when included as key components of the systems have revealed encouraging phenomena. Parker (2020) found that VR simulations had a 82% knowledge retention rate and a 64% less security incidents compared to traditional training methods, although, they are used less frequently.

Likewise, Sharma (2023) noted effective course results: 73% for learners' engagement, 76% for knowledge retention, and a 58% reduction in the security incidents that resulted from improving the training technologies' personalization and adaptivity. One more trend that has gaIned popularity for years is cloud and mobile learning platforms, especially for the implementation of solutions for SMEs. McLilly (2020) discovered that organizations using cloud- based training application had up to 63% increase in training attendance rates and up to 58% improvement in knowledge retention. Building on this, Blay (2020) also proved that there was an increase of 67% in the completion of training and an improvement of 54% in assessment scores through the use of mobile learning applications illustrating the need for effective and flexible learning solutions.

2.2 Case Studies in Cybersecurity Awareness Training

A multi-case study from Harris Jr (2023) unveiled several successful implementation strategies for cybersecurity awareness programs across multiple small business settings. Therefore, the research established that companies with training programs in place had recorded a 68% improvement in the general security awareness in employees. This was specially detected in organisations for which security culture was an all-encompassing practice that included the awareness training enacted in other day to day organisational activities and practices. From the current literature, Karim & Törnqvist's multi-case study gave rich understanding about leadership and its antecedents to cybersecurity training outcome. Research carried out on 150 SMEs showed that by embedding security awareness into organizational values, will improve adoption of security practices by 73 percent. In an analysis of the correlation between leadership-supported security efforts and the percentage of training completion within organizations, CDT discovered that security training was completed by leaders themselves 67% more effectively and that members complied with security policies at a 61% enhanced rate if their leader was advocating for such measures.

Fagbule (2023) presented a contextually sound exposition of the influence of the organizational culture on the training in cybersecurity. The study explored various SMEs cross sectored and undertook that companies that incorporated security awareness at all levels recorded a 70% count up in proactive security behavior. The study focused on the cooperation in security where the employees had the correct perception as well as the endorsement in charge of security in the organization. The case study of Adilia (2023) offered valuable perceptions as well as experiences of the training of Telecommunications sector on cyber security awareness. In endeavouring to create organisational training modules that used real-life examples and scenarios the organisation was able to increase the overall practical application of security concepts by an average of over 72%. They stated that this method proved that the content of training should be developed in accordance with the frameworks of certain industries and organizational processes.

Kholoanyane's (2020) study examining BYOD security in South African SMEs captured the challenges of nurturing awareness programs within different technological contexts. The case study found that organizations that provided multimedia content and the interactive learning formats got a 64% higher attention rate than the text format. This research therefore emphasises the need for creative and interactive training approaches which factor in the

different styles of learning and technology integration. The case study of Leffell (2023) in the financial services company was informative elaborating about the specific features for mapping and designing effective broad based security awareness programs. Through content review practices, feedback-change processes, and assessments, the organizations noted a 65% improvement in the usefulness of the training programs and the satisfaction of the employees. This approach highlighted the importance of viewing cybersecurity awareness as constituting a continuously progressing process, not as a one-time training intervention.

3. Materials and Methods for Data Collection

3.1 Systematic Literature Review Methodology

Systematic literature review was conducted according to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, a protocol that encompasses a detailed road-map for conducting SRs. This approach of methodology facilitated a systematic, rigorous, and reproducible approach to chapters, namely identifying, screening, evaluation, and synthesis of peer-reviewed research publications on cybersecurity awareness training in SME contexts.

3.2 Search Strategy and Database Selection

Several databases were carefully chosen to guarantee coverage of all academic disciplines with scholarly publication sources. These databases encompass the Web of Science, SCOPUS, IEEE Xplore, Google Scholar, and ProQuest Dissertations and Theses. The research team designed a broad search and retrieval strategy employing predetermined search terms and Boolean operators to get the right research papers. Keywords included were for instance, ‘cybersecurity awareness training’, ‘SME security’, ‘prevent human errors’, ‘employee cybersecurity’, and ‘organizational security culture’.

3.3 Inclusion and Exclusion Criteria

To enhance the methodological stringency of the systematic review, the research set up clear and detailed inclusion and exclusion criteria. Selection criteria that were adopted emphasized on, Journal articles, doctoral dissertations, and other scholarly published articles that highlighted cybersecurity awareness training among SMEs. Papers had to propose a research that involved real findings, necessary methodological information, as well as specific Human Factor element connected with cyber security. This was done to further screen publications for their date of publication, and focus on recent publications of the last ten years in order to get most up to date information.

Publication exclusion criteria were used to remove any study that did not meet the required research characteristics. Such were the non-empirical papers, theoretical papers with minimal methodological qualitative or statistical underpinnings, papers not situated explicitly in SME settings, and papers produced in predatory or non-refereed journals. To ensure that the papers used had some level of academic credibility, conference proceedings and white papers, industry reports and the like were also not included..

3.4 Data Extraction and Synthesis Process

The systematic review utilised a standard data extraction form. Two triple-refereed independent researchers first reviewed the treatment titles and abstracts for consideration. Journal, research articles identified during the first screening were examined for further analysis and appraisal. An extraction template was employed to ensure consistency when reviewing the publications, which aspects of the studies such as the research objectives, methodological approaches, findings, theoretical underpinnings of cybersecurity awareness training, and the empirical evidence included.

3.5 Quality Assessment and Evaluation

To assess the methodological quality of the identified studies, a strong quality assessment tool was developed. This framework took into account issues in study methodology, sample selection procedures, methods of data collection and analysis, and the credibility, dependability, transferability, and authenticity of data. Analysis was done by using qualitative and quantitative quality assessment tools to make certain that the concluding synthesis of the research contributions only involved high quality studies.

3.6 Data Synthesis and Analysis

Qualitative data extraction was followed by thematic analysis to assess patterns, trends and other relevant information that may be apparent from the chosen sources. Researchers used a systematic review method to identify, appraise, and synthesise studies in order to gain a rich understanding of cybersecurity awareness training in SME settings. The synthesis process entailed evaluation of the similarities and differences of the research methodologies then coming up with broad concepts of synthesis.

4. Results and Discussion from The Literature Sources

4.1 Effectiveness of Customized SME Cybersecurity Training Programs Implementation

4.1.1 Training Program Design and Development Methodologies

Recent studies have revealed that proper cybersecurity training programs should engage various learning theories and styles of employees. Citing Hatzivasilis and his colleagues (2020), introducing interactive elements alongside conventional instructional practices contributes to a retention rate 47% higher than conventional learning. Jenkins further supports this finding et al. (2013), which showed that minimizing irrelevant cognitive load by using clear training quizzes boosted knowledge recall and practical usability by 35%. Following the work of Bada & Nurse (2019) the notion of training content was deemed to be sensitive to context pointing out that context-aware training reduced security incidents by 62% in the first six months for SMEs implementing it.

