South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Cybersecurity mindset and upskilling: Resilience via lifelong learning and security education

Authors:
Siyabulela Sandi[1]
Carolien L. van den Berg[1]

Affiliations:
[1]Department of Information Systems, Faculty of Economic and Management Sciences, University of the Western Cape, Cape Town, South Africa

Corresponding author:
Carolien van den Berg,
cvandenberg@uwc.ac.za

Dates:
Received: 12 June 2025
Accepted: 28 July 2025
Published: 23 Sept. 2025

How to cite this article:
Sandi, S. & Van den Berg, C.L., 2025, 'Cybersecurity mindset and upskilling: Resilience via lifelong learning and security education', *South African Journal of Information Management* 27(1), a2044. https://doi.org/10.4102/sajim.v27i1.2044

Background: Cyber-crime has escalated globally, posing significant risks to individuals, organisations and governments. Traditional security approaches are no longer sufficient to address evolving threats, highlighting the need for a cybersecurity mindset grounded in education and continuous learning. This study responded to a critical gap in understanding how lifelong learning and upskilling contribute to building cyber resilience.

Objectives: This study aimed to investigate how cybersecurity education and awareness initiatives foster a cybersecurity mindset and resilience among individuals and enterprises. It also examined the challenges and opportunities in enhancing collaboration between academia, industry and government to strengthen cybersecurity education.

Method: A systematic literature review was conducted following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines, analysing 46 peer-reviewed articles published between 2020 and 2024. The review focused on educational strategies, awareness initiatives and collaboration models that support cybersecurity resilience.

Results: The review revealed that continuous education, when embedded in formal, informal and professional learning contexts, significantly strengthens cybersecurity awareness and behavioural change. A proactive, multidisciplinary approach and collaboration across sectors were consistently emphasised as vital for sustained impact.

Conclusion: Cybersecurity resilience is not solely a technological issue but a cultural and educational imperative. Embedding cybersecurity mindset development in national education strategies and organisational training programmes is essential to keeping pace with emerging threats.

Contribution: This study contributes a consolidated understanding of how cybersecurity education and lifelong learning foster digital resilience. It offers practical insights for policymakers, educators and industry leaders seeking to align training with the evolving cyber threat landscape.

Keywords: cyber-crime; cybersecurity; cybersecurity mindset; cyber-attack; cyber threat; lifelong learning; upskilling.

Introduction

The rapid advancement of digital technologies has transformed the way societies communicate, interact and conduct business. However, these developments have also introduced complex vulnerabilities that cybercriminals increasingly exploit (Aslan et al. 2023). Cyber-crime is defined as any illegal activity conducted via the Internet to inflict financial, emotional, psychological or reputational harm, affecting all sectors of society, including individuals, enterprises and governments (Chigada 2023). With perpetrators continuously adapting to exploit weaknesses in digital systems, the threat landscape is constantly evolving (Kagita et al. 2022). The World Economic Forum consistently lists cyber-crime among the top global risks, and its financial implications are staggering, costing enterprises trillions in losses globally (Alghamdi 2020). Beyond economic damage, cyber-crime undermines trust in public institutions and private enterprises, threatening social stability and digital transformation agendas (Adisa 2023).

This context underscores the urgent need for holistic responses that extend beyond technological solutions. Education, public awareness and cross-sector collaboration, particularly between academia, industry and government, are critical in cultivating a cybersecurity mindset across society. Lifelong learning and upskilling in information security can equip individuals and enterprises with the knowledge, attitudes and behaviours necessary to proactively mitigate cyber threats (Brooks 2023).

While numerous initiatives address technical cybersecurity measures, less attention has been paid to the human factors, especially the cultivation of a cybersecurity mindset and the role of continuous learning. Existing literature has explored cybersecurity awareness campaigns and isolated training efforts; however, few studies provide a comprehensive review of how lifelong learning and upskilling contribute to developing cyber-resilient individuals and institutions. Moreover, gaps remain in understanding how collaborative, multidisciplinary approaches involving academia, government and industry can be systematised to promote sustainable cyber education (Von Solms & Van Niekerk 2013).

This study responds to this gap by conducting a systematic literature review (SLR) to consolidate current knowledge and identify opportunities to enhance cybersecurity resilience through education, mindset development and strategic collaboration. The study is conceptually grounded in protection motivation theory (PMT) (Rogers 1983), which explains how individuals are motivated to engage in protective behaviours in response to perceived threats. In the context of cybersecurity, PMT provides a lens for understanding how threat appraisals (e.g. perceived vulnerability and severity) and coping appraisals (e.g. self-efficacy, response efficacy and response costs) shape an individual's willingness to adopt secure practices. By linking PMT to lifelong learning and educational interventions, this study positions cybersecurity education not only as a means of information dissemination but also as a driver of behavioural change and collective resilience.

This study aims to explore how cybersecurity education and continuous upskilling can foster a cybersecurity mindset that contributes to societal and organisational resilience. The specific objectives are:

- To investigate how ongoing cybersecurity education and awareness initiatives promote a cybersecurity mindset among individuals and enterprises.
- To identify key challenges and opportunities for strengthening collaboration between academia, industry and government in advancing cybersecurity education and resilience.

Through these objectives, the study seeks to inform the development of integrated, education-based strategies to enhance national and institutional cyber-readiness.

Literature review

Cybersecurity mindset

Cyber-crime has become a problem not only for developing countries but also for industrialised countries. As Aslan et al. (2023) state, as technology continues to advance and become more globally accessible, there are more opportunities for cybercriminals to exploit vulnerabilities and commit crimes online. Therefore, cybersecurity is becoming a global problem that requires international cooperation and coordination. To this end, a cybersecurity mindset is more important than traditional security training (Schoenmakers et al. 2023). Cybersecurity mindset refers to activities that involve processes that constantly watch for security flaws in the systems and not only implement security measures but also promote a culture of cybersecurity awareness (Andronache 2021). On the other hand, traditional security encompasses conventional approaches and practices used to protect information and information technology (IT) infrastructures from cyber threats. Although traditional security measures have been effective, alone, they are increasingly ineffective in the face of modern cyber threats (Yaacoub et al. 2020).

As human errors are often seen as the weakest link in cybersecurity, adopting a cybersecurity mindset is crucial for everyone (Ncubukezi 2022). Educating employees and society on best practices for detecting and preventing cyberthreats can significantly reduce the risk of data breaches and other security incidents. This approach is referred to as proactive rather than reactive and can create a solid culture of security awareness and responsibility across the country (Chatterjee 2021). From the perspective of PMT, the development of a cybersecurity mindset involves two key cognitive processes. Firstly, the threat appraisal refers to the recognition and evaluation of cyber risks, and secondly, the coping appraisal involves the individual's confidence in their ability to respond effectively to those risks (Sulaiman et al. 2022). Together, these appraisals shape an individual's motivation to engage in protective behaviours and form a critical foundation for cultivating a resilient cybersecurity mindset.

Cultivating a cybersecurity mindset

To effectively combat cyber-crime, a sustained and systemic approach to cultivating a cybersecurity mindset must be adopted at the national level (De Silva 2023). This involves shaping both the perception of threats, namely understanding the severity and potential impact of cyber harm and the belief that individuals can take effective action to prevent such harm (Schoenmakers et al. 2023). Within the framework of PMT, these elements correspond to perceived vulnerability, response efficacy and self-efficacy, all of which are critical in promoting protective cybersecurity behaviours. Achieving this requires the implementation of comprehensive education and training initiatives, developed and delivered through collaborative efforts between public and private stakeholders, including academic institutions. These key strategies are outlined and discussed next:

Real-world problem-solving

These include simulations in which actual cybersecurity problems are presented, and participants participate in solving the problems (Kavak et al. 2021). Enterprises can use this approach for their employees, and governments can use their state resources to communicate such initiatives to the general population, for example, in schools, clinics, home affairs, hospitals, etc.

