Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model

Tapiwa Gundu
Nelson Mandela University, Centre of Research in Information and Cyber Security (CRICS), Gqeberha, South Africa

tapiwag@mandela.ac.za

Abstract: In the ever-evolving cyberspace landscape, organisations face persistent threats that continuously mutate and adapt. To effectively defend against these dynamic cyber threats, a fundamental shift in cybersecurity culture is imperative. This paper presents a novel Adaptive Cybersecurity Culture Model (ACCM) that encapsulates the principles of "Learn, Unlearn, and Relearn" as a strategic stance to foster resilience and adaptability in the face of evolving cyber threats. The ACCM emphasizes the importance of continuous learning as the cornerstone of cybersecurity culture. It advocates the adoption of a growth mindset within organisations, encouraging employees to stay updated with emerging threats, technologies, and best practices. However, the model goes beyond mere learning; it underscores the significance of unlearning outdated practices and misconceptions that may hinder effective cybersecurity. Furthermore, the ACC model introduces the concept of "Relearn," emphasizing the need to rapidly adapt and evolve strategies and tactics in response to ever-changing cyber threats. It promotes a culture of agility and adaptability, enabling organisations to respond effectively to both known and unforeseen cyber challenges. The model presented in this paper draws from case studies of various industries to illustrate the successful adoption and transformation of cybersecurity culture using the Learn, Unlearn, and Relearn principles. The ACCM represents a paradigm shift in cybersecurity culture, acknowledging that the ability to adapt is as critical as the ability to protect. By fostering a culture of continuous learning, unlearning, and relearning, organisations can proactively enhance their cyber resilience and effectively defend against the ever-evolving cyber threat landscape. This paper provides a roadmap for organisations to embark on this transformative journey toward a more adaptive and resilient cybersecurity culture.

Keywords: Cybersecurity culture, Adaptive cybersecurity, Learn, Unlearn, Relearn, Cyber threat resilience, Growth mindset, Continuous learning

1. Introduction

Cybersecurity has become a paramount concern in the digital age due to the increasing dependence on digital technologies and the proliferation of interconnected systems (Gundu, 2023a). The rapid growth of the internet, cloud computing, mobile devices, and Internet of Things (IoT) has brought about unprecedented opportunities for innovation, communication, and convenience (Gundu et al., 2019). However, it has also given rise to a host of complex and evolving cyber threats that pose significant risks to individuals, organisations, and even nations (Craig, 2018). The digital age is characterized by a widespread transformation of various sectors, including finance, healthcare, energy, transportation, and communication. This transformation is driven by the adoption of digital technologies, data-driven decision-making, and the interconnectivity of devices and systems (Jin et al., 2023). While this connectivity enhances efficiency and accessibility, it also exposes critical assets and sensitive information to potential cyberattacks (Gundu, 2023b).

Massive data breaches have become common place, compromising the personal and financial information of millions of individuals (Madan et al., 2023). High-profile incidents involving renowned companies (e.g. T Mobile, Chat GPT, MailChimp, Google Fi, etc) have underscored the urgent need for robust cybersecurity measures (Farrelly, 2023). Additionally, concerns about data privacy, surveillance, and the misuse of personal information have led to the development of stringent data protection regulations, such as the European Union's General Data Protection Regulation (GDPR) (Team, 2020), the California Consumer Privacy Act (CCPA) (Wong et al., 2023) or South African Protection of Personal Information Act (POPIA) (Netshakhuma, 2019). The consequences of cyberattacks extend beyond immediate financial losses. Cyber incidents can disrupt critical infrastructure, disrupt supply chains, and result in the loss of intellectual property (Mmango & Gundu, 2023).

As technology advances, so do the tactics, techniques, and procedures of cybercriminals, hacktivists, state-sponsored actors, and other malicious entities. The threat landscape has evolved beyond traditional viruses and malware to include sophisticated attacks such as ransomware, advanced persistent threats (APTs), social engineering, and zero-day exploits (Anisetti et al., 2020; Rahman et al., 2023; Schiller et al., 2022). The ever-changing threat landscape and evolving nature of cybersecurity challenges faced by organisations in the digital realm are evident and can be seen by the continuous mutation and adaption of the threats presenting a moving target for cybersecurity defences. This dynamic environment is characterized by the rapid development of new attack techniques, exploitation methods, and vulnerabilities. Cyber adversaries constantly innovate and modify their tactics to bypass existing security measures, making it essential for organisations to stay vigilant and

responsive. The ever-changing threat landscape underscores the need for a proactive and adaptive cybersecurity culture that goes beyond static defences, emphasizing continuous monitoring, learning, and adjustment to effectively counter emerging cyber threats.