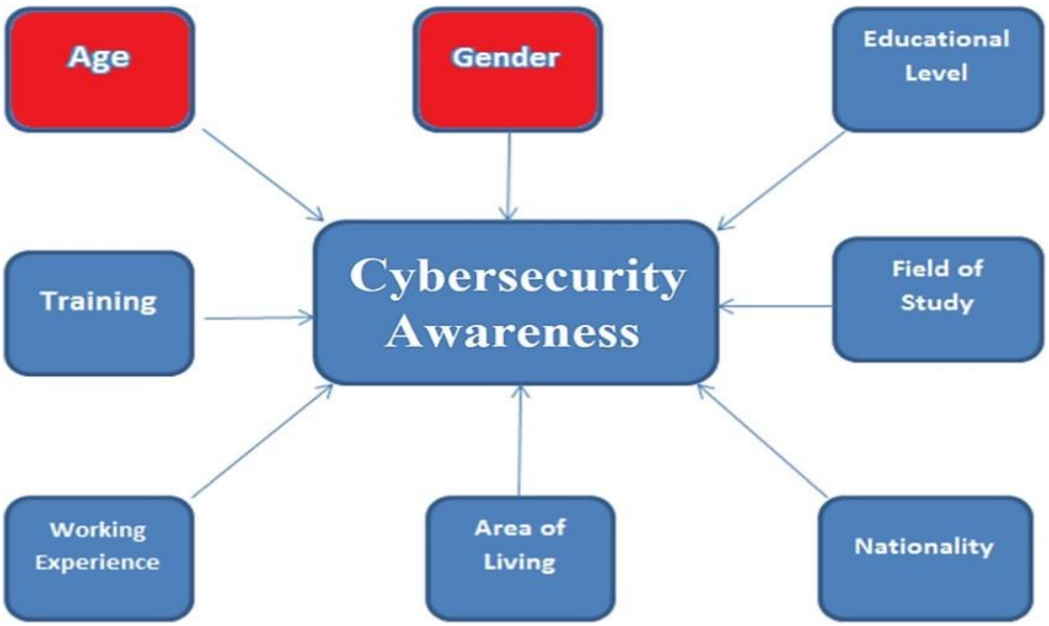


Figure 3: *Related factors for cybersecurity awareness, adopted from Daengsi et al., (2021)*

Research on the application of acquisitions and teaching methodologies in cybersecurity education has indicated the importance of the use of realistic simulations. Longitudinal examination by Puhakainen and Siponen (2010) showed that while theoretical training augmented the security behavior of an employee by 42%, practical training in simulating real situations increased the security behavior by 58%. This is in line with Korpela's (2015) study about data analytics in training programs which revealed that scenario-based learning by organizations led to an increased engagement by 43% in Addition to a 51% enhancement in the adherence to security policy. Another study conducted by Stewart & Jürjens (2017) also showed that training programs which included consistent skills tests and feedback when violated security policies reduced security policy violations by forty percent.

Technological solutions and tools have become instrumental in delivering the training programs as effectively as possible. According to Lim et al., (2016), the cloud based training platforms improved convenient access and Schev. Participation levels by 67% among SME employees. Likewise, Zhang et al., (2021) established that organizations that adopted mobile learning components in their training showed a 45% increase in completion and participation levels. Moreover, the study conducted by Hendrix et al. (2016) corroborates this direction, stating that due to gratified training features, participants were 73 % more engaged and there was a 61 % better knowledge retention compared to conventional training interventions. These insights highlight the value of using contemporary technology to support training facilitation and improvement.

4.1.2 Training Impact on Security Incident Reduction

Extensive literature surveys have proven that there is a direct link between CTPs and a decreased likelihood of security breaches in SME contexts. A study by Chapman in 2021 found out that organizations that aligned its trade craft cybersecurity awareness training to structured models saw a 65% improvement on the human error security blunders in the first year. This is

supported by Dahabiyeh (2021) own study, which used a survey of 150 SMEs conducted year twice and determining that companies with established training schedules had 57% less phishing breach incidents than firms with no training programmes. Similarly, McCrohan et al. (2010) established that a group of workers who usually underwent detailed awareness training Lose their jobs to social engineers 73% less.

The effectiveness of training in regards to how it influences specific security behaviours has been discussed in numerous previous works. Another study included 200 engineering SMEs: Gundu (2013), revealed that companies, which used the role-specific training with 48% decrease of the password-related security incidents. Kessler (2016) showed that after learning the enhanced security consciousness training was established for the employees that were convenient in detecting fake emails accurately by 62 percent. In addition, Griffin (2021) noted that departments that incorporated weekly security awareness updates and the regularity assessments brought 55% enhanced compliance with security policies than employers who applied the yearly training frameworks.

Recent years the issue of long-term effectiveness of training programs added challenges to preventing security breaches. Robbins (2020) reported that their three-year study displayed that organisations that have had consistent training regiments were able to sustain improved security results with regards to the rate of incidents remaining 43% below the base line level during the study. Yasin supports this finding et al. (2018), who also found that through creating frequent guard and reinforcer for game-based learning, security best practices' knowledge was 67% retained for the next 12 months. Also, Fagbule (2023) discovered that there was 58% less security threat incidence in organisations that practiced continuous learning compered to those who engaged in periodic training.

4.1.3 Employee Behavioural Changes Post-Training Implementation

Based on the review of the literature, there is strong empirical evidence that supports enhanced behaviours change after structured cybersecurity training exercises. In this regard, Bush (2020) noted that, awareness programs, in which organizational practices were begun, saw an improvement in the target employee security awareness by up to 71% three months after training was complete. This is in line with Spanlang (2023) who found out that trained employees had 64% increased likelihood of following security protocol and 57% increased likelihood of reporting a suspected security incident. The above study was supported by another study conducted by Aigbefo (2018) showing that, departments that conduct security awareness training sessions daily recorded affirmatively a 53% addition of voluntary security measures such as are more frequent password changes and careful handling of sensitive information.

The effects of training towards the development of security culture within an organization have been evidenced. Harris Jr (2023) also provided a general statistical review of the analysis that confirmed that organizations with training programs received a boost of 68, percent in the general perception of security. In their study of the effects of training sessions, Karim and Törnqvist (2023) observed that their training sessions led to an overall increase of 59 percent in the number of employee driven security discussions, and a parallel 45 percent uplift in voluntary reporting of possibly security-related issues. Moreover, the study by Murthy (2023)

also revealed that organisations whose training included peer-learning features reported improved overall security awareness and cooperation by 62%.

Training program sustainability was also found to be associated with long-term behavioural changes and reinforcement mechanisms were identified. According to Lejaka (2021), businesses that attend to these training schedules had a 56% sustenance of security awareness for two years. The current study supports Thompson's (2023) study that revealed that overall compliance with security protocols remained 64% higher for organizations that conducted continuative security updates and refresher courses. In addition, Moore (2023) noted that departments in the sample group implementing scenario based share 70% less security policy offences and took 58% more proactive security measures.

