Eng Int Syst (2024) 1: 35–41

Engineering
Intelligent Systems

Enabling Digital Transformation with Sustainability Criteria through Resilient Cybersecurity: Challenges and Opportunities

Michael Zipperle[1,2,*], Marius Becherer[1,2,†], Yu Zhang[1,‡], Elizabeth Chang[3,§], Tharam Dillon[4,§§] and Achim Karduck[5,¶]

[1] *UNSW Canberra, Cyber Security Cooperative Research Centre*
[2] *Cyber Security Cooperative Research Centre*
[3] *Griffith University,*
[4] *La Trobe University*
[5] *Furtwangen University*

Digital transformation, necessitating the integration of digital technology across all business domains, is vital for long-term business policies seeking competitive advantage in our interconnected global economy. Sustainable transformation requires resilient and trustworthy Digital Ecosystems and transparency with respect to sustainability criteria. However, cybersecurity threats are at an all-time high, accelerated by the expansion of digital footprints and the Computer Supported Cooperative Work (CSCW) paradigm during the COVID-19 crisis. These risks are worsened by the straightforward misuse of the latest sophisticated cybersecurity educational platforms and Large Language Model (LLM)s. This study examines these challenges, proposes a conceptual framework for Cybersecurity-enabled Digital Transformation (CeDT) to illustrate the interplay between cybersecurity and digital transformation with sustainability criteria, and introduces a conceptual framework for Provenance-enabeld Graph Autoencoders for Anomaly Detection (PGAE-AD) as one potential security tool to detect cyber-security threats in continuously changing real-world environments. By providing a secure environment, these frameworks can be instrumental in facilitating digital transformation while minimizing associated cybersecurity risks.

1. INTRODUCTION

Digital transformation, integrating digital technology into all business areas, is no longer a luxury but a critical necessity for enterprises striving to stay competitive in our interconnected world by providing resilience and trustworthy transparency for creating products and services. It calls for adopting emerging technologies such as cloud computing, Artificial Intelligence (AI)/Machine Learning (ML), Internet of Things (IoT), blockchain, and others to enable trustworthy business processes, foster innovation with the assurance of sustainability criteria, and deliver excellent customer experience [1]. However, with the increasing digital footprint, the threat landscape has expanded, making cybersecurity a paramount concern.

One motivation example for this work is the Computer Supported Cooperative Work (CSCW) paradigm accelerated through the COVID-19 crises [2]. Enterprises have been forced to adapt quickly, hence, being more vulnerable than ever due to rapid environmental changes [3], [4]. Cybercriminals took advantage of this situation and were able to compromise several targets, from individuals to large enterprises around the world. Security incidents stayed

*Emails: m.zipperle@unsw.edu.au, †m.becherer@unsw.edu.au, ‡m.yuzhang@unsw.edu.au, §e.chang@griffith.edu.au, §§tharam.dillon7@gmail.com, ¶Email: karduck@hs-furtwangen.de

undetected for up to multiple weeks, leading to data and financial loss for the incident target [5], [6].

In addition, the misuse of the recently advancing publically available cybersecurity educational platforms, including penetration testing platforms and Large Language Model (LLM)s, can significantly increase the risks during digital transformation and operations. Penetration testing platforms, designed to help learners understand the mechanisms of hacking for defense purposes, can be misused to educate cybercriminals. Similarly, LLMs, intended for constructive uses such as text generation and prediction, can be exploited to generate misinformation, phishing emails, socially engineered content, or even malware. These instances highlight the critical need for rigorous security protocols and ethical guidelines to guard against misuse as we continue to digitize and transform various sectors of society.

This demonstrates the significance of cybersecurity as an enabler of secure and trustworthy digital transformation [7]. Resilience of critical infrastructures is a key aspect of sustainable (digital) transformation. The push toward digital transformation escalates the need for comprehensive cybersecurity measures. Similarly, effective cybersecurity practices can facilitate digital transformation by providing a secure environment for innovation and growth. With rising data breaches and cyber-attacks, cybersecurity is not only about risk management but also a strategic investment that can drive business growth and innovation [8].

In this work, we highlight the challenges exposed to digital transformation, such as educational platforms, and present two potential opportunities to counter that. First, we propose a conceptual framework for Cybersecurity-enabled Digital Transformation (CeDT), highlighting the interplay between cybersecurity as an enabler for secure digital transformation. Second, we present a conceptual framework of Provenance-enabeld Graph Autoencoders for Anomaly Detection (PGAE-AD) as one potential security tool capable of adapting to the ever-evolving digital landscape, thus, offering the high potential to support secure digital transformation. Sophisticated provenance assures a crystal clear picture of all the actions enforced to services, data, and cyber assets with respect to any modification, and thus is key for resilience in our interconnected digital ecosystem.