Case studies

A case study approach can be beneficial for enterprises and the wider population when real-life incidents or cybersecurity breaches are analysed to identify lessons learned (Quader & Janeja 2021). This approach enables participants to gain a deeper understanding of their own cybersecurity issues and subsequently improve their security measures. In this way, enterprises and society can better understand the impact of cyber threats and therefore learn more helpful strategies for prevention and response.

Scenario-based learning

Scenario-based learning promotes critical thinking while engaging with a real-world problem (Reed, Mullen & Boyles 2020). In this approach, participants are presented with a theoretical but probable scenario and must decide how to solve it. In this way, participants apply their knowledge and skills in a practical setting, improving their problem-solving skills while preparing for similar situations that may arise. This creates an environment where participants gain a deeper insight into various cybersecurity problems through hands-on experience (Ošlejšek et al. 2020). Through these methods, enterprises, individuals and governments can collaborate with academic institutions and share information and policies to increase cybersecurity awareness among all stakeholders and create a safer digital environment for all. An aware and educated mindset will create processes that mitigate the risks of cyber threats and protect sensitive information from potential breaches.

The role of lifelong learning and upskilling

Continuous learning of cybersecurity practices has become increasingly vital considering the growing incidence and sophistication of cyber-crime in today's digital age (Thakur 2024). As technology evolves, cybercriminals continuously devise new methods to exploit vulnerabilities, reinforcing Nandan's (2021) argument that cybersecurity education must be approached as an ongoing process of lifelong learning and upskilling. Lifelong learning refers to educational and training activities that are continuous, voluntary and self-motivated in both personal and professional contexts (Latchem 2016). It not only enhances employability and effectiveness but also fosters social interaction, civic responsibility and personal development.

From the perspective of PMT, lifelong learning and continuing education play a central role in strengthening the coping appraisal process (Sapeta et al. 2022). By enhancing knowledge, technical competence and perceived agency, particularly self-efficacy, continuous learning equips individuals with the confidence to respond effectively to evolving cyber threats (Stavrou & Piki 2024). When individuals believe that secure behaviours are both effective (response efficacy) and within their capabilities (self-efficacy), they are more likely to adopt and sustain such practices.

In South Africa, the Department of Public Works and Infrastructure has suffered over 300 million Rand worth of cyber-attacks in the last 10 years, with the most recent being 24 million Rand in May 2024 (Cokayne 2024). This is because of negligence, outdated knowledge and training across the department. Collaboration between all stakeholders will ensure better education and training that will improve critical thinking, problem-solving skills and the overall wellness of cybersecurity practices (Reed et al. 2020). Different sectors may approach further education and training activities differently, using different methods that combine academic, non-academic and industry-based learning. These methods are:

Academic – Universities and colleges offer a wide range of cybersecurity educational programmes (e.g. bachelor's, master's or doctoral programmes). These programmes usually combine theoretical knowledge with a practical approach that widens the cybersecurity knowledge gap in society. The government may offer a scholarship to individuals who complete a cybersecurity degree programme and later employ them in their departments. In addition, governments can offer subsidies to enterprises that support their employees to pursue a cybersecurity degree.

Non-academic – For those who do not want to go the university or college route to learn cybersecurity practices, online courses are an option. Platforms such as Coursera, edX and Udemy offer reliable and flexible courses in cybersecurity that are available on demand (Karhu 2021). Cooperation between the public and private sectors and these institutions can enable society to participate in these courses. The knowledge gained can be used within the nation to strengthen the cybersecurity environment.

Seminars and workshops – These gatherings can be conducted on a national level by the government for society or by enterprises training their staff in cybersecurity.

Industry certificates – Certifications are becoming more popular recently as employers require or want applicants to have certain certifications before hiring them. Individuals need to be encouraged to take the certifications that are widely recognised to validate cybersecurity expertise. These are offered online by enterprises such as ISC ^{2}, CompTIA and ISACA and are specifically tailored to a particular sector.

Corporate training initiatives – Continuous professional development (CPD) is considered an effective way for employees to keep up-to-date with cybersecurity trends. Continuous professional development refers to continuous learning programmes that aim to improve employees' skills and understanding in professionalism (Drude, Maheu & Hilty 2019). Continuous professional development includes attending workshops, webinars and conferences as well as gaining further certifications to stay up-to-date with industry standards and best practice. Staff need to be supported to attend and complete their CPD hours, where the knowledge gained will help in the fight against cyber-crime.

Challenges

Promoting any initiative comes with inherent challenges, and the promotion of cybersecurity through mindset development and lifelong learning is no exception. These challenges are particularly pronounced in developing countries, where governments often prioritise urgent socio-economic issues, commonly referred to as 'bread-and-butter' issues, over long-term digital strategies (Kayode-Ajala 2023). Key obstacles include the high costs associated with establishing and maintaining educational programmes, limited time and resources and, in some cases, resistance from communities. These barriers significantly hinder the implementation of proactive and sustainable approaches to combating cybercrime (Qudus 2025).

To overcome these challenges, effective collaboration between the public and private sectors is essential. Such partnerships can facilitate the design and delivery of cost-effective and contextually relevant strategies (Bechara & Schuch 2021). One innovative approach is the gamification of cybersecurity education, particularly for Generation Alpha – children born between 2010 and 2024 – who are highly engaged by interactive, game-based content (McCrindle 2023). Gamification involves the integration of game elements into educational content to increase learner motivation and participation (Macías, Hernández & Saenz 2020). Developing gamified cybersecurity education programmes could significantly enhance engagement across demographics, especially among youth.

Additionally, the growing popularity of hybrid learning accelerated by the coronavirus disease 2019 (COVID-19) pandemic presents a promising avenue for expanding access to cybersecurity training (Hussain, Tummalapalli & Chakravarthy 2024). Public–private partnerships should be leveraged to offer hybrid cybersecurity education programmes, with government support in funding and policy facilitation. Encouraging widespread participation in such models will contribute to greater public awareness, digital literacy and societal resilience against cyber threats (Chibunna et al. 2020).

The future of cybersecurity education

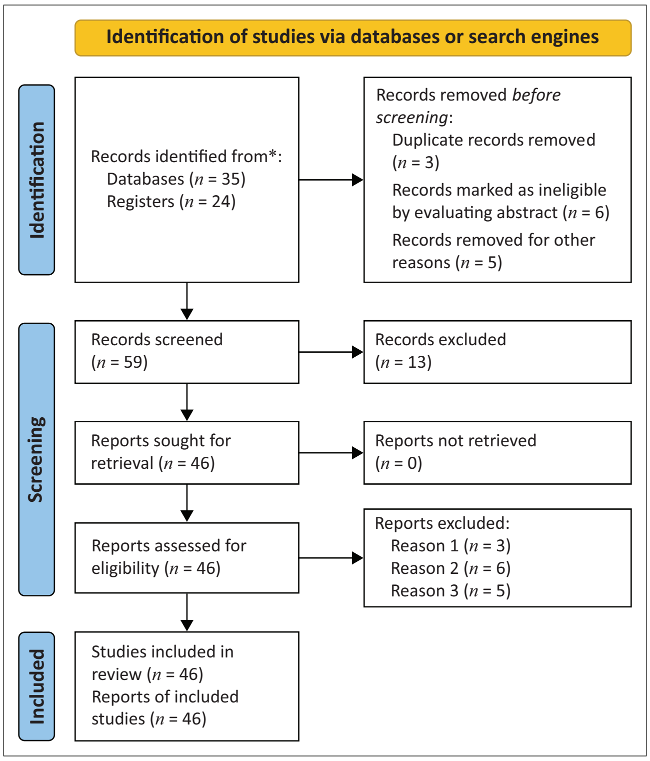
As cybersecurity education continues to evolve, integrating PMT into curriculum design offers a valuable framework for fostering sustained behavioural change. This highlights the importance of understanding how educational interventions shape learners' perceptions of cyber threats and their confidence in managing them and core psychological drivers of secure behaviour, as outlined by PMT (Boehmer et al. 2015). With strategic partnerships among stakeholders, including government, academia and industry, the future of cybersecurity education holds significant promise.

