The MTNK Platform for Making Cybersecurity Accessible to SMEs

Francesca Igini[1,2,*], Francesco Greco[3,*], Samuele Lupidi[4], Sara Chimienti[1] and Flaminia Del Conte[4]

[1]Seedble S.r.l., Rome, Italy
[2]Sapienza University of Rome, Italy
[3]University of Bari, Via Orabona 4, 70125 Bari, Italy
[4]Hackable S.r.l., Rome, Italy

Abstract

Small and medium-sized enterprises (SMEs) face increasingly sophisticated cyber threats, while often being constrained by limited resources in the implementation of robust security measures. This paper presents MTNK, an integrated platform that aims to improve the resilience of companies on cybersecurity and foster technological innovation in SMEs. The modular architecture of MTNK —consisting of the Learn, Ecosystem, Technology radar, Challenge, and Crowdsourcing modules— can address socio-technical security gaps, facilitate the adoption of new technologies and foster a collaborative cybersecurity ecosystem. Notably, in this work we present the "Learn" module and its two distinct learning paths: the Cybersecurity Awareness course, designed for employees of any technology expertise level, and the Cybersecurity Advanced course, designed for IT operators with limited cybersecurity expertise within SMEs. Key challenges are also explored, including barriers to adoption, scalability constraints and data security considerations

Keywords

Small and medium-sized enterprises, Training, Learning, Cybersecurity, Employees

1. Introduction

The global rise in cyberattacks has created an increasingly challenging digital environment for businesses of all sizes [1, 2]. Cybercrime damages are expected to reach $10.5 trillion annually by the end of 2025, making it the third-largest economy globally if measured as a country [3]. This growth in cyber threats is also driven by advancements in artificial intelligence, rapid digitalization, and the increasing sophistication of attack methods such as ransomware and phishing [4, 5]. For instance, ransomware attacks grew by 67% in 2023, while phishing attempts rose by 58% [6]. If successful, these attacks can lead to a data breach, which costs almost $5 million in average [4] to the attacked company. This cost is often unbearable in the case of small and medium-sized enterprises (SMEs), which risk closing down within 6 months from the attack [7]. In addition to direct financial losses, these vulnerabilities can disrupt operations and business continuity, and damage the company's reputation.

As the costs associated with cyberattacks are rising, also the financial burden of cybersecurity is escalating rapidly. Spending on information security and risk management products and training is expected to grow by about 15% compared to 2024, reaching $212 billion by the end of 2025 [8]. Despite this increased investment, many organizations struggle to keep pace with the evolving threat landscape. Together with the shortage of qualified cybersecurity experts [9], this creates a challenging scenario for businesses, particularly SMEs, which often lack the resources to allocate significant budgets toward cybersecurity.

SMEs are indeed disproportionately affected by these challenges due to their limited financial and technical resources [6]: these often lack access to advanced security solutions and skilled personnel,

Joint Proceedings of IS-EUD 2025: 10th International Symposium on End-User Development, 16-18 June 2025, Munich, Germany.
*Corresponding author.
francesca.igini@seedble.com (F. Igini); francesco.greco@uniba.it (F. Greco); samuele.lupidi@seedble.com (S. Lupidi); sara.chimienti@seedble.com (S. Chimienti); flaminia.delconte@seedble.com (F. D. Conte)
0009-0004-9365-996X (F. Igini); 0000-0003-2730-7697 (F. Greco); 0009-0005-6911-0747 (S. Lupidi)

making them preferred targets for cybercriminals. SMEs are more likely to face unique vulnerabilities, like outdated IT infrastructure and insufficient incident response protocols, which increase their exposure to cyberattacks.

Increasing these risks are the issues of growing technical debt and low digital literacy among employees. Technical debt arises when businesses prioritize short-term solutions over long-term IT best practices, leading to unpatched systems and inadequate security measures [10]. Low digital literacy also negatively impacts the cybersecurity behavior of employees [11] and often leads to human error, which is the main common cause of data breaches [12]. Cybersecurity training programs —for example simulated phishing campaigns— are very costly for companies [13], but they are not always effective [14]. To be effective, the training content should be designed to be both highly engaging and appealing to employees while remaining concise and easily digestible [15, 16, 17].