Cybersecurity culture refers to the shared values, beliefs, attitudes, behaviours, and practices within an organisation that collectively shape its approach to information security. Cybersecurity culture plays a pivotal role in determining how an organisation perceives, prioritises, and addresses security issues. A strong cybersecurity culture should foster a proactive and security-conscious mindset among employees at all levels, encouraging them to consider security in their day-to-day activities. It involves creating an environment where individuals understand the importance of protecting sensitive information, recognise potential security risks, and actively contribute to maintaining a secure digital ecosystem. A positive cybersecurity culture promotes awareness, accountability, and a commitment to best practices, ensuring that security measures are not just seen as technical requirements but as integral components of the overall organisational ethos. Cultivating a cybersecurity culture involves leadership commitment, continuous education, clear communication, and the integration of security considerations into the organisation's policies and processes. Given the high stakes associated with cyber threats, a robust cybersecurity culture is instrumental in fortifying an organisation's defences against the ever-evolving landscape of cyber threats.

The objectives of this study are to address the critical need for a paradigm shift in cybersecurity culture within organisations, given the persistent and ever-evolving threats in cyberspace. The primary goal is to introduce and elucidate a novel model, the Adaptive Cybersecurity Culture Model (ACCM), built on the principles of "Learn, Unlearn, and Relearn." This model aims to serve as a strategic baseline for fostering resilience and adaptability in the face of dynamic cyber threats. The study seeks to emphasize the significance of continuous learning as the foundation of a robust cybersecurity culture, advocating for a growth mindset among employees to stay abreast of emerging threats, technologies, and best practices. Furthermore, the study aims to highlight the importance of unlearning outdated practices and misconceptions that may hinder effective cybersecurity measures. The concept of "Relearn" is introduced to underscore the need for organisations to rapidly adapt and evolve strategies in response to ever-changing cyber threats.

2. Related Literature

2.1 Evolution of Cyber Threats and Their Impact on Traditional Security Practices

The evolution of threat vectors in the realm of cybersecurity reflects the dynamic nature of the digital landscape and the continuous innovation by malicious actors seeking to exploit vulnerabilities (Anisetti et al., 2020). Initially, cybersecurity threats were primarily virus and malware-driven, often spread through infected files or email attachments. As technology advanced, so did the threat vectors, with the emergence of more sophisticated tactics such as phishing, where attackers manipulate individuals into divulging sensitive information (Rahman et al., 2023). The rise of interconnected systems and the Internet of Things (IoT) introduced new threat vectors, allowing attackers to exploit vulnerabilities in interconnected devices and networks (Gundu & Maronga, 2019). Social engineering became increasingly prevalent, leveraging psychological manipulation to deceive individuals or gain unauthorized access (Kilavo et al., 2023). Advanced Persistent Threats (APTs) marked another shift, involving prolonged and targeted attacks for data exfiltration or system compromise (Quintero-Bonilla & Martín del Rey, 2020). With the expansion of cloud computing and mobile technologies, threats evolved to exploit weaknesses in these platforms. Additionally, the use of artificial intelligence and machine learning by both defenders and attackers added a layer of complexity to the threat landscape (Taddeo et al., 2019). As technologies like 5G, edge computing, and quantum computing emerge, the evolution of threat vectors continues, requiring cybersecurity strategies to adapt to these advancements and anticipate future challenges. The ongoing evolution underscores the importance of proactive measures, a holistic cybersecurity approach and continuous vigilance by employees (Sun et al., 2023).