Emerging tools such as Cyber Range, Serious Games and Automated Learning are at the forefront of shaping the global cybersecurity education landscape. Cyber Range is an advanced training approach that offers hands-on experience within a secure virtual environment, often a realistic digital twin of actual systems, enabling participants to practise skills in simulated threat scenarios (Hatzivasilis et al. 2021). Serious Games present cybersecurity scenarios within emulated environments, created using domain-specific languages, where learners assume the roles of attackers or defenders in multiplayer settings to make real-time security decisions (Yamin, Katt & Nowostawski 2021). Automated learning, enhanced through artificial intelligence (AI) and machine learning, supports personalised learning by offering real-time feedback and continuously evaluating participants' strengths and areas for improvement (Sarker 2023).

These advanced educational tools provide learners with practical, real-world competencies needed to effectively address evolving cyber threats. Collectively, they foster highly participative, adaptive and collaborative learning environments that not only enhance technical proficiency. They also instil a proactive cybersecurity mindset and help cultivate a culture of digital security awareness across society.

Research methods and design

In this study, an SLR was conducted in the field of cybersecurity and information security, using Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) as a guide. An SLR is an in-depth exploratory method of collecting, evaluating and integrating knowledge from existing research on a particular topic (Cando et al. 2022; Chukwuere 2022; Tranfield, Denyer & Smart 2023). The researchers followed a methodical and clear process by identifying the relevant literature, assessing its quality and obtaining relevant and necessary results to answer the study questions. The study utilised SLR to obtain current information on the role of education and awareness in combating cyber threats while paving the way for future research (Khan, Khan & Subramaniam 2023). The SLR technique was suitable for this study as it provided a systematic understanding of the missing research areas and addressed the research objectives. As shown in Figure 1, the PRISMA method was used, where literature was collected from sources between June 2020 and December 2024 via search engines such as Google Scholar, Research Gate, JSTOR and Library Search. Key search terms like 'cyber-crime', 'cybersecurity', 'cybersecurity mindset', 'cybersecurity awareness' and 'information security education' were utilised to ensure a comprehensive review of relevant studies. As illustrated in Figure 1, this process enabled a transparent and replicable screening and selection of studies. The inclusion criteria for articles were based on their relevance to the topic of cybersecurity and information security


Identification of studies via databases or search engines
Identification
Records identified from*:
Databases (n = 35)
Registers (n = 24)
Records removed before screening:
Duplicate records removed (n = 3)
Records marked as ineligible by evaluating abstract (n = 6)
Records removed for other reasons (n = 5)
Screening
Records screened (n = 59)
Records excluded (n = 13)
Reports sought for retrieval (n = 46)
Reports not retrieved (n = 0)
Reports assessed for eligibility (n = 46)
Reports excluded:
Reason 1 (n = 3)
Reason 2 (n = 6)
Reason 3 (n = 5)
Included
Studies included in review (n = 46)
Reports of included studies (n = 46)

Source: Adapted from Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D. et al., 2020, 'The PRISMA 2020 statement: An updated guideline for reporting systematic reviews', *Research Methods and Reporting – Open Access* 10, 1–9

*, Records retrieved electronically.

FIGURE 1: Preferred reporting items for systematic reviews and meta-analyses flow diagram.

education, while exclusion criteria focused on outdated or irrelevant sources, as filtered systematically in the steps outlined in Figure 1.

Fifty-nine articles were initially identified from the following search engines: 21 from Google Scholar, 16 from Research Gate, 11 from JSTOR and 11 from Library Search. After careful review of the articles, 46 were included in this study. Appendix 1 – Table 1-A1 provides a summary of the 46 selected articles, including their titles, authors, publication years and key areas of contribution to this study. There were three duplicate articles; six articles were excluded as inappropriate after the researchers evaluated the abstracts; and five articles were removed after reading the entire articles because the content did not align with the objectives of the study. In addition, the researchers were able to conduct a comprehensive review of the existing literature on cybersecurity mindset and upskilling through lifelong learning and information security education for this study. Aarseth et al. (2017) point out that SLR is considered the most practical and clear research approach compared to traditional research approaches.

Inclusion and exclusion criteria

To ensure the rigour and relevance of the SLR, a set of predefined inclusion and exclusion criteria was applied during the article selection process. The initial screening involved a review of article abstracts to determine eligibility based on the following inclusion parameters:

- Studies were published in English, ensuring accessibility and consistency in interpretation.
- The articles focused on cybersecurity and information security.
- Only publications from accredited and peer-reviewed journals or conference proceedings were considered.
- The publication timeframe was restricted to the period between 2020 and 2024, reflecting the rapidly evolving nature of the information security landscape.
- Studies specifically addressed aspects of lifelong learning, upskilling or cybersecurity education, aligning with the core themes of the review.

The selection process prioritised the inclusion of high-quality, current and thematically aligned studies to enhance the validity and applicability of the review's findings.

Theoretical perception

The application of PMT in information systems, particularly within cybersecurity research, has gained momentum because of its ability to explain how individuals assess and respond to cyber threats (Ifinedo 2012; Johnston & Warkentin 2010). Protection motivation theory provides a valuable framework for predicting individuals' intentions to adopt protective behaviours and for understanding their responses to perceived cyber risks. The theory posits that such behaviour is shaped by two key appraisals: threat appraisal, which includes perceived severity and vulnerability and coping appraisal, which involves self-efficacy, response efficacy and response costs (Clubb & Hinkle 2015). This theoretical lens is particularly useful in evaluating the effectiveness of cybersecurity awareness programmes, training initiatives and behavioural interventions. By identifying the psychological factors that influence decision-making when individuals are confronted with cyber threats, PMT can inform the development of strategies that promote a culture of cybersecurity awareness, responsibility and compliance across society.

Ethical considerations

Ethical clearance to conduct this study was obtained from the University of the Western Cape, Humanities and Social Science Research Ethics Committee (HS24/10/64). Although this study is based on an SLR and did not involve direct human participants or primary data collection, ethical considerations remain integral to the study process. Initially, the review process adhered to academic integrity principles by ensuring that all sources were appropriately cited, and intellectual contributions from original authors were acknowledged. Ethical consistency was further maintained through a transparent and systematic methodology following the PRISMA guidelines. This approach ensured that article selection, inclusion and exclusion criteria and data extraction were conducted objectively, thereby minimising bias and enhancing reliability.

Furthermore, the thematic focus on cybersecurity education and behavioural change inherently engages with ethical concerns around privacy, trust and digital responsibility. By promoting a cybersecurity mindset rooted in ethical awareness, the study contributes to developing not only technically competent but also ethically conscious digital citizens (Permana et al. 2023). With that, the study alludes to the fact that cultivating cyber resilience requires a moral commitment to safeguarding information. It also involves respecting user autonomy and promoting responsible digital behaviour across all sectors of society.

Discussion

Results and recommendations

The results of the SLR conducted in this study underscore the critical importance of continuous cybersecurity education in cultivating a resilient, security-conscious society. As the cyber threat landscape becomes increasingly complex and dynamic, both individuals and organisations must adopt a proactive stance towards cybersecurity awareness and training (Victor-Mgbachi 2024). The review reveals that lifelong learning, when embedded in both formal education systems and workplace training initiatives, substantially improves individuals' capabilities to detect, prevent and respond effectively to cyber threats.