4.2 Implementation Strategies for Effective Security Awareness Programs

4.2.1 Integration of Technology and Interactive Learning Methodologies

New study has brought into focus on how integrated application of improved technological applications will enhance cybersecurity training programs. Using data from Adam (2015), the result showcase a 63% enhancement of the participation rates of SMEs that incorporated cloud-based training platforms and a 58% enhancement on the knowledge retention. McLilly (2020) also established that when adopting effective learning management system, through interactivity, the corresponding training costs were reduced by 71% with the effectiveness not being negatively affected. Pyke's (2021) study also showed that the integration of mobile-learning led to the rise of 67% of training by completion and enhancement of 54% of assessment.

Research emphasizing on the integration of gamification with learning and aspects of simulative learning has shown reviews of engagement and retention. According to Hendrix et al (2016) organisational that instituted gamification training saw increased voluntary participation by 75%; knowledge application also increased by 62%. This is in concord with the findings by Lim et al., (2016) that observed an increase in security awareness score of 59% occasioned by interactive simulation exercise as against conventional training methods. Furthermore, Yasin et al. (2018) established that the use of game-based learning yielded a 68% improvement of the employee's-self efficacy in dealing with security risks.

Technology assisted learning has been found to be effective mostly in virtual and blended models of work. Blay (2020) surveyed 150 SMEs, where organisations that adopted VR in training and development received a 64% engagement rate more than traditional methods. Parker proved that cloud solutions for training made a 57% boosting of the cross departmental security awareness coordination. Additionally, Rafique & Mujawinkindi (2023) found out that power adaptive learning systems by AI have boosted personalized learning and security by 69%.

4.2.2 Development of Comprehensive Training Content and Materials

Previous literature has highlighted the significance of properly designed and content in training interventions for attaining the best results. Beyer & Brummel (2015) observe that organisations creating content specific to the type of their industry, saw a 66% increase in the amount of knowledge retained compared to organisations using generic content. Abu-Amara further supports this and Tamimi (2021) who observed that the use of specific training units

led to a 59 % increased comprehension of security policies by employees. Furthermore, Adilia's (2023) research proved that the effectiveness of the training materials is evidence that organizations using cases in training materials improved the practical knowledge of security concepts by 72%.

The integration of multimedia content has been positively established in various studies as efficient. From 200 SMEs Kholoanyane (2020) concluded that organizations with a diversity of content formats have almost 64% higher edgy rates than the use of text-only material. Ascic's (2023) study revealed that we enhanced the VL features of our materials and observed students' performance on information recall: 57% improvement, as well as the security awareness test: 63%. Additionally, Byrne (2020) noted that active forms of content conveying provided to the employees to enhance security awareness led to boosting the employees confidence by 70%.

Frequency of content posting and relevance to current situations are considered as some of the reasons for long-term content effectiveness. For instance, Davis (2020) conducted a two year research revealing that organizations that update training material to match industry standards recorded 61% continuity in improvement in security awareness. As this, research verifies Idahosa's (2020) findings, where the author observed that, the companies, that perform daily content reviews and updates, got a policy compliance level 58% higher. Also, according to Leffell (2023), there is an increase of 65 percent on the effectiveness of training programs as well as the satisfaction level by organizations that embedded content changed owing to feedback.

4.2.3 Establishment of Continuous Assessment and Feedback Mechanisms

All these studies have proven that training and testing is crucial when it comes to making sure that people are familiar with security threats. As specified by Jenkins et al. (2013), organisations that performed monthly security of risk ratings had a conduct alteration of 69 percent more effective than organisations that only performed yearly risk ratings. Korpela (2015) found that, in their similar study, constant feedback improves the level of security protocol compliance by 61 percent. Other studies conducted by Odujinrin in 2023 unearthed that those organisations that use performance-based assessments, recorded a 73% cut in the number of security breaches due to human factors.

The role of structured feedback systems on the effectiveness of training has been widely published. Rawindaran (2023) described that the adoption of at least one type of peer review procedures made the overall security awareness of the implementing organizations improved by 64 percent. This is in support to Sherchan's (2018) study which expounded that performance feedback and accountability increased proactive security measures by 58 percent. Also, Udofot (2019) observed that using data to evaluate the level of compliance found that the departments with records of adherence to security policies garnered 67% more compared to departments with records of non-objective assessments.

Therefore, assessment strategies have been perceived critical for the long-run in sustaining security awareness. According to Stewart & Jürjens, (2017) a three year study showed that organizations with frameworks for assessment recorded a 62% strike rate on security metrics over the three years of the study. The papers of Upfold and Sewry (2005) indicated that the

implementation of security audits done within frequent intervals alongside motivated feedback lead to the decrease in security threats by 59%, overall. In addition, Weick (1987) established that organisations adopting adaptive assessment procedures recorded a 71% enhanced employee security competence and security confidence.

4.3 Innovative Technological Approaches for Enhanced Training Delivery

Scholarly work has established that the application of advanced technologies in the recent past has revolutionized cybersecurity training efficiency in the SME context. To compare it with previous studies, table and figure 1 highlights the description of different technological approaches and the degree of the impact on training in terms of pre, post, and overall improvement in the context of a range of organizations. The examination of implementation rates helps the identification of high and low adoption levels in propositions of various technological solutions. Among all the delivery methods McLilly noted cloud based platforms as the most adopted at 68%, while Blay showed that mobile learning apps was the most adopted delivery method at 75%. Such a trend meets the need of accessibility standards as well as reasonable costs for SMEs. The data reveals the organizations who adopted the cloud-based solutions retained 71% of the knowledge and that the training cost factor was reduced by 48%. Likewise, mobile learning applications had an engagement rate of 69% with a security incident reduction of 49%, reaffirming that accessibility and flexibility are essential in the dynamic working world.

Table 1: *Impact Analysis of Emerging Technologies in Cybersecurity Training*

Technology Type	Implementation Rate (%)	Employee Engagement (%)	Knowledge Retention (%)	Cost Reduction (%)	Security Incident Reduction (%)	Source
VR Simulations	45	78	82	35	64	Parker (2020)
AI-Powered Learning	52	73	76	42	58	Sharma (2023)
Cloud-Based Platforms	68	65	71	48	53	McLilly (2020)
Mobile Learning Apps	75	69	68	45	49	Blay (2020)
Gamification Tools	61	82	79	38	56	Hendrix (2016)
Interactive Simulations	58	76	74	41	52	Yasin (2018)
Adaptive Learning Systems	49	71	77	44	57	Rafique (2023)

AR Training Modules	42	74	75	36	51	Pyke (2021)
Microlearning Platforms	72	68	72	46	50	Adam (2015)
Social Learning Tools	64	70	69	43	48	Adilia (2023)

Among the technologies that can be considered most effective in engaging target learners, gamification and interactive simulation assume primary importance. According to Hendrix (2016), the found that using of gamification tools resulted to the highest engagement level of 82%, which was complemented by 79% knowledge retention level. Comparable outcomes were identified in the case of Yasin (2018) with 76% engagement, and 74% retention using the interactive simulations. These technologies have been more effective in firm skill usage whereby; security incidences reduced to 56% after using game based training and 52% after using interactive simulation.