2.2 Employees - The Weakest Link

Employees are often considered the weakest link in cybersecurity, highlighting the vulnerabilities introduced by their behaviours, actions, and decisions within the organisations digital environment (Thomson et al., 2006). Despite advancements in technology and sophisticated cybersecurity measures, employees remain susceptible to various cyber threats (Zimmermann & Renaud, 2019). Employee-related vulnerabilities manifest in actions such as falling victim to phishing attacks, using predictable passphrases, neglecting software updates, or unintentionally disclosing sensitive information. One key reason for this vulnerability is the lack of awareness about cybersecurity risks and best practices (Zwilling et al., 2022). Many individuals may not fully comprehend

the potential consequences of their actions in the digital realm, leading to inadvertent security lapses (Moustafa et al., 2021). Cybercriminals often exploit this lack of awareness through social engineering tactics, such as tricking individuals into clicking malicious links or sharing confidential information (Thomson & Niekerk, 2018).

Building cybersecurity awareness is crucial to mitigating the human factor as a weak link (Zwilling et al., 2022). Education and training programs can empower individuals to recognize and respond to cyber threats effectively. This includes understanding the tactics employed by cybercriminals, recognizing phishing attempts, and adopting secure online practices. Awareness efforts should also emphasize the importance of maintaining strong passphrases, use of onetime pins, regularly updating software, and exercising caution in online interactions. However, most information security awareness programs only place strong emphasis on learning new practices, strategies, and skills to enhance an individual's ability to safeguard digital assets and sensitive data neglecting a crucial aspect of unlearning outdated or ineffective security practices (Hielscher et al., 2022).

2.3 The Concept of Unlearning and Relearning in Information Security Awareness and Training Contexts

In the context of information security awareness and training, the concepts of unlearning and relearning play crucial roles in adapting to the ever-evolving cybersecurity landscape. Unlearning involves letting go of outdated practices, misconceptions, or habits that may pose security risks (Zhao & Wang, 2020). In the rapidly changing field of information security, clinging to outdated knowledge or approaches can be detrimental. Therefore, individuals need to actively unlearn practices that may have been effective in the past but are no longer sufficient in addressing current cybersecurity threats.

Relearning, on the other hand, emphasizes the continuous acquisition of new knowledge and skills to stay abreast of emerging threats and technologies (Zhao & Wang, 2020). Cybersecurity is a dynamic field, and what may be considered best practices today might become obsolete tomorrow. Relearning involves staying proactive, seeking out the latest information on cybersecurity threats, tools, and strategies, and adapting one's knowledge base to effectively counter new and sophisticated challenges.

Awareness campaigns should not only focus on imparting foundational knowledge but also encourage participants to question existing practices, discard obsolete methodologies, and adopt new and more effective security measures (Sharma & Lenka, 2019). This involves creating a culture of agility and adaptability, where individuals are empowered to evolve their understanding of cybersecurity in response to the rapidly changing threat landscape. Moreover, case studies and real-world examples of security breaches can serve as powerful tools for unlearning and relearning. Analysing past incidents allows individuals to understand the consequences of outdated security practices and reinforces the importance of staying current with the latest cybersecurity trends.

2.4 Adaptive Cybersecurity

Adaptive cybersecurity involves the continuous process of adjusting and evolving cybersecurity strategies, practices, and technologies to effectively counter new and emerging threats (Addae et al., 2017). Unlearning and relearning play a pivotal role in achieving adaptive cybersecurity by addressing outdated practices and acquiring new knowledge and skills. For ease of adaptive learning, people should possess cognitive skills, these involve the mental capacity to switch between different concepts, perspectives, or strategies in response to changing situations (Caulkins et al., 2019).

2.5 Cognitive Flexibility and its Relevance to Adaptive Cybersecurity

Cognitive flexibility refers to the ability of employees to mentally adapt, shift perspectives, and adjust their thinking to effectively respond to evolving cyber threats. It is a cognitive skill that enables employees to navigate the complex and dynamic nature of the cybersecurity landscape .Cognitive flexibility enables the employees to adapt to new information, think creatively, and solve complex problems (Caulkins et al., 2019). They can shift their focus and strategies to address emerging threats without being constrained by rigid mindsets or established practices.

In an ever-changing cyber landscape, cognitive flexibility enables professionals to identify anomalies and patterns that may indicate a potential attack (Ask et al., 2023). Cyber threats are often not straightforward and may involve complex, non-obvious indicators. During a cyber incident, the ability to switch between different response strategies and adapt to the changing nature of the attack is crucial. Cognitive flexibility helps cybersecurity teams quickly assess the situation, determine the appropriate course of action, and adjust their response as needed.