Considering this, PMT suggests that increased knowledge strengthens both self-efficacy and response efficacy, critical components of coping appraisal, which in turn influence the adoption of secure behaviour (Alam et al. 2025).

Recent empirical studies reinforce the important role of structured education in strengthening cybersecurity awareness and behaviour. For instance, Shillair et al. (2022), drawing on national-level survey data across multiple countries, found that individuals who participated in formal cybersecurity awareness programmes demonstrated over 40% higher likelihood of adopting secure password practices, recognising phishing attempts and reporting suspicious activity compared to those without training. Similarly, Stavrou and Piki (2024) observed that professionals who engaged in continuous re-skilling programmes in cybersecurity reported a notable increase in self-efficacy and threat appraisal, key components of PMT, which in turn positively influenced their adherence to security protocols. These findings affirm that cybersecurity education should not be treated as a one-off intervention but rather as a dynamic, lifelong process that evolves in tandem with emerging threats. Institutions and governments are therefore encouraged to institutionalise lifelong cybersecurity education as part of national resilience strategies and workforce development plans.

Figure 2 illustrates six key practical recommendations integrated within the cybersecurity mindset framework that emerged from this study. These recommendations are aimed at strengthening cybersecurity resilience through education, policy and collaboration across sectors. As shown in Figure 2, the core recommendations include:

- Strengthening cybersecurity education and lifelong learning,
- Enhancing collaboration between academia, industry and government,
- Promoting a culture of cybersecurity awareness,
- Improving cybersecurity policy and regulatory frameworks,
- Leveraging technology for cybersecurity training and awareness and
- Embracing PMT as a behavioural foundation.

Each of these components depicted in Figure 2 will be discussed in more detail to demonstrate their contribution to cultivating a proactive cybersecurity culture and mindset.

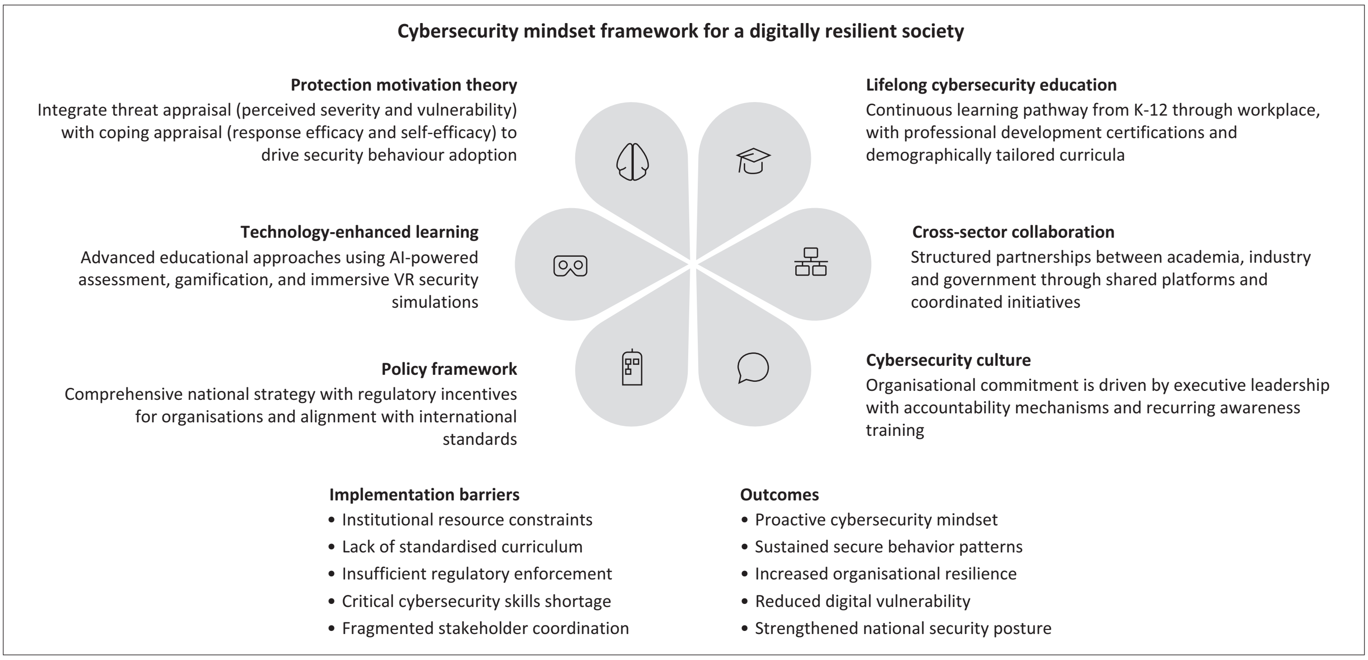
Strengthening cybersecurity education and lifelong learning

Strengthening cybersecurity education and lifelong learning is very important to ensure that individuals and enterprises are equipped to defend against evolving cyber threats (Shillair et al. 2022). There are various strategies on how this can be achieved; integrating cybersecurity awareness and training programmes at all levels of education, from primary to secondary schools and higher education, is paramount. Cybersecurity awareness has become an important aspect of modern education because of the increasing reliance on technology in all aspects of society (Arishi et al. 2024). Therefore, using the school system as a vehicle to introduce cybersecurity awareness can create early opportunities for the future generation to understand the importance of a safe cyber environment. This early exposure can, in turn, contribute to strengthening national cybersecurity resilience.

Developing specialised cybersecurity curricula tailored to the specific needs of the industry can help enterprises focus and better prepare their human resources to ensure that better strategies are implemented to combat direct cyber threats (Towhidi & Pridmore 2023). Thus, training programmes should be tailored to the specific challenges confronting these enterprises, ensuring that their human capital possesses the requisite skills and knowledge to safeguard sensitive data. In addition, employee participation in CPD programmes and cybersecurity certification programmes can leverage their knowledge to increase cyber resilience within the enterprise.

Enhancing collaboration between academia, industry and government

Improving collaboration between academia, industry and government presents not only some opportunities but also some challenges. Opportunities include building public–private partnerships to share knowledge, resources and best practices in cybersecurity (ThankGod 2024). This can be done through programmes such as collaborative research groups, joint internships between sectors and industry–academia partnerships. In addition, clear and open channels of interaction and platforms for knowledge sharing can address challenges such as conflicting priorities, lack of interaction and divergent goals between academic, industry and government stakeholders.



Cybersecurity mindset framework for a digitally resilient society

Protection motivation theory
Integrate threat appraisal (perceived severity and vulnerability) with coping appraisal (response efficacy and self-efficacy) to drive security behaviour adoption

Lifelong cybersecurity education
Continuous learning pathway from K-12 through workplace, with professional development certifications and demographically tailored curricula

Technology-enhanced learning
Advanced educational approaches using AI-powered assessment, gamification, and immersive VR security simulations

Cross-sector collaboration
Structured partnerships between academia, industry and government through shared platforms and coordinated initiatives

Policy framework
Comprehensive national strategy with regulatory incentives for organisations and alignment with international standards

Cybersecurity culture
Organisational commitment is driven by executive leadership with accountability mechanisms and recurring awareness training

Implementation barriers
- Institutional resource constraints
- Lack of standardised curriculum
- Insufficient regulatory enforcement
- Critical cybersecurity skills shortage
- Fragmented stakeholder coordination

Outcomes
- Proactive cybersecurity mindset
- Sustained secure behavior patterns
- Increased organisational resilience
- Reduced digital vulnerability
- Strengthened national security posture

AI, artificial intelligence; VR, virtual reality.

FIGURE 2: Cybersecurity mindset framework.