Given this challenging context, the **MTNK** platform offers a tailored solution for Italian SMEs, which comprise 99% of the country's businesses, to address their unique cybersecurity challenges. The MTNK platform, thanks to its modular structure, empowers users with an ecosystem of tools, able to address various cybersecurity needs and challenges in a coordinated manner. Spanning from education of the personnel, through the application of the proper innovative technologies to a company's IT system, MTNK has different modules ready to set a holistic cybersecurity strategy. By providing accessible and effective cybersecurity measures, MTNK aims to empower Italian SMEs to strengthen their defenses against evolving threats in a cost-effective manner.

The paper continues as follows: Section 2 presents MTNK, the cybersecurity platform developed for Italian SMEs. Section 3 details the learning module of MTNK. Section 4 presents the discussions about the potential benefits and limitation of adopting the platform. Section 5 discusses future works and concludes the paper.

2. MTNK: a comprehensive cybersecurity platform for SMEs

MTNK (named after the renowned hacker Kevin Mitnick) is a comprehensive cybersecurity platform tailored for small and medium-sized enterprises (SMEs)[1].

To develop the platform, a preliminary market analysis was conducted to assess the presence of similar tools in the context of cybersecurity for SMEs in Italy. The analysis led to identifying three main cybersecurity e-learning platforms: *Cyber Guru*[2] focuses on human risk reduction through continuous cognitive and experiential training, leveraging gamification, micro-learning, and AI-driven simulations, and is notably accredited by Italy's national cybersecurity agency. Swascan's *Cyber E-learning*[3] offers a more accessible, base-level approach with interactive slides, cartoon-format video tips, and ongoing content updates aimed at making learning engaging and easy to digest. Finally, *CyberBrain*[4] utilizes AI to tailor training programs to individual employee levels, includes regular attack simulations, and ensures compliance with mandatory cybersecurity training standards, all while requiring minimal time commitment. However, the main problem with these platforms is that they either focus exclusively on training (like Cyber Guru) or only provide training on a basic level (like Cyber E-learning and CyberBrain).

After this preliminary analysis, a deeper analysis was conducted, which included interviewing some firms that face cybersecurity-related challenges on a daily basis. Notably, five different companies (names are omitted for anonymity purposes) were chosen with a convenience sampling method for conducting semi-structured interviews to understand their needs in the cybersecurity context. It emerged that, within their organizations, there is a need for a comprehensive platform that improves the cybersecurity posture of their company on the technical and human side.

Therefore, MTNK offers a suite of innovative tools designed to assess and safeguard the overall

[1] https://www.mtnk.io/
[2] https://www.cyberguru.it/cyber-guru-training-platform/
[3] https://www.swascan.com/cyber-academy/
[4] https://www.cyberbrain.it/awareness-FormazioneCyber

cybersecurity posture of companies. The platform provides a structured framework that integrates cybersecurity education, expert collaboration, technology discovery, and collaborative innovation. Its core modules —*Learn, Ecosystem, Tech Radar, Challenge*, and *Crowdsourcing*— each target distinct aspects of cybersecurity, from raising awareness and engaging experts to scouting emerging technologies and fostering innovation. Figure 1 presents the platform's modular architecture. Hereafter, we describe the core modules of MTNK:

- The **Learn** module provides on-demand cybersecurity training for employees with various roles and responsibilities. Through interactive learning pathways, employees gain essential cybersecurity skills, reducing the likelihood of human error as a primary attack vector. This module enhances employee awareness and skills, reducing the risk of cyber incidents, which is high due to the current lack of structured training in SMEs.
- The **Ecosystem** module serves as a centralized hub connecting SMEs with cybersecurity professionals, research institutions and solution providers to overcome the company's difficulty in accessing expert cybersecurity resources. Providing a map of relevant industry players and offering interactive knowledge-sharing fora, this platform facilitates direct engagement with experts, providing guidance on security strategy, compliance requirements and emerging threat trends. Also, the company's decision-making process is enhanced and a more proactive approach to cybersecurity is fostered by the ability to consult industry peers and access expert-led discussions.
- The **Tech Radar** module provides a dynamic landscape of cybersecurity solutions, enabling decision makers to evaluate emerging technologies and industry trends in real-time. Using AI-driven insights, the module provides tailored recommendations based on the organization's industry, infrastructure, and risk profile. This allows executives to make informed security investment decisions, optimizing cybersecurity investments and comply with both operational needs and budgetary constraints.
- The **Challenge** module introduces an open innovation mechanism that allows SMEs to publish specific cybersecurity challenges such as those related to industrial automation, IoT security or supply chain integrity, inviting proposals from start-ups, researchers, and industry experts. This fosters a competitive environment for cybersecurity problem solving, and may enables access to innovative and cost-effective security solutions that might otherwise remain inaccessible to SMEs due to the innovation adoption lag.
- The **Crowdsourcing** module promotes collaborative cybersecurity innovation by facilitating collective intelligence and knowledge sharing within a global security community. This module enhances collaborative problem solving and supports the co-development of best practices and risk mitigation strategies by SMEs.

3. The Learn Module in MTNK

An adequate training program can bring important benefits to companies [18], with an improvement of 45% to 65% in protection from security breaches [19]. In fact, even if users are often considered the weakest link in an organization's cybersecurity, proper training and awareness programs can transform them into the first line of defense against cyberattacks [20, 14, 21]. As previously mentioned, the MTNK platform is divided into different modules, which empower the user with the possibility to choose and adapt the technology to their needs. One of these modules is the Learn Module, which is dedicated to employee education.

Inside an SME there are different levels of training with respect to cybersecurity. Therefore, in the MTNK platform we proposed two distinct courses. The first one, named "**Cybersecurity Awareness**" is dedicated to basic training and understanding of the fundamentals. This course was designed to