Ultimately, cognitive flexibility supports a culture of continuous learning and improvement within cybersecurity teams (Caulkins et al., 2019). Professionals who can readily unlearn outdated practices and relearn new ones contribute to the organisation's ability to stay ahead of emerging threats.

2.6 Factors Contributing to the Persistence of Outdated Practices

The persistence of outdated security practices within organisations can be attributed to a combination of factors. Key contributing factors include cognitive inertia, as people tend to resist change and may be reluctant to unlearn outdated practices; lack of awareness about the rapid evolution of cyber threats; resource constraints, with limited budgets hindering investments in new technologies; organisational culture favouring tradition over innovation; misaligned incentives when individuals are unaffected by outdated practices; fear of disruption during the transition to new practices; compliance-driven decision-making that can impede adaptive change; a lack of training and skill development; the perception of low risk in the absence of significant incidents; unclear communication about the urgency of updating security practices; a short-term focus prioritizing immediate tasks over long-term cybersecurity preparedness; and the challenge of legacy systems and dependencies. Overcoming these factors necessitates a comprehensive approach involving effective communication, education, leadership support, incentivisation, and a cultural shift towards adaptability and innovation, enabling organizations to successfully unlearn outdated practices and embrace the principles of adaptive cybersecurity.

2.7 Risks Associated With Clinging to Obsolete Security Practices

Clinging to outdated cybersecurity practices poses numerous risks and adverse consequences for organisations. Such practices increase vulnerability to emerging threats, leaving organizations exposed to modern attack techniques and advanced persistent threats (Sharma & Lenka, 2019). Ineffective threat detection and response capabilities may result in delayed incident responses and prolonged unauthorized access. This can lead to data breaches, compromising sensitive information and exposing organizations to legal consequences and non-compliance with data protection regulations. Cybersecurity incidents stemming from obsolete practices can disrupt business operations, impact revenue, and harm customer trust and loyalty. Moreover, organizations adhering to outdated practices may hinder innovation and competitiveness, impacting employee morale, productivity, and the ability to attract and retain skilled cybersecurity professionals (Zhao & Wang, 2020). To mitigate these risks, organizations must prioritize the adoption of adaptive cybersecurity practices that align with current threat trends, leverage modern technologies, and promote a culture of continuous learning and improvement.

3. The Proposed Model

The Adaptive Cybersecurity Culture Model is cyclical, emphasizing that cybersecurity environment should not be, instead, it requires a continuous, dynamic, and iterative process. The model acknowledges that learning is not enough; unlearning outdated practices and relearning in response to evolving threats are equally critical components of a robust cybersecurity culture. This iterative process ensures that organizations are not only prepared for current threats but also adaptive to future challenges in the ever-changing cybersecurity landscape.

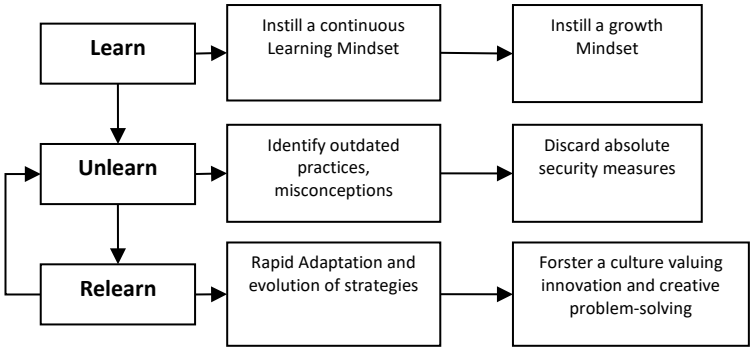

Figure 1: Adaptive Cybersecurity Culture Model

3.1 Learn

Continuous Learning: The "Learn" component emphasizes the importance of ongoing education and development in the field of cybersecurity. This involves implementing regular training programs, workshops, and

educational sessions to ensure that cybersecurity professionals stay informed about the latest threats, technologies, and best practices.