The establishment of industry-led research projects that focus on real-world cybersecurity challenges can also contribute to unified collaboration (Mukherjee et al. 2024). This is done by developing practical solutions that address the current cyber threat landscape affecting the global critical IT infrastructure. To foster collaboration, government-led cybersecurity initiatives such as awareness campaigns should be developed and implemented through the government to citizens to ensure a digitally secure environment for all (Shillair et al. 2022). The initiative should be comprehensive; therefore, the government should establish a cybersecurity centre where society and businesses are regularly informed about current trends in cybersecurity.

Promoting a culture of cybersecurity awareness

Because of the ever-growing number of cyber incidents around the world, the culture of cybersecurity is becoming increasingly important in society. As noted by Reegård, Blackett and Katta (2019), cybersecurity culture is broad and encompasses a wide range of practices, behaviours and attitudes towards protecting digital information assets. Implementing mandatory cybersecurity training for all employees across all sectors can ensure that employees are knowledgeable and equipped with current trends to protect critical IT infrastructure. In addition, senior management should demonstrate proactive cybersecurity leadership by promoting and supporting cybersecurity activities within enterprises (Abrahams et al. 2024). This can be achieved by promoting a culture of cybersecurity awareness and prioritising ongoing training for employees. As Yamin et al. (2021) state, the development of game-based learning approaches and hands-on virtual reality simulations can help to make cybersecurity training engaging and effective. Incorporating these strategies can help retain employee knowledge and reduce the risk of cyber-attacks.

Improving cybersecurity policy and regulatory frameworks

As enterprises continue to grapple with the escalating cyber threat landscape, strengthening their cybersecurity defences will become increasingly important (Abrahams et al. 2024). Policy and regulatory frameworks are key areas that any industry or government must strengthen to ensure order among businesses or in society. Advocating for robust cybersecurity policies that emphasise education and proactive cybersecurity strategies becomes even more necessary for industry regulators than it is for the government to enforce them. This makes the alignment of national cybersecurity strategies with international best practices and standards a key concern (AlDaajeh & Alrabaee 2024).

By aligning with international best practices, nations can also improve communication and collaboration with other nations in addressing cybersecurity challenges. Another proven strategy is to create incentives for enterprises that implement comprehensive cybersecurity training programmes (Zhang et al. 2021). This strategy can encourage enterprises to prioritise cybersecurity education for their employees, leading them to an overall more secure digital environment (AlDaajeh et al. 2022). Offering incentives can assist in offsetting the costs associated with implementing these training programmes and make them more accessible, especially for small and medium-sized businesses that lack these resources to combat cybercrime.

Leveraging technology for cybersecurity training and awareness

Artificial intelligence has become an increasingly prevalent and transformative technology used in various sectors of the economy (Abbas Khan et al. 2024). Using this technology for cybersecurity training and awareness can enhance the ability to personalise the learning experiences of participants. This can be achieved by integrating machine learning algorithms to analyse personal learning styles and preferences to improve engagement and intelligence retention (Essa, Celik & Human-Hendricks 2023). On the other hand, AI can mimic real-world cyber threats and attacks, allowing participants to further develop their skills and knowledge in a hands-on learning environment.

The development of freely accessible online cybersecurity training resources in the form of courses for small businesses and the public can help improve citizens' awareness and knowledge of cybersecurity best practices (Willie 2023). This approach will ensure the involvement of a wider population and help to close the gap in cybersecurity skills and knowledge. As Li and Liu (2021) stated, the better-informed people are, the better equipped they are to protect themselves from cyber threats and attacks, leading to an overall safer cyber environment for all.

Embracing protection motivation theory as a behavioural foundation

Following the implementation of the preceding five practical recommendations, it becomes essential to adopt a theoretical framework that can effectively guide behavioural change in cybersecurity education (Chowdhury, Adam & Teubner 2020). Given that this study is grounded in PMT, it is well suited to serve this purpose. Protection motivation theory offers a robust foundation for understanding how individuals assess and respond to cyber threats (Alam et al. 2025). This recommendation, therefore, advocates for the integration of threat appraisal encompassing perceived severity and vulnerability with coping appraisal. The latter includes response efficacy and self-efficacy, both of which should be embedded into the design of cybersecurity education interventions. Embedding these constructs into educational strategies can foster deeper behavioural engagement, enhance motivation to adopt secure practices and ultimately support the development of a cybersecurity-conscious society.

Limitations

While this study provides valuable insights into the role of cybersecurity education and lifelong learning in fostering resilience, several limitations should be acknowledged. Firstly, as an SLR, the findings are inherently dependent on the quality, scope and geographic representation of the selected publications. Although efforts were made to ensure a comprehensive review using PRISMA guidelines, the final sample of 46 peer-reviewed articles may not fully capture emerging practices or regional nuances, particularly in underrepresented or non-English-speaking contexts.

Secondly, the study did not include primary empirical data such as interviews or surveys with stakeholders from academia, industry or government. As a result, the analysis is limited to secondary sources and may not reflect the most current on-the-ground realities or sector-specific challenges in implementing cybersecurity education programmes. Future research could benefit from mixed-method approaches that triangulate literature findings with field data to provide deeper, context-rich perspectives.

Thirdly, the dynamic nature of cybersecurity threats and rapid technological advancements mean that conclusions drawn from literature published between 2020 and 2024 may quickly become outdated. The fast-paced evolution of the threat landscape demands continuous updating of educational frameworks and policies, which this study could only address to a limited extent. Ongoing monitoring and adaptive research will be crucial to maintaining the relevance of proposed strategies for fostering cyber resilience through education.

Conclusion

Technology is evolving at an unprecedented pace, often outstripping the ability of individuals and organisations to maintain up-to-date technological competencies. This creates opportunities for cybercriminals to exploit emerging vulnerabilities and behavioural gaps (Yamin et al. 2021). In this context, the integration of PMT into cybersecurity education offers a valuable framework for designing interventions that do more than disseminate information – they empower individuals to adopt and sustain secure behaviours. By understanding how individuals perceive and respond to cyber threats, educators and policymakers can develop strategies that strengthen both threat appraisal (awareness of severity and vulnerability) and coping appraisal (belief in the effectiveness of protective actions and confidence in one's ability to act). This approach underscores the importance of cultivating a cybersecurity mindset as a foundation for building a resilient and security-conscious society.

The findings of this study, based on an SLR, highlight the critical role of continuous cybersecurity education, cross-sector collaboration, sound policy development and the use of contextually relevant technological tools in promoting a robust cybersecurity culture. Strengthening cybersecurity education and lifelong learning is fundamental to ensuring that individuals and enterprises possess the competencies required to navigate an evolving threat landscape. Embedding cybersecurity awareness into both formal education systems and workplace training allows organisations to foster a proactive defence posture. Such integration not only enhances individual preparedness but also supports organisational resilience and national digital security.

Collaboration between academia, industry and government remains a key requirement for effective cybersecurity education and capacity building. A unified approach that leverages resources, expertise and best practices can bridge existing gaps, especially in resource-limited environments. Promoting a culture of cybersecurity awareness and accountability at all levels of society will ensure that security becomes a shared responsibility and not an isolated task. By working together, all stakeholders can better enable society to keep abreast of the latest cyber threats and further improve their skills by developing proactive approaches through lifelong learning and information security education (Bechara & Schuch 2021).

To create a safer digital environment for all, the role of lifelong learning and the future of cyber education are critical to preparing enterprises, governments and society for future cybersecurity challenges. Continuous education through lifelong learning will protect enterprises, governments and society from evolving cyber threats and ensure a more resilient digital landscape.

Acknowledgements

This article is partially based on the author, S.S.'s PhD thesis entitled, 'The development of a maturity framework to guide small to medium enterprises in the implementing of cybersecurity practices in the Eastern Cape', towards the degree of Doctor of Philosophy in Information Systems in the Department of Information Systems, University of the Western Cape, South Africa, with supervisor Professor Carolien van den Berg. At the time of publication, the thesis was still in progress.