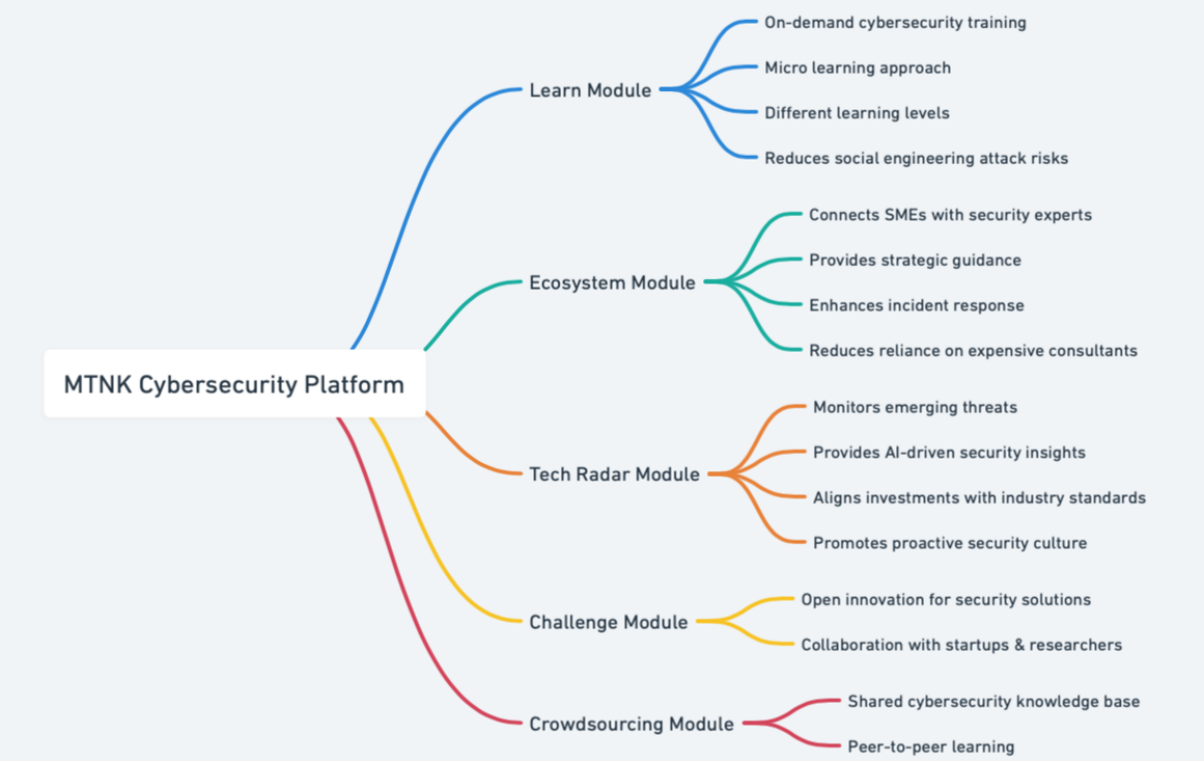

Figure 1: Conceptual framework of the MTNK cybersecurity platform (authors' own elaboration)

accommodate the learning needs of any employee of the SME with a low to null knowledge about cybersecurity risks. The second one, called "**Cybersecurity Advanced**" is meant for IT managers and people who already work with technologies, but want to improve their strategies and knowledge about cybersecurity risks and available tools.

These two courses follow the same scientific approach behind learning which, in nowadays state of the art, falls under the name of *micro-learning*. Micro-learning is defined as: "[...] relatively small, focused learning units consisting of condensed learning activities (usually one to 10 minutes), available on multiple devices." [22]. This approach allows users to access materials wherever they are and in different moments. Moreover, the conciseness of the courses can improve their effectiveness, as users generally can dedicate little time to security aspects during their work hours [23].

The conceptualization of the two courses followed an iterative process, where four researchers independently designed and compared their proposals, identifying advantages and disadvantages of each devised structure, and repeating until coming to an agreement. Regarding the learning paths for the Cybersecurity Awareness and Cybersecurity Advanced courses, we followed the structure the NIST Framework for improving critical infrastructure cybersecurity [24], namely the 5 functions there defined "Identify", "Protect", "Detect", "Respond", and "Recover". Therefore, the modules in the two courses are designed to cover each of the NIST functions to guarantee an all-round cybersecurity formation for the employees, at a different level of granularity. The two courses were developed by a multi-disciplinary team composed of three instructional designers and a cybersecurity expert, coming from both academic and corporate environments.

The Cybersecurity Awareness course is organized in 10 modules of about 15 minutes each as follows:

Module 1. Introduction to Cybersecurity: CIA principles (Confidentiality, Integrity, Availability).

Module 2. Common threats (*Identify*): malware, phishing, and ransomware.

Module 3. Password and Credentials (*Protect*): authentication methods, MFA (multi-factor authentication).

Module 4. Patching and Software updates (*Protect*): importance in preventing cyber attacks.

Module 5. Security of Mobile Devices (*Protect*): app permissions, mobile threats, and best practices.

Module 6. Device Security working remotely (*Protect*): VPN (Virtual Private Network), company policies.

Module 7. Data protection and privacy (*Protect*): GDPR (General Data Protection Regulation) salient articles.

Module 8. Recognizing malicious sites (*Detect*): phishing threats, SSL certificate forging, malvertising.

Module 9. Responding to a security incident (*Respond*): best practices and importance of reporting cyberattacks.

Module 10. Backup and data recovery (*Recover*): type of backups and best practices.

Each module is composed of (i) a textual *introduction* section, which introduces the user to the topic of the module, (ii) a short *animated video-clip* of 3-6 minutes, which details the topic in a frontal teaching manner, (iii) a closed-ended questions *quiz*, which tests the user knowledge on the module's subjects, and (iv) a *checklist* document which contains practical guidelines for the employee to apply the theoretical concepts into the workplace's everyday life. Optionally, (v) a module can have an *additional resources* document, which reports links to books, guides, papers, or videos to delve deeper into the covered topics, to address the needs of more interested users.