Growth Mindset: Encouraging a growth mindset within the organization is crucial. This mindset fosters the belief that skills and intelligence can be developed through dedication and hard work. In the context of cybersecurity, it motivates individuals to embrace challenges, learn from failures, and seek opportunities for improvement.

3.2 Unlearn

Identify Outdated Practices: The "Unlearn" component involves recognizing and acknowledging practices, methodologies, or beliefs that have become outdated or ineffective in the face of evolving cyber threats. This step requires a critical assessment of existing security measures to identify areas that need to be revamped or abandoned.

Willingness to Let Go: Unlearning is not just about recognizing outdated practices but also about fostering a culture where individuals are willing to let go of established habits or approaches that may no longer contribute to effective cybersecurity. It involves overcoming resistance to change and embracing new and improved strategies.

3.3 Relearn

Rapid Adaptation: In the "Relearn" phase, organizations focus on the ability to rapidly adapt and evolve their cybersecurity strategies in response to changing threats. This requires a proactive approach to adjusting security measures, staying ahead of emerging risks, and implementing timely updates to defences.

Foster a Culture of Innovation: Relearning emphasizes fostering a culture that values innovation and creative problem-solving. It encourages cybersecurity professionals to think outside the box, explore new approaches, and continuously improve strategies based on real-world experiences and feedback.

Continuous Improvement: Implementing feedback loops is crucial for continuous improvement. This involves regularly evaluating the effectiveness of security measures, learning from incidents or breaches, and making iterative adjustments to enhance overall cybersecurity posture.

4. Discussion

Relearning new techniques is a crucial component of the Adaptive Cybersecurity Culture Model, involving the continuous acquisition and mastery of updated knowledge, skills, and practices to effectively counter evolving cyber threats. In the dynamic landscape of cybersecurity, keeping abreast of the latest techniques is imperative for maintaining a robust defence against rapidly changing attack vectors and vulnerabilities. One area of focus within adaptive cybersecurity involves emerging employee-related trends and techniques that address the human element of cybersecurity. These strategies acknowledge that employees are both targets and potential vulnerabilities, aiming to enhance user awareness, behaviour, and overall cyber hygiene. Noteworthy trends include the use of behavioural analytics and user profiling to detect anomalies, phishing simulation and testing to assess employees' recognition of social engineering attempts, and continuous user authentication methods like biometrics and multi-factor authentication. Other approaches encompass insider threat detection, secure remote work practices, threat deception, and employee-centric incident response plans. Additionally, organisations should foster cybersecurity cultures that integrate security into daily operations, utilising tailored training, microlearning, ethical hacking programs, and security champions to enhance overall cybersecurity awareness. Recognising the emotional and psychological factors influencing user behaviour, these trends collectively contribute to a more resilient cybersecurity posture, reducing the likelihood of successful cyberattacks stemming from employee vulnerabilities.

Strategies for acquiring new knowledge and skills in cybersecurity are multifaceted and essential for employees to navigate the rapidly evolving landscape of cyber threats. A foundational approach involves the increasing investment in comprehensive security awareness training programs, designed to educate employees about common cyber threats, phishing tactics, and safe online practices, thereby minimizing the risk of errors. An innovative strategy employs gamification for training, integrating gaming elements into cybersecurity education to make the learning process engaging, foster active participation, and enhance knowledge retention among employees. Additionally, efforts are being made to make cybersecurity education more inclusive, addressing diverse learning styles, backgrounds, and abilities. Embracing a continuous learning mindset is emphasized, recognizing the dynamic nature of the cybersecurity field, encouraging individuals to stay proactive in updating their knowledge and skills to align with the latest industry developments. Versatile approaches include enrolling

in online courses, tutorials, and e-learning platforms offered by websites like Coursera, edX, Udemy, and Khan Academy, covering a wide array of cybersecurity topics. Pursuing recognized professional certifications such as CompTIA Security+, CISSP, CEH, or CCSP remains a cornerstone for skill acquisition. Seeking mentorship from experienced professionals, following cybersecurity blogs and podcasts, and cultivating curiosity to explore new topics further contribute to a comprehensive and adaptive framework for acquiring and honing cybersecurity knowledge and skills.