The authors acknowledge the late Prof Joel Chigada, who sadly passed away in February 2025, for his invaluable guidance and support as a supervisor. His insights, particularly in shaping the literature review, significantly contributed to the development of this article. His scholarly input and mentorship are deeply appreciated and will be fondly remembered.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Author's contributions

S.S. conceptualised the idea and shared it with C.L.v.d.B C.L.v.d.B developed the structure and key issues of the article. S.S. was responsible for identifying research articles that resonated with the study. Subsequently, S.S. did the write-up and handed it to C.L.v.d.B for editing and final structure and submission of the article to the journal. S.S. was responsible for the conceptualisation, methodology, formal analysis, investigation and writing – original draft. C.L.v.d.B was responsible for the formal analysis, project administration, validation, writing – review and editing and supervision.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The data that support the findings of this study are available from the corresponding author, C.L.v.d.B, upon reasonable request.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. They do not necessarily reflect the official policy or position of any affiliated institution, funder, agency or that of the publisher. The authors are responsible for this article's results, findings and content.

References

Aarseth, W., Ahola, T., Aaltonen, K., Okland, A. & Andersen, B., 2017, 'Project sustainability strategies: A systematic literature review', *International Journal of Project Management* 35(6), 1071–1083. https://doi.org/10.1016/j.ijproman.2016.11.006

Abbas Khan, M., Khan, H., Omer, M.F., Ullah, I. & Yasir, M., 2024, 'Impact of artificial intelligence on the global economy and technology advancements', in S.E. Hajjami, K. Kaushik & I. Ullah Khan (eds.), *Artificial general intelligence (AGI) security: Smart applications and sustainable technologies*, pp. 147–180, Springer, Singapore.

Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. & Dawodu, S.O., 2024, 'Cybersecurity awareness and education programs: A review of employee engagement and accountability', *Computer Science & IT Research Journal* 5(1), 100–119. https://doi.org/10.51594/csitrj.v5i1.708

Adisa, O.T., 2023, 'The impact of cybercrime and cybersecurity on Nigeria's national security', International Master's in Security, Intelligence and Strategic Studies, Erasmus Mundus, pp. 1–17.

Alam, S.S., Ahsan, N., Kokash, H.A., Alam, S. & Ahmed, S., 2025, 'A students' behaviors in information security: Extension of Protection Motivation Theory (PMT)', *Information Security Journal: A Global Perspective* 34(3), 191–213. https://doi.org/10.1080/19393555.2024.2408264

AlDaajeh, S. & Alrabaee, S., 2024, 'Strategic cybersecurity', *Computers & Security* 141, 1–22. https://doi.org/10.1016/j.cose.2024.103845

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F. & Choo, K.K.R., 2022, 'The role of national cybersecurity strategies on the improvement of cybersecurity education', *Computers & Security* 119, 1–21. https://doi.org/10.1016/j.cose.2022.102754

Alghamdi, M.I., 2020, 'A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide', *International Journal of Engineering Research and Technology* 9(6), 731–735.

Andronache, A., 2021, 'Increasing security awareness through lenses of cybersecurity culture', *Journal of Information Systems & Operations Management* 15(1), 7–22.

Arishi, A.A., Kamarudin, N.H., Bakar, K.A.A., Shukur, Z.B. & Hasan, M.K., 2024, 'Cybersecurity awareness in schools: A systematic review of practices, challenges, and target audiences', *Integration* 15(12), 1–13. https://doi.org/10.14569/IJACSA.2024.0151249

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. & Akin, E., 2023, 'A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions', *Electronics* 12(6), 1–42. https://doi.org/10.3390/electronics12061333

Bechara, F.R. & Schuch, S.B., 2021, 'Cybersecurity and global regulatory challenges', *Journal of Financial Crime* 28(2), 359–374. https://doi.org/10.1108/JFC-07-2020-0149

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S. & Cotten, S., 2015, 'Determinants of online safety behaviour: Towards an intervention strategy for college students', *Behaviour & Information Technology* 34(10), 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448

Brooks, C., 2023, *Academia, industry, and government can create innovative partnerships*, viewed 29 April 2025, from https://www.forbes.com/sites/chuckbrooks/2023/07/13/academia-industry-and-government-can-create-innovative-partnerships-and-help-secure-our-digital-future/.

Cando, L.F., Perias, G.A., Tantengco, O.A., Dispo, M.D., Ceriales, J.A., Girasol, M.J. et al., 2022, 'The global prevalence of Schistosoma mansoni, S. japonicum, and S. haematobium in pregnant women: A systematic review and meta-analysis', *Tropical Medicine and Infectious Disease* 7(11), 354–367. https://doi.org/10.3390/tropicalmed7110354

Chatterjee, D., 2021, *Cybersecurity readiness: A holistic and high-performance approach*, Sage Publications, California.

Chibunna, U.B., Hamza, O., Collins, A., Onoja, J.P., Eweja, A. & Daraojimba, A.I., 2020, 'Building digital literacy and cybersecurity awareness to empower underrepresented groups in the tech industry', *International Journal of Multidisciplinary Research and Growth Evaluation* 1(1), 125–138. https://doi.org/10.54660/.IJMRGE.2020.1.1.125-138

Chigada, J., 2023, 'Towards an aligned South African national cybersecurity policy framework', Doctoral dissertation, University of Cape Town, Faculty of Commerce, Department of Information Systems, viewed 23 May 2025, from http://hdl.handle.net/11427/38253.

Chowdhury, N.H., Adam, M.T.P. & Teubner, T., 2020, 'Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures', *Computers & Security* 97, 1–13.

Chukwuere, J.E., 2022, 'Social media and COVID-19 pandemic: A systematic literature review', *Journal of African Films and Diaspora Studies* 5(1), 5–31. https://doi.org/10.31920/2516-2713/2022/5n1a1

Clubb, A.C. & Hinkle, J.C., 2015, 'Protection motivation theory as a theoretical framework for understanding the use of protective measures', *Criminal Justice Studies* 28(3), 336–355. https://doi.org/10.1080/1478601X.2015.1050590

Cokayne, R., 2024, 'New public works minister discloses R300m cyber-related theft from department', *MoneyWeb*, viewed 19 July 2025, from https://www.moneyweb.co.za/news/south-africa/new-public-works-minister-discloses-r300m-cyber-related-theft-from-department/.

De Silva, B., 2023, 'Exploring the relationship between cybersecurity culture and cyber-crime prevention: A systematic review', *International Journal of Information Security and Cybercrime (IJISC)* 12(1), 23–29. https://doi.org/10.19107/IJISC.2023.01.03

Drude, K.P., Maheu, M. & Hilty, D.M., 2019, 'Continuing professional development: Reflections on a lifelong learning process', *Psychiatric Clinics* 42(3), 447–461. https://doi.org/10.1016/j.psc.2019.05.002

Essa, S.G., Celik, T. & Human-Hendricks, N.E., 2023, 'Personalized adaptive learning technologies based on machine learning techniques to identify learning styles: A systematic literature review', *IEEE Access* 11, 48392–48409. https://doi.org/10.1109/ACCESS.2023.3276439

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Braghin, C. et al., 2021, 'The threat-arrest cyber range platform', in *2021 IEEE International Conference on Cyber Security and Resilience*, Institute of Electrical and Electronics Engineers (IEEE), Rhodes, Greece, July 26–28, 2021, pp. 422–427.