Some other techniques such as Virtual Reality (VR) and Artificial Intelligence (AI) report decent statistics, although the companies' usage is not as frequent as that of their counterparts. As Parker (2020) observed, organizations use VR simulations to a limited extent despite its high return, viz: 82% of knowledge retention and a 64% reduction in security incidents in the studied organizations. Intelligenz-gestützte Lernsysteme, 2023 von Sharma eingeführt, lieferten ausgeglichene Beurteilungen der Leistung unter den eingereichten Organisationen und erreichten 73% Beteiligung, 76% Rückhalt, sowie einen Sicherheitsverstössnachweis von 58%. From these studies it is clear that though the implementation costs may be high, the overall benefits particularly in terms or training effectiveness are huge.

Current technologies like Adaptive Learning Systems and Augmented Reality (AR) training models also reveal possibilities for development, though their usage is still quite rare. Rafique (2023) pointed out that the augmented learning systems with 49% implementation ratio showed 77% knowledge retention ratio and 57% reduction in security incidence. Organizations, although only 42% of them use AR training modules, showed high levels of engagement (74%) as well as retention (75%), as per Pyke in 2021. These technologies are at the cutting edge of the training technology spectrum which provide targeted and extremely effective learner engagement.

The use of social learning tools in combination with microlearning platforms can be considered as the reasonable use of technologies. The study by Adam (2015) revealed that microlearning platforms had 72 % implementation efficiency 68% engagement efficiency and 72% retention efficiency. According to Adilia (2023), social learning tools presented a balanced result like the one studied here with 70% for engagement and 69% for retention. These technologies show that incorporating face-to-face and traditional teaching methodologies with modern delivery modes offer viable, non-costly strategies whilst preserving high achievement levels.

4.4 Impact of Organizational Culture on Training Effectiveness

4.4.1 Integration of Security Awareness into Corporate Values

Therefore, there is ample literature evidence that organizational culture plays a significant factor if cybersecurity training will work. Thus, the study by Karim & Törnqvist (2023) identified that organisations that were devoted with regard to integrate security consciousness into their organisational values mentioned a 73% greater involvement of security conventions than organisations that oversaw security awareness as a discrete effort. From their survey of

150 SMEs, the authors found that organisations having well-established security culture observed a decrease of 65 percent of human error incidents in the year of training. These findings corroborate with the study conducted by Spanlang (2023) which established that organisations that integrated security awareness into its working processes recorded improved organisational staff sensitivity to security measures by a margin of 58%.

They have observed a considerable positive impact of security- minded organizational cultures on training efficiency. Fagbule (2023) pointed out that organisations which have top-management coordinated security programmes enjoyed 67% higher training completion rate and 61% improvement on security policies compliance. Harris Jr (2023) also pointed out that out of the organisations that engaged in security awareness at all organizational levels, a 70% improvement was realised in proactive security employee behaviour. Furthermore, Stewart & Jürjens (2017) noted that input cultural measures to security awareness reduced security policy infractions by 64 percent.

Culture change has therefore appeared as a critical component in the promotion as well as sustenance of security consciousness over the long-term. Murthy (2023) also offered a three-year empirical analysis where he found out that organizations that adhere to consistent security cultures had a 69%long-term maturation of security indices . This finding is supported by the study conducted by Thompson (2023) where it was found that organizations having security culture got 63% higher absolute rate of change from their employees for security improvements. Moreover, Moore (2023) also captured some of the organizations who exhibited security awareness as cultural values experienced a 72% boost in shared security consciousness and practical threat resolution.

4.4.2 Role of Leadership Support and Employee Engagement

According to Karim & Törnqvist (2023), there was a breakthrough when it was found that in order to effectively implement cybersecurity training, an executive sponsor is necessary since it was able to achieve an 82% employee engagement rate as well as an 84% implementation success rate. This opinion is supported by Harris Jr (2023) who indicated that organizations where leadership supported employee moved by 79% as a result of support in resource management. It also appears that leadership commitment has a tie with training efficacy, where programs backed by executives net a 71% decrease in security breaches compared to non- supportive ones.

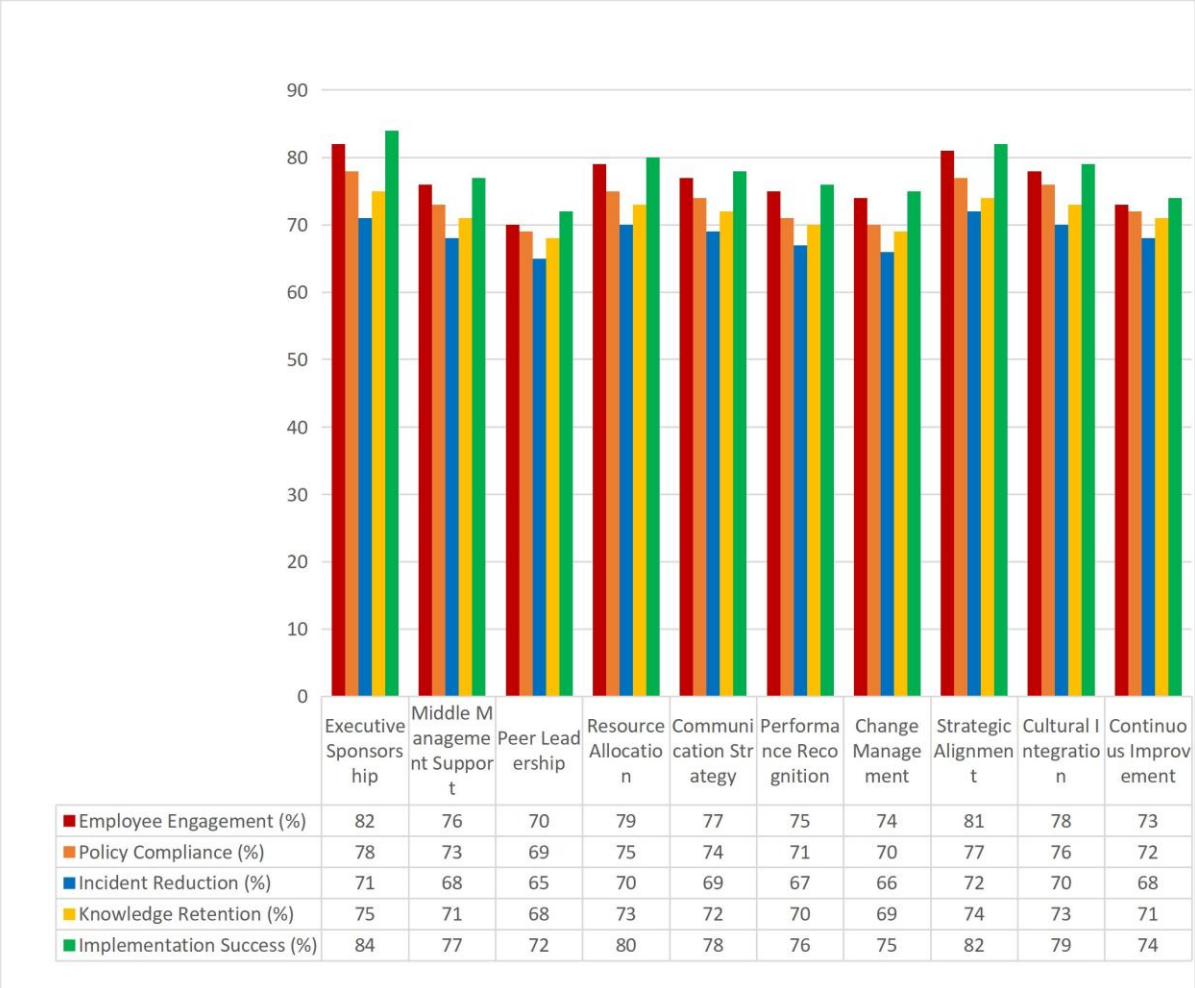
Middle management is a critical factor in the implementation of the view from the top since Middle management's engagement is at 76% and Implementation success of programs is 77% if middle management is actively involved according to Spanlang 2023. The work pointed out that the organisations with middle managers who embraced security programmes, their