In the pursuit of an adaptive cybersecurity culture, organizations must instill a mindset of unlearning and relearning. Key strategies for fostering such a culture include securing leadership support and buy-in, where organizational leaders play a pivotal role in endorsing continuous learning and motivating employees to discard outdated practices for embracing new knowledge (Thomson et al., 2006). Clear communication and awareness campaigns are essential to underscore the imperative of unlearning and relearning (Bada et al., 2019), emphasizing the rapidly changing nature of cybersecurity threats and the inherent benefits of staying current. Creating diverse learning opportunities through regular training, workshops, and access to educational resources, along with hands-on practice and experimentation, equips employees with the skills needed to adapt to evolving challenges (Anisetti et al., 2020). Leading by example, wherein organizational leadership openly discusses their commitment to ongoing learning, sets a positive precedent for employees to follow suit. Recognizing and rewarding active participation in learning initiatives (Gundu et al., 2019), as well as incorporating learning into performance evaluations, further reinforces the importance of continuous skill development. Encouraging cross-functional collaboration, providing channels for feedback and reflection, and establishing a safe environment for experimentation are additional strategies. Recognising changing paradigms, promoting self-directed learning, and utilizing case studies and lessons learned contribute to a comprehensive approach. Ensuring inclusivity in learning programs, celebrating learning achievements, and fostering a long-term outlook on unlearning and relearning as continuous processes are integral components of creating a culture where adapting to new challenges is not only encouraged but celebrated. Ultimately, these strategies collectively form the foundation for achieving and maintaining excellence in cybersecurity and other dynamic fields.

5. Conclusion

In conclusion, this paper introduces an Adaptive Cybersecurity Culture Model (ACCM) to effectively combat the ever-evolving landscape of cyber threats. ACCM is grounded in the principles of "Learn, Unlearn, and Relearn," emphasising the continuous pursuit of knowledge, shedding outdated practices, and swiftly adapting to emerging threats. The strategies outlined for cultivating this culture encompass leadership support, clear communication, diverse learning opportunities, and recognition of employees' active participation. By fostering a culture that embraces ongoing learning and adaptation, organizations can bolster their resilience and responsiveness in the face of dynamic cybersecurity challenges. The recognition of human factors as central to cybersecurity, the acknowledgment of the need to unlearn outdated practices, and the promotion of a long-term perspective on continuous learning form the cornerstone of this transformative journey. The roadmap provided in this paper serves as a guide for organisations embarking on this transformative journey, fostering a culture where the ability to adapt is recognised as equally critical as the ability to protect. Ultimately, ACCM represents a paradigm shift, acknowledging that cybersecurity excellence is not a static state but an ongoing, dynamic process of learning, unlearning, and relearning.

Proposed future research directions encompass a range of promising avenues, notably the integration of advanced technologies such as artificial intelligence and machine learning. An emphasis is placed on evaluating the potential of these technologies in automating threat analysis and fortifying defence mechanisms. Additionally, the proposed future research could be around the development of quantitative metrics to measure the effectiveness of adaptive cybersecurity, aiming to furnish an objective evaluation of employee preparedness for paradigm shift.

References

Addae, J. H., Brown, M., Sun, X., Towey, D., & Radenkovic, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. *Information and Computer Security*, *25*(5), 560–579. https://doi.org/10.1108/ICS-11-2016-0085

Anisetti, M., Ardagna, C., Cremonini, M., Sessa, J., & Costa, L. (2020). Security Threat Landscape. *Security Threats*.

Ask, T. F., Lugo, R., Fritschi, J., Veng, K., Eck, J., Özmen, M.-T., Bärreiter, B., Knox, B. J., & Sütterlin, S. (2023). *The role of cognitive styles and cognitive flexibility in deepfake detection skills and metacognitive accuracy*.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv Preprint arXiv:1901.02672*.

Caulkins, B., Marlowe, T., & Reardon, A. (2019). Cybersecurity Skills to Address Today's Threats. In T. Z. Ahram & D. Nicholson (Eds.), *Advances in Human Factors in Cybersecurity* (pp. 187–192). Springer International Publishing.