The Cybersecurity Advanced course has a more complex structure and is composed of 7 modules which can be divided into submodules, for a total of 12 didactic units. The structure is as follows:

Module 1. Introduction to Cybersecurity and the Framework

Module 2. (*Identify*) Common Threats and Emerging Technologies

- Module 2.1. Common Threats
- Module 2.2. Identifying threats

Module 3. (*Protect*) Protection Phase (Part 1)

- Module 3.1. Network Security
- Module 3.2. Human Factor, Phishing and Training
- Module 3.3. Credentials and account management

Module 4. (*Protect*) Protection Phase (Part 2)

- Module 4.1. Software Updates and Patch Management
- Module 4.2. Mobile and IoT Device Security
- Module 4.3. Protection of Sensitive Data and Privacy

Module 5. (*Detect*) Threat monitoring, logging and detection

Module 6. (*Response*) Incident Management

Module 7. (*Recovery*) Backup and Data Recovery

The (sub-)modules in the Advanced course are longer compared to those in the Awareness course, but follow a similar structure. These are composed of (i) a textual introduction that presents the subject that will be covered in the module, (ii) an animated video clip of 5-7 minutes that details the topic of matter, (iii) a closed-ended question quiz, and (iv) a document containing more advanced additional resources. Additionally, (v) depending on the theoretical subject explained in the module, there can also

be a textual practical guide that is meant to guide the user into implementing a technological solution within their systems, to provide a practical instance of the theoretical subject. Some of the modules also have a video tutorial which directly follows the content of the guide. The video tutorials have a varying duration of about 5 to 10 minutes, depending on the complexity of the subject. Finally, there are some modules with a "talk-with-expert" content, which is a brief video (1-2 minutes) of a recorded interview with a cybersecurity expert discussing about a topic of interest to the module. These videos are meant to increase the authority, credibility, and relevance of the course and the proposed subject, underlying the importance of certain cybersecurity topics. Table 1 better details the more complex structure of the Cybersecurity Advanced course.

4. Discussions

The MTNK platform offers an integrated approach to enhancing the cybersecurity resilience of SMEs by combining employee training, external collaboration with experts, and technology innovation. Its modular design targets both technological and human vulnerabilities.

The Tech Radar module, by enabling proactive adoption of advanced security tools through real-time AI-driven insights, can allow the company to align its cybersecurity investments with evolving risks and operational requirements. The Ecosystem module allows the SME to further improve its security stance by connecting with cybersecurity professionals, research institutions, and industry peers, facilitating knowledge transfer, mentorship, and shared situational awareness. The Challenge module can encourage SMEs to articulate specific cybersecurity issues and explore tailored solutions from external innovators, including startups, researchers, and cybersecurity experts — this collaboration can shorten the gap that is typical in academic to industrial transfer [31]. Meanwhile, the Crowdsourcing module can serve as a communication bridge with the broader cybersecurity community, facilitating the co-development of best practices within the company.

The Learn module facilitates continuous, micro-learning-based workforce upskilling and supports governance models that emphasize the human factor in cybersecurity. Notably, the two courses offered in the platform can address different needs of the employees. The basic course, i.e., *Cybersecurity Awareness*, limits the content to the essential concepts for the generic employee, who may not be interested in following longer didactic units. On the other hand, the *Cybersecurity Advanced* course comprises more detailed units to provide a deeper formation to employees who have to improve the cybersecurity posture of their company, while remaining as essential and practical as possible.

Despite the expected benefits of MTNK there are several challenges in the adoption of the platform by an organization. These include perceived platform complexity and reluctance to shift from traditional models. The effectiveness of community-driven features such as the Crowdsourcing module also depends on sustained user engagement, regular data updates, and rigorous validation of shared content. Privacy concerns represent an additional barrier, as SMEs may hesitate to share sensitive information due to competitive risks and regulatory obligations, such as the GDPR [30].