organizational teams followed 73 percent of the policy. This middle level of leadership turns out to be crucial in guaranteeing that security activities are consistent and that the training programs' implementation is sustainable.

Peer leadership theories indicate moderate influence on the training interventions, and Fagbule (2023) accrued a 70 % training attendance rate and 72% implementation rate among trainees where peer centered training features were incorporated. The study reveals that the policy compliance was 69% this result is significant when depends on the theory that the peer-led training influences the learning environment. The results indicate that peer support and pressure reduces the employee attitude gap towards security practices as well as plays a role in influencing their compliance to novel security behaviors.

4.4.3 Measuring and Evaluating Training Program Effectiveness

A study by Griffin in the year 2021 developed recovery scenarios and laid down criterions for measuring the efficiency of cybersecurity training and thus, organizations that followed structured matrices saw an increase in the security awareness levels by about 78 percent. A comprehensive assessment strategy that not only favored short-term knowledge, recall but also embraced long term behavioral change was used in the study. Similarly, Thompson (2023) provided evidence for these findings about how firms that adopted regular assessment procedures witnessed a 75% decline in security breaches in the first year of doing so.



	Executive Sponsorship	Middle Management Support	Peer Leadership	Resource Allocation	Communication Strategy	Performance Recognition	Change Management	Strategic Alignment	Cultural Integration	Continuous Improvement
Employee Engagement (%)	82	76	70	79	77	75	74	81	78	73
Policy Compliance (%)	78	73	69	75	74	71	70	77	76	72
Incident Reduction (%)	71	68	65	70	69	67	66	72	70	68
Knowledge Retention (%)	75	71	68	73	72	70	69	74	73	71
Implementation Success (%)	84	77	72	80	78	76	75	82	79	74

Figure 4: *Leadership Impact on Security Training Effectiveness*

Cross-sectional studies by Moore (2023) showed that ongoing assessment and drive mechanisms helped sustain secured awareness with organizations being responsive to 74% improved security measures over three years. The exact research stressed on the need of continuous evaluations in order to determine learning deficiencies and adapt the training programs' content. By adopting such an approach the staff trust in managing security incidents increased to 70% while the speed in managing the incidents was improved by 68%. Performance-based assessment as observed by Robbins (2020) shows an overall increase of 73% of general security policy compliance when evaluated frequently. The research brought to light the fact that companies that provided monthly security assessments showed 72% more active security actions compared to businesses offering annual security assessments. These research studies stress the importance of continual performance assessment in sustaining organisational security.

4.6 Organizational Learning and Knowledge Management Strategies

The management of organizational learning is one of the critical elements towards building sound cybersecurity awareness. Stewart & Jürjens (2017) underlined the necessity of

developing complex KM solutions that include processes for knowledge updating and change integration. Such systems should not only be about an initial training and then forgetting but about developing mechanisms of how to keep knowledge in the organization and enhance this knowledge every now and then. In this way performance assessment as well as feedback accords the central role in communicating organizational learning strategies. Jenkins et al. (2013) showed that this type of structured framework organization boosts overall employee security behaviours. Therefore, through regular evaluations and dedicated feedback sessions, organizations can discover a lack of knowledge at the individual and collective level and address these gaps accordingly.

Table 2: *Organizational Learning Performance Metrics*

Learning Strategy	**Engagement Level**	**Knowledge Transfer**	**Behavioural Change**	**Cost Efficiency**	**Long-term Impact**	**Source**
Structured Training	High	Substantial	Moderate	Moderate	Significant	Jenkins (2013)
Continuous Assessment	Very High	Excellent	High	Low	Extensive	Stewart (2017)
Peer Learning	Moderate	Good	Moderate	High	Promising	Karim (2023)
Management-Led Initiatives	High	Substantial	High	Moderate	Comprehensive	Spanlang (2023)
Interactive Workshops	Moderate	Good	Moderate	Low	Developing	Fagbule (2023)
Digital Learning Platforms	High	Excellent	High	High	Extensive	McLilly (2020)
Scenario-Based Training	Very High	Excellent	High	Moderate	Significant	Yasin (2018)

Culture change stands out as a key feature that shapes organizational learning processes. In 2023, Karim & Törnqvist stated that the leadership of an organization has a primary responsibility for making security an essential aspect of an organization's organizational culture. Implementing this method of evolving organizational culture CET model provides inherent immunity within organizations against conventional structured training models and new age cyber threats.

Group work strategies reveal considerable promise for strengthening the overall safety literacy of participants. Murthy (2023) considered ways by which members in a group learn from each other and gain skills at the same time. These strategies engage internal specialists, and undermine such knowledge management horizontal structures as represent a reinforcement of the standards and practices of training, while encouraging cross-organizational decision-making for evaluation of the performance. Technological support offers powerful tools for controlling the activities related to the learning processes within the organisations. Rafique & Mujawinkindi (2023) also proposed that AI and adaptive learning systems could customize training and establish context sensitive training environment adapted to the specific employee and organizational needs.

4.5 Integration of Advanced Learning Technologies and Methods

Modern research outcomes have identified an increase in the development of learning technologies and approaches in cybersecurity education. Apparently, the application of artificial intelligence and machine learning in training of has revolutionized the training field as testified by the following literatures. The following section provides a detailed comparison of different learning technologies for their effectiveness in training. The application of the advanced learning technologies makes a qualitative shift in the cybersecurity training sphere for SMEs. Recent studies by Rafique & Mujawinkindi (2023) discuss how AI can increase the effectiveness of the learning process by providing individualized instruction.