Hussain, S.M., Tummalapalli, S.R.K. & Chakravarthy, A.S.N., 2024, 'Cyber security education: Enhancing cyber security capabilities, navigating trends and challenges in a dynamic landscape', *Advances in Cyber Security and Digital Forensics* 3, 9–33. https://doi.org/10.58532/nbennurch254

Ifinedo, P., 2012, 'Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory', *Computers & Security* 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Johnston, A.C. & Warkentin, M., 2010, 'Fear appeals and information security behaviors: An empirical study', *MIS Quarterly* 34(3), 549–566. https://doi.org/10.2307/25750691

Kagita, M.K., Thilakarathne, N., Gadekallu, T.R., Maddikunta, P.K.R. & Singh, S., 2022, 'A review on cybercrimes on the internet of things', in M. Aaisha & K. Neeraj (eds.), *Deep learning for security and privacy preservation in IoT*, pp. 83–98, Springer, Singapore.

Karhu, A., 2021, 'Mapping study of MOOC providers: The current state of computer science education and platform technical capabilities', Thesis, Lappeenranta-Lahti University of Technology LUT, viewed 18 May 2025, from https://lutpub.lut.fi/bitstream/handle/10024/163184/Kandidaatintyo_Aleksi_Karhu.pdf?sequence=1.

Kavak, H., Padilla, J.J., Vernon-Bido, D., Diallo, S.Y., Gore, R. & Shetty, S., 2021, 'Simulation for cybersecurity: State of the art and future directions', *Journal of Cybersecurity* 7(1), 1–13. https://doi.org/10.1093/cybsec/tyab005

Kayode-Ajala, O., 2023, 'Establishing cyber resilience in developing countries: An exploratory investigation into institutional, legal, financial, and social challenges', *International Journal of Sustainable Infrastructure for Cities and Societies* 8(9), 1–10.

Khan, M.A., Khan, S.M. & Subramaniam, S.K., 2023, 'A systematic literature review on security issues in cloud computing using edge computing and blockchain: Threat, mitigation, and future trends', *Malaysian Journal of Computer Science* 36(4), 347–367. https://doi.org/10.22452/mjcs.vol36no4.2

Latchem, C., 2016, 'Learning technology and lifelong informal, self-directed, and non-formal learning', in R. Nick & D.W. Surry (eds.), *The Wiley handbook of learning technology*, pp. 180–199, Wiley, Hoboken, New Jersey, USA.

Li, Y. & Liu, Q., 2021, 'A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments', *Energy Reports* 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Macías, Z.L.V., Hernández, A.A.R. & Saenz, C.L.S., 2020, 'Digital games (gamification) in learning and training: An approach to adaptation and integration in the classroom', *Gist: Education and Learning Research Journal* 20, 171–188. https://doi.org/10.26817/16925777.765

McCrindle, M., 2023, *Generation alpha, edition: Illustrated*, Hachette, Sydney.

Mukherjee, M., Le, N.T., Chow, Y.W. & Susilo, W., 2024, 'Strategic approaches to cybersecurity learning: A study of educational models and outcomes', *Information* 15(2), 117–133. https://doi.org/10.3390/info15020117

Nandan, A.B., 2021, 'Cybercrimes and its alarming escalation during recent times', *International Journal of Law Management & Humanities* 4(4), 2413–2423.

Ncubukezi, T., 2022, 'Human errors: A cybersecurity concern and the weakest link to small businesses', in R.P. Griffin, U. Tatar & B. Yankson (eds.), *Proceedings of the 17th International Conference on Information Warfare and Security*, Academic Conferences International Limited, Albany, New York, USA, March 17–18, 2022, pp. 395–401.

Ošlejšek, R., Rusňák, V., Burská, K., Švábenský, V., Vykopal, J. & Čegan, J., 2020, 'Conceptual model of visual analytics for hands-on cybersecurity training', *IEEE Transactions on Visualization and Computer Graphics* 27(8), 3425–3437. https://doi.org/10.1109/TVCG.2020.2977336

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D. et al., 2020, 'The PRISMA 2020 statement: An updated guideline for reporting systematic reviews', *Research Methods and Reporting – Open Access* 10, 1–9.

Permana, I.K.A., Yasa, I.K.A.S., Saputra, I.K.A.D. & Sudwika, I.P.R., 2023, 'Citizenship in the digital age: Implications and challenges', *Journal of Digital Law and Policy* 3(1), 52–62. https://doi.org/10.58982/jdlp.v3i1.510

Quader, F. & Janeja, V.P., 2021, 'Insights into organizational security readiness: Lessons learned from cyber-attack case studies', *Journal of Cybersecurity and Privacy* 1(4), 638–659. https://doi.org/10.3390/jcp1040032

Qudus, L., 2025, 'Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges', *International Journal of Science and Research Archive* 14(1), 1146–1163. https://doi.org/10.30574/ijsra.2025.14.1.0225

Reed, S.S., Mullen, C.A. & Boyles, E.T., 2020, 'Bringing problem-based learning to elementary schools to benefit children's readiness for a global world', *Handbook of Social Justice Interventions in Education* 1(1), 1–29. https://doi.org/10.1007/978-3-030-29553-0_128-2

Reegård, K., Blackett, C. & Katta, V., 2019, 'The concept of cybersecurity culture', in B. Micheal & Z. Enrico (eds.), *The 29th European Safety and Reliability Conference*, Research Publishing, Singapore, Hannover, Germany. September 22–26, 2019, pp. 4036–4043.

Rogers, R., 1983, 'Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation', in J. Cacioppo & R. Petty (eds.), *Social psychophysiology*, pp. 153–177, Guilford Press, New York, NY.

Sapeta, P., Centeno, C., Belar, A. & Arantzamendi, M., 2022, 'Adaptation and continuous learning: Integrative review of coping strategies of palliative care professionals', *Palliative Medicine* 36(1), 15–29. https://doi.org/10.1177/02692163211047149

Sarker, I.H., 2023, 'Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects', *Annals of Data Science* 10(6), 1473–1498. https://doi.org/10.1007/s40745-022-00444-2

Schoenmakers, K., Greene, D., Stutterheim, S., Lin, H. & Palmer, M.J., 2023, 'The security mindset: Characteristics, development, and consequences', *Journal of Cybersecurity* 9(1), 1–15. https://doi.org/10.1093/cybsec/tyad010

Shillair, R., Esteve-González, P., Dutton, W.H., Creese, S., Nagyfejeo, E. & Von Solms, B., 2022, 'Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise', *Computers & Security* 119, 1–11. https://doi.org/10.1016/j.cose.2022.102756

Stavrou, E. & Piki, A., 2024, 'Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity', *Information & Computer Security* 32(4), 523–541. https://doi.org/10.1108/ICS-02-2024-0038

Sulaiman, N.S., Fauzi, M.A., Hussain, S. & Wider, W., 2022, 'Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks', *Information* 13(9), 1–17. https://doi.org/10.3390/info13090413

Thakur, M., 2024, 'Cyber security threats and countermeasures in digital age', *Journal of Applied Science and Education (JASE)* 4(1), 1–20. https://doi.org/10.54060/a2zjournals.jase.42

ThankGod, J., 2024, 'Public-private partnerships in strengthening cybersecurity for international trade: Examining the role of collaborative efforts between governments and private sector entities in crafting and enforcing robust cybersecurity measures for global trade', *SSRN Electronic Journal* 1–12. https://doi.org/10.2139/ssrn.4858776

Towhidi, G. & Pridmore, J., 2023, 'Aligning cybersecurity in higher education with industry needs', *Journal of Information Systems Education* 34(1), 70–83.

Tranfield, D., Denyer, D. & Smart, P., 2023, 'Towards a methodology for developing evidence-informed management knowledge by means of systematic review', *British Journal of Management* 14(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Victor-Mgbachi, T., 2024, 'Navigating cybersecurity beyond compliance: Understanding your threat landscape and vulnerabilities', *Iconic Research and Engineering Journals* 7(7), 70–81.