All and all, a platform like MTNK has the potential to reshape SME cybersecurity practices on both national and European levels. By integrating key functions—ranging from education and technology evaluation to expert consultation and innovation sourcing—into a single, interoperable environment, MTNK offers a scalable and proactive alternative to the fragmented cybersecurity tools and services currently available to SMEs. To fully realize this potential, policy incentives and public-private partnerships may be necessary to lower adoption barriers and foster a supportive ecosystem for digital transformation.

5. Conclusions and future work

This paper presented MTNK, a cybersecurity platform designed to address key vulnerabilities in SMEs. By using modular functionalities, MTNK provides a structured framework that encourages proactive security measures rather than the reactive approaches that typically characterize SME cybersecurity

Table 1
Structure of the Cybersecurity Advanced course

(Sub-) Module	Introduction + Video clip + Quiz	Additional resources	Practical guide	Video Tutorial	Talk with expert
Module 1. Intro	Overall view on cybersecurity risks, CIA principles, NIST framework	ISO/IEC 27001 [25]	-	-	-
		Module 2. Identify			
2.1	Common Threats and Cyber kill chain	Vulnerability assessment tools	Use of WPscan software	Yes	-
2.2	Traditional and innovative technologies threat identification	Cloud security services (AWS, Azure, Google Cloud), antivirus software	Use of VirusTotal software	Yes	-
		Module 3. Protect (part 1)			
3.1	Network security – firewall and VPNs	Setting VPNs for cloud services guides	Defining firewall rules with UFW	-	-
3.2	Human factors, phishing, training campaigns	Usable security academic resources [26, 27]	-	-	Importance of Human factors in security
3.3	Password management, Identity Access Management	MFA providers	-	-	-
		Module 4. Protect (part 2)			
4.1	Software updates and patch management	MITR3 Att&ck [28], National Vulnerability Database [29]	Protecting a WordPress website	Yes	-
4.2	Mobile and IoT threats, Mobile device Management (MDM)	Configuring an MDM service guide	-	-	Minimal tips for IoT security
4.3	Privacy, sensitive data, data anonymization	GDPR external resources [30], data anonym. techniques	-	-	GDPR and ethics
Module 5. Detect	Monitoring, detecting and logging tools (SIEM, IDS, IPS)	SIEM solutions links	Use of Snort as a network IDS	-	-
Module 6. Response	Key components for effective responses and policies	Useful contacts in case of attack	-	-	-
Module 7. Recovery	Data backup and recovery	Backups with cloud services guides	Backups with MS OneDrive	Yes	-

practices. Particularly in environments where SMEs lack the resources to build dedicated internal

security teams, MTNK has the potential to fill critical gaps in cybersecurity preparedness.

The learning module of the platform includes two distinct courses– *Cybersecurity Awareness* and *Cybersecurity Advanced*– to address the learning needs of employees with different levels of cybersecurity expertise and responsibilities. The former course was designed to train employees of all levels to limit the risks of human errors and socio-technical attacks such as phishing, ransomware, and malware download. On the other hand, the latter is meant to improve the cybersecurity knowledge and skills of employees with a higher responsibility regarding the IT posture of the company.

Despite the expected benefits of MTNK, its implementation faces significant challenges, such as adoption barriers, the need of an active cybersecurity community, and privacy concerns. While this paper provides a conceptual application of MTNK, real-world testing will be required to measure the actual impact of the platform adoption on the cybersecurity resilience of SMEs. In addition, we did not consider sector-specific differences in cybersecurity needs. Future studies should explore how MTNK's functionalities can be tailored to different industries, such as healthcare, finance, and industrial manufacturing, where regulatory and operational risks vary significantly. Finally, quantitative evaluations are needed to assess the effectiveness of MTNK in reducing cybersecurity incidents, improving risk management, and enhancing the long-term security posture of SMEs.