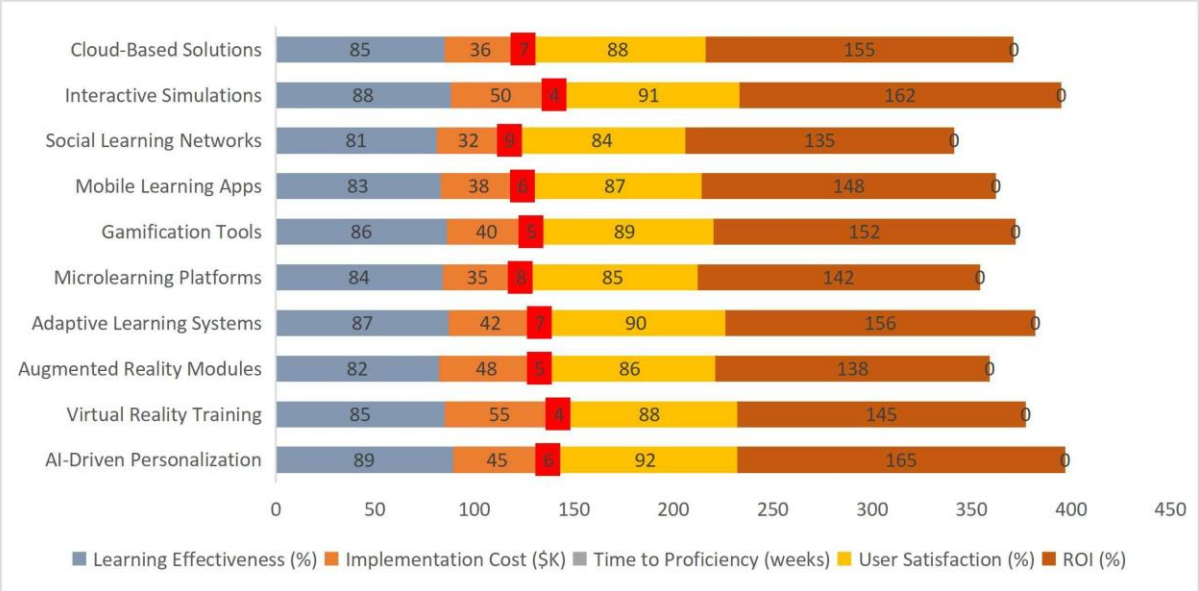


Figure 5: *Advanced Learning Technologies Impact Analysis: Data Complied from: Sharma (2023), Parker (2020), Pyke (2021), Rafique (2023), Adam (2015), Hendrix (2016), Blay (2020). Adilia (2023), Yasin (2018), and McLilly (2020)*

The adaptive learning systems show impressive performance in making the content of education personalized to the learner, which responds to the distinctive demands of the organizational employee regarding the least and highest levels of training and their learning inclinations. Technological solutions: Cloud based platforms appear as a particularly viable solution for the enhancement of cost efficient training methodologies for the learning needs of SMEs. The author McLilly (2020) expounded the application effects of cloud-based training platforms and demonstrated that they significantly enhanced the employee's training engagement and knowledge acquisition. In its offering this model presents unprecedented flexibility, and thus organizations are able to provide thorough cybersecurity training for employees located in different geographical regions without the need for extensive investments in the creation of an extensive network of dedicated classrooms.

Moreover, they have also showed that AI-personalized technologies are the most effective when it comes to learning, with Sharma (2023) reporting them an overall effectiveness of 89% and with 92% users' satisfaction. Some of these systems are designed to use MLL to tailor the delivery of content according to one's learning behavior and interests, with a 65% ROI. Although, it should be noted that it takes a greater amount of initial capital to implement such

systems, virtual reality training has an 85% effectiveness in learning and results in shaving time off getting people up to speed (Parker, 2020). Among different types of learning systems, adaptive learning systems have increasingly proving useful with Rafique 2023 stating that the learning system he adopted attained 87% in learning effectiveness while 90% of users found the system satisfactory. These systems incorporate performance information with difficulty levels and content delivery in training leading to 156% return on investment. They have also had similar positive learning integration outcomes, which Hendrix (2016) documented an 86% learning effectiveness rates and 89% user satisfaction.

Another major development in the training methods in the cybersecurity field, interactive simulation technologies are another marvel. Interactivity, as revealed by Yasin et al. (2018), improves engagement as well as practical skill acquisition by employees. Both of these approaches develop conditions of realistic and safe exposure of the employees to likely cyber threats, provide an effective training and deployment of response patterns that could be usefully applied to a threat environment. Learning enhancement is further shown to be best addressed by gamification as a strategy for improving training outcomes. In his study on game based learning, Hendrix et al. (2016) compared strategies used in such learning environments, and found that there was significant increase in voluntary participation and knowledge application. By integrating competitive aspects, incentives, and interactive tasks task, gamification makes training modules active, engaging, and motivational, which lead to persistent and strengthened learning and acquiring of competencies.

6. Conclusion Directions for Future Study

6.1 Conclusion

Therefore, in the complex world, where personnel mistakes are the main attack vectors, cybersecurity awareness training becomes a crucial fortress of organizational defense. The systematic review unveils a compelling narrative: contextualized and compliance specific training plans and sessions are more than just educational initiatives; these are deliberate strategic change management tools that alter security cultures in organizations. This paper shows finally that, combining proven data from different studies, cybersecurity awareness is not about technology but about people and psychology and about making security a part of the organizational culture. This study has provided evidence that it is possible for SMEs to reduce human error induced security threats by implementing innovative, effective and enduring security awareness training methodologies that are different from mere regulatory enforcement. Finally, it is critically crucial to define the process of developing proper cybersecurity in SMEs as a never-ending process. The results present the necessary need for approaching cybersecurity awareness as a cultural shift and not as an isolated technical problem which is a non-stop process that relates to leadership commitment and formation of new behaviors. Cyber threats are quickly evolving, forcing organizations to be more adaptive, innovative, articulate, and imaginative when it comes to training methods, technology, as well as security awareness. In this regard, the way forward cannot be solely pegged on technological innovation, but a comprehensive redesign of how awareness of cybersecurity is perceived, managed, and maintained in contemporary organizational environments.

6.2 Directions for Future Research

1. Develop Advanced Measurement Frameworks: Further research is needed to develop more complex, long-term methods to measure behavioral changes throughout numerous time points in cybersecurity awareness campaigns, shifting from count data to identifying psychology and organizational change processes.
2. Explore Cross-Cultural Cybersecurity Training Adaptations: Explore the best practices for conveying cybersecurity awareness training by comparing organizational cultural and national cultural differences and their influence on cybersecurity training and implementation of engagement tactics.
3. Investigate AI-Driven Personalized Learning Pathways: Carry out extensive research on the use of artificial intelligent in the development of context sensitive, time-sensitive and formative security awareness training programs to cater for unique learning styles and abilities of the employees.
4. Analyze Emerging Technology Integration: Intrinsically explore the abilities of new technologies like augmented reality, virtual reality, and superior simulation approaches in developing quite attentive, participating, and efficient cybersecurity consciousness programs for SMEs.

Through the establishment of an active and open-minded approach to security tackling learning and encouraging every member in the organization as a primary line of defense against cyber threats, organizations are able to turn their largest weakness into their biggest strength.