Von Solms, R. & van Niekerk, J., 2013, 'From information security to cyber security', *Computers & Security* 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Willie, M.M., 2023, 'The role of organizational culture in cybersecurity: Building a security-first culture', *Journal of Research, Innovation and Technologies* 2(16), 179–198. https://doi.org/10.57017/jorit.v2.2(4).05

Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A. & Malli, M., 2020, 'Cyber-physical systems security: Limitations, issues and future trends', *Microprocessors and Microsystems* 7(7), 1–33. https://doi.org/10.1016/j.micpro.2020.103201

Yamin, M.M., Katt, B. & Nowostawski, M., 2021, 'Serious games as a tool to model attack and defense scenarios for cyber-security exercises', *Computers & Security* 110(2), 1–22. https://doi.org/10.1016/j.cose.2021.102450

Zhang, J., 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

Appendix starts on the next page →

Appendix 1

TABLE 1-A1: Systematic literature review: Summary of selected articles.

No.	Author(s)	Year	Title	Key findings / Contribution
1	Abbas Khan et al.	2024	Impact of artificial intelligence on the global economy and technology advancements.	Artificial intelligence (AI)'s influence on global economy and tech
2	Abrahams et al.	2024	Cybersecurity awareness and education programs: A review of employee engagement and accountability.	Importance of employee engagement
3	Adisa, O.	2023	The impact of cybercrime and cybersecurity on Nigeria's national security.	Cybercrime threat to national security
4	AlDaajeh and Alrabaee	2024	Strategic cybersecurity.	National approaches to cyber strategies
5	AlDaajeh et al.	2022	The role of national cybersecurity strategies on the improvement of cybersecurity education.	Education enhancement via national strategies
6	Alam et al.	2025	A students' behaviours in information security: Extension of Protection Motivation Theory (PMT).	Cybersecurity behaviours
7	Arishi et al.	2024	Cybersecurity Awareness in Schools: A Systematic Review of Practices, Challenges, and Target Audiences**.**	Challenges in promoting awareness
8	Bechara, F and Schuch, S.	2021	Cybersecurity and global regulatory challenges	Global regulatory challenges
9	Brooks, C.	2024	Academia, industry, and government can create innovative partnerships.	Cybersecurity collaboration and partnership
10	Cando et al.	2020	Systematic review and meta-analysis.	Systematic review
11	Chatterjee, D.	2021	Cybersecurity readiness: A holistic and high-performance approach.	Cybersecurity readiness
12	Chibunna et al.	2020	Building Digital Literacy and Cybersecurity Awareness to Empower Underrepresented Groups in the Tech Industry.	Cybersecurity awareness
13	Chigada, J.	2023	Towards an aligned South African national cybersecurity policy framework.	Cybersecurity policy framework
14	Chukwuere, J. E.	2022	Social media and COVID-19 pandemic: A systematic literature review.	Long-life learning and cybersecurity threats
15	De Silva, B.	2023	Exploring the relationship between cybersecurity culture and cyber-crime prevention: A systematic review.	Cybersecurity culture
16	Essa, S. G., Celik, T., and Human-Hendricks, N. E.	2023	Personalized adaptive learning technologies based on machine learning techniques to identify learning styles.	Cybersecurity education and awareness
17	Hatzivasilis et al.	2021	The threat-arrest cyber range platform.	Cybersecurity resilience
18	Hussain et al.	2024	Cybersecurity education: enhancing cybersecurity capabilities, navigating trends and challenges in a dynamic landscape.	Cybersecurity trends and challenges
19	Kayode-Ajala, O.	2023	Establishing cyber resilience in developing countries.	Institutional, legal, financial and social challenges related to cyber issues
20	Kagita et al.	2022	A review on cybercrimes on the internet of things.	Deep learning for security and privacy preservation
21	Karhu, A.	2021	Mapping study of MOOC providers: the current state of computer science education and platform technical capabilities.	Cybersecurity education
22	Kavak et al.	2021	Simulation for cybersecurity: state of the art and future directions	Cybersecurity simulations
23	Khan, M. A., Khan, S. M., and Subramaniam, S. K.	2023	A systematic literature review on security issues in cloud computing using edge computing and blockchain.	Cybersecurity issues on computing
24	Li, Y., and Liu, Q.	2021	A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments.	Cybersecurity education and reflection
25	Macías, Z. L. V., Hernández, A. A. R., and Saenz, C. L. S.	2020	Digital games (Gamification) in learning and training: An approach to adaptation and integration in the classroom.	Cybersecurity training and awareness
26	Mukherjee et al.	2024	Strategic approaches to cybersecurity learning: A study of educational models and outcomes.	Cybersecurity strategies
27	Nandan, A. B.	2021	Cybercrimes and Its Alarming Escalation during Recent Times	Cybersecurity threats
28	Ncubukezi, T., 2022,	2022	Human errors: A cybersecurity concern and the weakest link to small businesses.	Cybersecurity lifelong learning and awareness
29	Ošlejšek et al.	2020	Conceptual model of visual analytics for hands-on cybersecurity training.	Cybersecurity training
30	Quader, F., and Janeja, V. P.	2021	Insights into organizational security readiness: Lessons learned from cyber-attack case studies.	Cybersecurity education and reflection
31	Qudus, L.	2025	Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges.	Cybersecurity governance
32	ThankGod, J.	2024	Public-Private Partnerships in Strengthening Cybersecurity for International Trade	Collaboration and learning
33	Towhidi, G., and Pridmore, J.	2023	Aligning cybersecurity in higher education with industry needs.	Cybersecurity lifelong learning
34	Reed, S. S., Mullen, C. A., and Boyles, E. T.	2020	Bringing problem-based learning to elementary schools to benefit children's readiness for a global world.	Cybersecurity education
35	Sarker, I. H.	2023	Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects.	Behavioural learning and cybersecurity education
36	Schoenmakers et al.	2023	The security mindset: characteristics, development, and consequences.	Cybersecurity mindset
37	Shillair et al.	2022	Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise.	Raising cybersecurity and awareness

Table 1-A1 continues on the next page →

TABLE 1-A1 (Continues…): Systematic literature review: Summary of selected articles.

No.	Author(s)	Year	Title	Key findings / Contribution
38	Stavrou, E., and Piki, A.	2024	Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity.	Upskilling in cybersecurity
39	Sulaiman et al.	2022	Cybersecurity behaviour among government employees: the role of protection motivation theory and responsibility in mitigating cyberattacks.	Understanding motivation theory in mitigation of cyber-attacks
40	Thakur, M.	2024	Cyber security threats and countermeasures in digital age.	Cybersecurity threats
41	Tranfield, D., Denyer, D., and Smart, P.	2023	Towards a methodology for developing evidence-informed management knowledge by means of systematic review.	The development of cybersecurity methodologies
42	Victor-Mgbachi, T.	2024	Navigating cybersecurity beyond compliance: understanding your threat landscape and vulnerabilities.	Challenges of cybersecurity and understanding the threat landscape
43	Willie, M. M.	2023	The role of organizational culture in cybersecurity.	Cybersecurity culture
44	Yaacoub et al.	2020	Cyber-physical systems security.	Limitations, issues and future trends cyber-attacks
45	Yamin, M. M., Katt, B., and Nowostawski, M.	2021	Serious games as a tool to model attack and defence scenarios for cyber-security exercises.	Modelling cyber-attack and cyber defence
46	Zhang et al.	2021	Cybersecurity awareness training programs: a cost–benefit analysis framework.	Cybersecurity training and awareness

Note: Please see the full reference list of this article, Sandi, S. & Van den Berg, C.L., 2025, 'Cybersecurity mindset and upskilling: Resilience via lifelong learning and security education', *South African Journal of Information Management* 27(1), a2044. https://doi.org/10.4102/sajim.v27i1.2044, for more information.