To assess usability, engagement and measurable security improvements, future research will focus on pilot implementations of MTNK in real-world SME environments. Longitudinal studies tracking security performance before and after implementation would provide valuable empirical data on the impact of the platform. Further exploration of AI-driven automation within the Tech Radar and Crowdsourcing modules could also enhance the value of MTNK, enabling predictive analytics to anticipate emerging threats and optimize security decision-making.

As cybersecurity threats keep evolving, the integration of accessible security frameworks such as MTNK can play a critical role in strengthening the cybersecurity resilience of SMEs, ensuring that even resource-constrained organizations be able to implement and maintain effective security measures.

Acknowledgments

This work has been supported by the Italian Ministry of University and Research (MUR) and by the European Union – NextGenerationEU, under grant PRIN 2022 PNRR "Innovation, digitalisation and sustainability for the diffused economy in Central Italy", acronym **VITALITY** (Project code ECS_00000041) – Mission 4, Component 2, Investment 1.5, Spoke 1 – CUP E13C22001060006.

The research of Francesco Greco is funded by a PhD fellowship within the framework of the Italian "D.M. n. 352, April 9, 2022"– under the National Recovery and Resilience Plan, Mission 4, Component 2, Investment 3.3 – PhD Project "Investigating XAI techniques to help user defend from phishing attacks", co-supported by "Auriga S.p.A." (CUP H91I22000410007).

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] E. Charlton, 2023 was a big year for cybercrime – here's how we can make our systems safer, 2024. URL: https://www.weforum.org/stories/2024/01/cybersecurity-cybercrime-system-safety/.

[2] U. Tariq, I. Ahmed, A. K. Bashir, K. Shaukat, A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review, 2023. URL: https://www.mdpi.com/1424-8220/23/8/4117. doi:10.3390/s23084117.

[3] C. Sausalito, 2024 cybersecurity almanac: 100 facts, figures, predictions and statistics, 2024. URL: https://cybersecurityventures.com/cybersecurity-almanac-2024/.

[4] IBM, Cost of a data breach report, 2024. URL: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec.

[5] SentinelOne, Key cyber security statistics for 2025, 2024. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/.

[6] Embroker, Cyberattack statistics 2025, 2025. URL: https://www.embroker.com/blog/cyber-attack-statistics/.

[7] R. Johnson III, 60 percent of small companies close within 6 months of being hacked, 2019. URL: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/.

[8] Gartner, Gartner forecasts global information security spending to grow 15% in 2025, 2024. URL: https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025.

[9] M. Mukherjee, N. T. Le, Y.-W. Chow, W. Susilo, Strategic approaches to cybersecurity learning: A study of educational models and outcomes, 2024. doi:10.3390/info15020117.

[10] M. Siavvas, T. Dimitrios, J. Marija, K. Dionysios, , D. Tzovaras, Technical debt as an indicator of software security risk: a machine learning approach for software development enterprises, Enterprise Information Systems 16 (2022) 1824017. URL: https://doi.org/10.1080/17517575.2020.1824017. doi:10.1080/17517575.2020.1824017.

[11] M. Elrayah, S. Jamil, Impact of digital literacy and online privacy concerns on cybersecurity behaviour: The moderating role of cybersecurity awareness, International Journal of Cyber Criminology 17 (2023). URL: https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/205.

[12] Verizon, 2024 data breach investigations report, 2024. URL: https://www.verizon.com/business/resources/reports/dbir/#DBIR2024NR.

[13] L. Brunken, A. Buckmann, J. Hielscher, M. A. Sasse, "to do this properly, you need more resources": The hidden costs of introducing simulated phishing campaigns, 2023. URL: https://dl.acm.org/doi/10.5555/3620237.3620467.

[14] D. Lain, K. Kostiainen, S. Čapkun, Phishing in organizations: Findings from a large-scale and long-term study, in: 2022 IEEE Symposium on Security and Privacy, 2022, pp. 842–859. URL: https://doi.org/10.1109/SP46214.2022.9833766. doi:10.1109/SP46214.2022.9833766.