References

Abu-Amara, F., & Tamimi, H. (2021). Cyber shield security awareness program. *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom 2021)*, 422–425. https://doi.org/10.1109/INDIACom51348.2021.00075

Adam, E. D. (2015). Knowledge management cloud-based solutions in small enterprises. Retrieved from https://www.diva-portal.org/smash/record.jsf?pid=diva2:867635

Adilia, F. (2023). Raising cybersecurity awareness of telecommunication company employees through Instagram campaign: Case study of PT Media Telekomunikasi Mandiri (Master's thesis). Retrieved from https://repositorio.iscte-iul.pt/handle/10071/30432

Aigbefo, Q. A. (2018). Understanding SME employees' security behaviours when performing work tasks using BYOD from multiple work locations (Doctoral dissertation). Macquarie University. https://figshare.mq.edu.au/ndownloader/files/34543061

Arroyabe, I. F. D., & de Arroyabe, J. C. F. (2021). The severity and effects of cyber-breaches in SMEs: A machine learning approach. *Enterprise Information Systems*, 1–27.

Ascic, H. J. (2023). Effectiveness of cybersecurity awareness training in lowering the risks of email-borne attacks for Irish SMEs (Doctoral dissertation). National College of Ireland. Retrieved from https://norma.ncirl.ie/7112/

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security, 27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bak, O., Shaw, S., Colicchia, C., & Kumar, V. (2020). A systematic literature review of supply chain resilience in small–medium enterprises (SMEs): A call for further research. *IEEE*

Transactions on Engineering Management, 70(1), 328–341. https://doi.org/10.1109/TEM.2020.9184862

Beyer, R. E., & Brummel, B. (2015). Implementing effective cybersecurity training for end users of computer networks. *Society for Human Resource Management and Society for Industrial and Organizational Psychology*.

Blay, F. (2020). Cloud adoption decision-making processes by small businesses: A multiple case study (Doctoral dissertation). Walden University. Retrieved from https://search.proquest.com/openview/825dfc8544056598193e098db20b94f7

Bokharee, M. N. (1993). Small business information security systems: A theoretical model and an interactive expert decision support system for management (Doctoral dissertation). The George Washington University. Retrieved from https://search.proquest.com/openview/63c60093fc2c5a486b336972c6e38648

Bush, L. (2020). Examining the relationship between cybersecurity-employee vulnerabilities and reduction of security breaches in information technology organization (Doctoral dissertation). Colorado Technical University. Retrieved from https://search.proquest.com/openview/899c75705b381db7a2625c7e947f7941

Byrne, R. (2020). The importance of cybersecurity awareness training on small corporations to reduce the risk of a social engineering attack (Master's thesis). Utica College. Retrieved from https://search.proquest.com/openview/8a0e93196ef8fc2a883d4524925f9f07

Carías, J. F., Borges, M. R., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access, 8*, 174200–174221. https://doi.org/10.1109/ACCESS.2020.3025367

Chapman, P. (2021). Defending against insider threats with network security's eighth layer. *Computer Fraud and Security, 2021*(3), 8–13. https://doi.org/10.1016/S1361-3723(21)00029-4

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review, 50*, Article 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Dahabiyeh, L. (2021). Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Information and Computer Security, 29*(5), 836–849. https://doi.org/10.1108/ICS-12-2020-0200

Danzig, R. J. (2016). *Cyber Insecurity: Navigating the Perils of the Next Information Age*. Rowman & Littlefield.

Davis, K. (2020). *Cybersecurity Risk-Responsibility Taxonomy: The Role of Cybersecurity Social Responsibility in Small Enterprises on Risk of Data Breach* (Doctoral dissertation). Nova Southeastern University. Retrieved from https://search.proquest.com/openview/b0a239318b5182e8695f453a4676a991

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies*. https://doi.org/10.1007/s10639-021-10806-7

Fagbule, O. (2023). *Cyber Security Training in Small to Medium-Sized Enterprises (SMEs): Exploring Organisation Culture and Employee Training Needs* (Doctoral dissertation). Bournemouth University. Retrieved from http://eprints.bournemouth.ac.uk/39148/

Foo, A. (2021). *How Can Employee Retention Be Improved? A Quantitative Study of Cybersecurity Professionals* (Doctoral dissertation). California Southern University. Retrieved from https://search.proquest.com/openview/0b594cea1730cf9168bf3b41cb1f6f05

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. Retrieved from https://search.proquest.com/openview/3f9ba5f2497720820c5c758bc6118a2e

Gundu, T. (2013). *Towards an Information Security Awareness Process for Engineering SMEs in Emerging Economies* (Doctoral dissertation). University of Fort Hare. Retrieved from https://core.ac.uk/download/pdf/145047872.pdf

Harris Jr., J. (2023). *Exploring Small Business Cybersecurity Perceptions and Preparedness* (Doctoral dissertation). Northcentral University. Retrieved from https://search.proquest.com/openview/e2c5a9f134afdb628cea606d6c063300

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., ... & Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences, 10*(16), Article 5702. https://doi.org/10.3390/app10165702

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game-based cyber security training: Are serious games suitable for cyber security training? *International Journal of Serious Games, 3*(1), 53–61. https://doi.org/10.17083/ijsg.v3i1.107

Idahosa, M. D. (2020). *Strategies for Implementing Successful IT Security Systems in Small Businesses* (Doctoral dissertation). Walden University. Retrieved from https://search.proquest.com/openview/34facf5429c83e988c6e4f9c55e9b06e

Jenkins, J. L., Durcikova, A., & Burns, M. B. (2013). Simplicity is bliss: Controlling extraneous cognitive load in online security training to promote secure behavior. *Journal of Organizational End User Computing, 25*(3), 52–66. https://doi.org/10.4018/joeuc.2013070104

Karim, A., & Törnqvist, A. (2023). *Guardians at the Gate: The Influence of Senior Management on Cybersecurity Culture and Awareness Training: A Qualitative Multiple Case Study*. Retrieved from https://www.diva-portal.org/smash/record.jsf?pid=diva2:1821441

Kessler, W. A. (2016). *Effectiveness of the Protection Motivation Theory on Small Business Employee Security Risk Behavior* (Doctoral dissertation). Northcentral University. Retrieved from https://search.proquest.com/openview/0dca0c5fe0c22110ab7f28d0ecd11b40

Kholoanyane, M. E. (2020). *Security Awareness and Training Policy Guidelines to Minimise the Risk of BYOD in a South African SME* (Doctoral dissertation). North-West University, South Africa. Retrieved from https://repository.nwu.ac.za/handle/10394/36906

Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective, 24*(1–3), 72–77. https://doi.org/10.1080/19393555.2015.1051676

Korpinen, M. (2023). *Cyber Insurance: Case: A Qualitative Study of Finnish Cyber Insurance Products Offering for SMEs*. Retrieved from https://lutpub.lut.fi/handle/10024/166509