Craig, J. (2018). Cybersecurity Research—Essential to a Successful Digital Future. *Engineering*, *4*(1), 9–10. https://doi.org/10.1016/j.eng.2018.02.006

Farrelly, J. (2023, October 10). *High-Profile Company Data Breaches 2023*. Electric. https://www.electric.ai/blog/recent-big-company-data-breaches

Gundu, T. (2023a). Chatbots: A Framework for Improving Information Security Behaviours using ChatGPT. In S. Furnell & N. Clarke (Eds.), *Human Aspects of Information Security and Assurance* (pp. 418–431). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-38530-8_33

Gundu, T. (2023b). Internet Of Things: Sensor Layer Security Risk Mitigation Framework. *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1–8. https://doi.org/10.1109/ICECET58911.2023.10389252

Gundu, T., Maronga, M. I., & Boucher, D. (2019). Industry 4.0 Business Perspective: Fostering a Cyber Security Culture in a Culturally Diverse Workplace. *Proceedings of 4th International Conference on The*, *12*, 85–94.

Gundu, T., & Maronga, V. (2019). IoT Security and Privacy: Turning on the Human Firewall in Smart Farming. *Kalpa Publications in Computing*, *12*, 95–104. https://doi.org/10.29007/j2z7

Hielscher, J., Kluge, A., Menges, U., & Sasse, M. A. (2022). "Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting. *Proceedings of the 2021 New Security Paradigms Workshop*, 108–122. https://doi.org/10.1145/3498891.3498902

Jin, C., Xu, A., Zhu, Y., & Li, J. (2023). Technology growth in the digital age: Evidence from China. *Technological Forecasting and Social Change*, *187*, 122221. https://doi.org/10.1016/j.techfore.2022.122221

Kilavo, H., J. Mselle, L., I. Rais, R., & Mrutu, S. I. (2023). Reverse Social Engineering to Counter Social Engineering in Mobile Money Theft: A Tanzanian Context. *Journal of Applied Security Research*, *18*(3), 546–558. https://doi.org/10.1080/19361610.2022.2031702

Madan, S., Savani, K., & Katsikeas, C. S. (2023). Privacy please: Power distance and people's responses to data breaches across countries. *Journal of International Business Studies*, *54*(4), 731–754. https://doi.org/10.1057/s41267-022-00519-5

Mmango, N., & Gundu, T. (2023). Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs. *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1–6. https://doi.org/10.1109/ICECET58911.2023.10389226

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, *12*. https://www.frontiersin.org/articles/10.3389/fpsyg.2021.561011

Netshakhuma, N. S. (2019). Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA). *Global Knowledge, Memory and Communication*, *69*(1/2), 58–74. https://doi.org/10.1108/GKMC-02-2019-0026

Quintero-Bonilla, S., & Martín del Rey, A. (2020). A New Proposal on the Advanced Persistent Threat: A Survey. *Applied Sciences*, *10*(11), Article 11. https://doi.org/10.3390/app10113874

Rahman, M. R., Mahdavi-Hezaveh, R., & Williams, L. (2023). What are the attackers doing now? Automating cyber threat intelligence extraction from text on pace with the changing threat landscape: A survey. *ACM Computing Surveys*, *55*(12), 1–36. https://doi.org/10.1145/3571726

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

Sharma, S., & Lenka, U. (2019). Exploring linkages between unlearning and relearning in organizations. *The Learning Organization*, *26*(5), 500–517. https://doi.org/10.1108/TLO-10-2018-0164

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials*, *25*(3), 1748–1774. https://doi.org/10.1109/COMST.2023.3273282

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), Article 12. https://doi.org/10.1038/s42256-019-0109-1

Team, I. G. P. (2020). *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition*. IT Governance Ltd.

Thomson, K.-L., & Niekerk, J. van. (2018). Towards Culturally Sensitive Policy: Africanising Approaches to Prevent Social Engineering. *Advanced Science Letters*, *24*(4), 2499–2503. https://doi.org/10.1166/asl.2018.10990

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11.

Wong, R. Y., Chong, A., & Aspegren, R. C. (2023). Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW1), 82:1-82:26. https://doi.org/10.1145/3579515

Zhao, Y., & Wang, X. (2020). Organisational unlearning, relearning and strategic flexibility: From the perspective of updating routines and knowledge. *Technology Analysis & Strategic Management*, *32*(11), 1251–1263. https://doi.org/10.1080/09537325.2020.1758656

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97.