[15] M. Dixon, N. A. G. Arachchilage, J. Nicholson, Engaging users with educational games: The case of phishing, 2019. URL: https://doi.org/10.1145/3290607.3313026. doi:10.1145/3290607.3313026.

[16] P. S. Hogle, Microlearning in Corporate Settings, 1st edition ed., Routledge, New York, 2021, p. 16. URL: https://www.taylorfrancis.com/chapters/edit/10.4324/9780367821623-12/microlearning-corporate-settings-pamela-hogle. doi:10.4324/9780367821623.

[17] J. T. Karlsen, E. Balsvik, M. Rønnevik, A study of employees' utilization of microlearning platforms in organizations, The Learning Organization 30 (2023) 760–776. URL: https://doi.org/10.1108/TLO-07-2022-0080. doi:10.1108/TLO-07-2022-0080.

[18] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, B. von Solms, Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise, Computers & Security 119 (2022) 102756. URL: https://www.sciencedirect.com/science/article/pii/S0167404822001511. doi:https://doi.org/10.1016/j.cose.2022.102756.

[19] F. Ugbebor, O. Aina, M. Abass, D. Kushanu, Employee cybersecurity awareness training programs customized for sme contexts to reduce human-error related security indicents, Journal of Knowledge Learning and Science Technology 3 (2024) 382–409. URL: https://doi.org/10.60087/jklst.vol3.n3.p382-409. doi:10.60087/jklst.vol3.n3.p382-409.

[20] D. Jampen, G. Gür, T. Sutter, B. Tellenbach, Don't click: towards an effective anti-phishing training. a comparative literature review, Human-centric Computing and Information Sciences 10 (2020) 33. URL: https://doi.org/10.1186/s13673-020-00237-7. doi:10.1186/s13673-020-00237-7.

[21] M. A. Sasse, S. Brostoff, D. Weirich, Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security, BT Technology Journal 19 (2001) 122–131. URL: https://doi.org/10.1023/A:1011902718709. doi:10.1023/A:1011902718709.

[22] M. Shail, Using micro-learning on mobile applications to increase knowledge retention and work performance: A review of literature, Cureus 11 (2019). URL: https://www.cureus.com/articles/21612-using-micro-learning-on-mobile-applications-to-increase-knowledge-retention-and-work-performance-a-r doi:10.7759/cureus.5307.
[23] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, J. Hong, Teaching johnny not to fall for phish, ACM Transactions on Internet Technology 10 (2010) 1–31. URL: https://doi.org/10.1145/1754393.1754396. doi:10.1145/1754393.1754396.
[24] NIST, The nist cybersecurity framework (csf) 2.0, 2024. URL: https://doi.org/10.6028/NIST.CSWP.29. doi:10.6028/NIST.CSWP.29.
[25] ISO/IEC, Information security, cybersecurity and privacy protection - information security management systems - requirements, 2022. URL: https://www.iso.org/standard/27001.
[26] A. Adams, M. A. Sasse, Users are not the enemy, Commun. ACM 42 (1999) 40–46. URL: https://doi.org/10.1145/322796.322806. doi:10.1145/322796.322806.
[27] A. Sasse, I. Flechais, Usable Security: Why Do We Need It? How Do We Get It?, O'Reilly, Sebastopol, US, 2005, pp. 13–30. URL: https://discovery.ucl.ac.uk/id/eprint/20345/2/cransimpsonbook.pdf.
[28] MITRE, Mitre att&ck, 2015. URL: https://attack.mitre.org/.
[29] NIST, National vulnerability database, 2022. URL: https://nvd.nist.gov/vuln.
[30] EU, General data protection regulation (gdpr), 2016. URL: https://gdpr-info.eu/.
[31] S. A. M. Dolmans, B. Walrave, S. Read, N. van Stijn, Knowledge transfer to industry: how academic researchers learn to become boundary spanners during academic engagement, The Journal of Technology Transfer 47 (2022) 1422–1450. URL: https://doi.org/10.1007/s10961-021-09882-1. doi:10.1007/s10961-021-09882-1.