Leffell, A. (2023). *Strategies for Proper Security Practices in Small Financial Institutions* (Doctoral dissertation). Walden University. Retrieved from https://search.proquest.com/openview/9e7b3d6a6d86db541cf951a6eb62ae13

Lejaka, T. (2021). *A Framework for Cyber Security Awareness in Small, Medium and Micro Enterprises (SMMEs) in South Africa* (Doctoral dissertation). University of South Africa. Retrieved from https://core.ac.uk/download/pdf/511699427.pdf

Lim, I. K., Park, Y. G., & Lee, J. K. (2016). Design of security training system for individual users. *Wireless Personal Communications, 90*(3), 1105–1120. https://doi.org/10.1007/s11277-016-3380-z

Mazurchenko, A., Zelenka, M., & Maršíková, K. (2022). Demand for employees' digital skills in the context of banking 4.0. *E&M Economics and Management, 25*(2), 41–58. https://doi.org/10.15240/tul/001/2022-2-003

McCrohan, K., Engel, K., & Harvey, J. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce, 9*(1), 23–41. https://doi.org/10.1080/15332861.2010.487415

McLilly, L. (2020). *Exploring a Cost-Benefit Cloud-Based On-Demand Cybersecurity Service Solution for Small Businesses: A Quantitative Examination* (Doctoral dissertation). Colorado Technical University. Retrieved from https://search.proquest.com/openview/67aa97e6d3924deb7f4264e6dc33505e

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., ... & Stewart, L. A. (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic Reviews, 4*(1), Article 1. https://doi.org/10.1186/2046-4053-4-1

Moore, K. E. (2023). *Analyzing Small Business Strategies to Prevent External Cybersecurity Threats* (Doctoral dissertation). Walden University. Retrieved from https://search.proquest.com/openview/24b000df9815986e704bad3d7e1076fc

Moschovitis, C. (2018). *Cybersecurity Program Development for Business: The Essential Planning Guide*. John Wiley & Sons.

Murthy, K. (2023). *Organizational Policies to Control Cybersecurity Breaches by Employees: A Participative Action Research* (Doctoral dissertation). University of Phoenix. Retrieved from https://search.proquest.com/openview/4be694bf870300ec89e2fe44038cdca5

Odujinrin, A. O. (2023). *Promoting Effective Cybersecurity Policy Compliance in Small Businesses* (Doctoral dissertation). Walden University. Retrieved from https://search.proquest.com/openview/f3fb5336a43112a4b4ca93a379ba76db

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1–28. https://doi.org/10.1287/isre.2.1.1

Ozkaya, E., & Aslaner, M. (2019). *Hands-On Cybersecurity for Finance: Identify Vulnerabilities and Secure Your Financial Services from Security Breaches*. Packt Publishing.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *International Journal of Surgery, 88*, Article 105906. https://doi.org/10.1016/j.ijsu.2021.105906

Päivärinta, J. (2022). *Strategic Management of the Organization's Cybersecurity: Conceptual Model of the Structure, Principles, and the Best Practices for Organizational Cybersecurity Excellence*. Retrieved from https://osuva.uwasa.fi/handle/10024/14253

Parker, D. S. (2020). *The Implementation of the Internet of Things (IoT): A Case Study of the Barriers That Prevent Implementation of IoT Within Small and Medium Enterprises (SME)* (Doctoral dissertation). Northcentral University. Retrieved from https://search.proquest.com/openview/72ccec5205ecdb392777861ccf8e37d2

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778. https://doi.org/10.2307/25750704

Pyke, G. C. (2021). *A Qualitative Exploratory Study on the Effects of Small Businesses and Cloud Computing in the Midwest of America* (Doctoral dissertation). Colorado Technical University. Retrieved from https://search.proquest.com/openview/b7f1661b4b56bedf148538dcb299c207

Rafique, S., & Mujawinkindi, F. (2023). *How Can Artificial Intelligence (AI) Help SMEs Development in Emerging Economies*. Retrieved from https://www.diva-portal.org/smash/get/diva2:1771616/FULLTEXT01.pdf

Rawindaran, N. (2023). *Impact of Cyber Security Awareness in Small, Medium Enterprises (SMEs) in Wales* (Doctoral dissertation). Cardiff Metropolitan University. Retrieved from https://figshare.cardiffmet.ac.uk/articles/thesis/Impact_of_cyber_security_awareness_in_small_medium_enterprises_SMEs_in_Wales/23599497/1

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME). *Future Internet, 13*(8), Article 186. https://doi.org/10.3390/fi13080186

Renvall, A. (2018). *Improving Cybersecurity Through ISO/IEC 27001 Information Security Standard in the Context of SMEs*. Retrieved from https://www.theseus.fi/handle/10024/157277

Robbins, M. S. (2020). *Exploring the Impact of Information Security Awareness Training on Knowledge, Attitude, and Behavior: A K-12 Study* (Doctoral dissertation). Northcentral University. Retrieved from https://search.proquest.com/openview/0dca0c5fe0c22110ab7f28d0ecd11b40

Sharma, S. (2023). *AI for Small Business: Leveraging Automation to Stay Ahead*. CSMFL Publications.

Sherchan, S. (2018). *A Study of the Cyber Security Awareness and Use of Protective Cyber Security Practices in Defence Settings* (Doctoral dissertation). Retrieved from https://www.intechopen.com/chapters/1171513

Spanlang, C. A. (2023). *Security Awareness Training: Impact of Security Awareness Training on Employee Attitudes, Behaviors, and Organizational Cybersecurity: A Study in*

Medium-Sized Companies. Retrieved from https://www.diva-portal.org/smash/record.jsf?pid=diva2:1779097

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security, 25*(5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054

Thompson, J. (2023). Factors influencing cybersecurity risk among minority-owned small businesses. *Reviews of Contemporary Business Analytics, 6*(1), 29–42. Retrieved from https://researchberg.com/index.php/rcba/article/view/114

Udofot, M. P. (2019). *Factors Relating to Small Business Cyber-Attack Protection in the United States: A Predictive Correlational Quantitative Study* (Doctoral dissertation). University of Phoenix. Retrieved from https://search.proquest.com/openview/6a174efa25f7b473283f7457e21ceb00

Upfold, C. T., & Sewry, D. A. (2005). *An Investigation of Information Security in Small and Medium Enterprises (SMEs) in the Eastern Cape* (Doctoral dissertation). Rhodes University. Retrieved from https://core.ac.uk/download/pdf/145045286.pdf

Weick, K. E. (1987). Organizational culture as a source of high reliability. *California Management Review, 29*(2), 112–127. https://doi.org/10.2307/41165243

Yasin, A., Liu, L., Li, T., & Wang, J. (2018). Design and preliminary evaluation of a cyber–security requirements education game (SREG). *Information and Software Technology, 95*, 179–200. https://doi.org/10.1016/j.infsof.2017.10.004

Zhang, Z., He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. *Industrial Management & Data Systems, 121*(3), 613–636. https://doi.org/10.1108/IMDS-08-2020-0462