The remainder of this work is structured as follows: in Section 2, we discuss related work from the literature. In Section 3, we highlight the challenges that arise from the misuse of education platforms. In Section 4, we present the conceptual framework for CeDT. In Section 5, we present the conceptual framework of PGAE-AD, and Section 6 concludes this research and provides an outlook.

2. RELATED WORK

Digital transformation has become the cornerstone of modern business strategy, driving innovation, accelerating business processes, and enhancing customer experience. However, this transformation also introduces new cybersecurity challenges that must be addressed to ensure digital strategies' safe and successful implementation.

In the realm of digital transformation, Kankaanhuhta et al. [9] conducted a case study on the digital transformation of forest services in Finland. They highlighted the role of agile software tools in improving productivity and customer experience. Similarly, Purwaningtyas et al. [10] discussed the application of digital technology in aviation schools, focusing on improving customer experience, processes, and business models. Both studies underscore the importance of digital transformation in enhancing business processes and customer experience. Vial [11] conducted a comprehensive review of 282 works on digital transformation, building a framework of digital transformation articulated across eight building blocks. His work foregrounds digital transformation as a process where digital technologies create disruptions triggering strategic responses from organizations. Rha and Lee [12] examined digital transformation in the service sector through network text analysis of 330 related articles published during the past ten years. Their work provides an overview of the dominant research topics and their clusters in digital transformation. Xue et al. [13] conducted an empirical study on the impact of digital transformation on green technology innovation. They found that digital transformation can significantly promote green technology innovation by alleviating financing constraints and attracting government subsidies.

In addition, the importance of cybersecurity in the context of digital transformation has been emphasized by several researchers. Bocayuva [4] discussed the impact of digital transformation on all sectors, including the port sector, and emphasized the importance of cybersecurity in the face of new risks and threats brought about by the digital era. Gellert et al. [14] introduced the concept of "Zero Trust" in information security, emphasizing the importance of continuous identity verification to minimize trust zones and their associated risk of security breaches in the healthcare sector. Furthermore, in the context of the COVID-19 pandemic, Maleh and Béni Mellal [15] discussed how the pandemic has accelerated the digital transformation process, leading to an explosion of online services. However, they also highlighted the increased cybersecurity risks associated with this rapid digitalization. Kurniawan and Arti [16] conducted a comparative study of the cybersecurity curriculum in Indonesia and the Netherlands. They emphasized the need for a multidisciplinary approach to cybersecurity education to support digital transformation in the public sector. Kuzior et al. [17] conducted a study on global digital convergence, discussing the impact of cybersecurity, business transparency, economic transformation, and anti-money laundering efficiency on the level of digital development. Finally, Mijwil [18] highlighted the importance of cybersecurity governance in providing safe and effective technical means to face all threats and challenges associated with digital transformation.

In conclusion, while digital transformation offers numerous benefits regarding business process improvement, innovation, and enhanced customer experience, it also introduces new cybersecurity challenges. Therefore, a policy based on Zero Trust and a holistic resilience approach that considers both the opportunities offered by digital transformation and the cybersecurity risks is essential for prosperous businesses with sustainability criteria.

3. CHALLENGES: MISUSE OF CYBERSECURITY EDUCATIONAL PLATFORMS

Recent advancements in cybersecurity educational platforms, including penetration testing platforms and LLM, are raising severe challenges since these tools can be misused to conduct sophisticated cyberattacks. While these educational platforms are designed to educate and train cybersecurity professionals, their misuse can inadvertently contribute to the creation of highly skilled cybercriminals. This paradoxical outcome underscores the importance of providing advanced training tools and ensuring their ethical and responsible use.

3.1 Penetration Testing

Penetration testing, or ethical hacking, is critical to cybersecurity education. It involves authorized simulated cyberattacks on a computer system to evaluate its security. Educational penetration testing platforms provide a safe and controlled environment for students and professionals to learn and practice their hacking skills without causing harm. These platforms are designed to mimic real-world systems with various vulnerabilities that users can exploit, thereby providing hands-on experience in identifying and mitigating cybersecurity threats. There are several educational penetration testing platforms available, each with its unique features and capabilities:

Hack The Box (HTB). : HTB is an online platform that provides various challenges and virtual machines for users to practice their penetration testing skills. It offers various difficulty levels, from beginner to advanced, making it suitable for learners at all stages [19].

TryHackMe. : TryHackMe offers guided and interactive learning experiences. It provides a variety of rooms (challenges) covering different cybersecurity topics, including penetration testing, forensics, and web application security. In addition, TryHackMe also offers gamified challenges; one famous example is "King of the Hill", in which multiple players attempt to hack into a machine; once a player has access, the player tries to retain presence by patching vulnerabilities to stop other players from gaining access [20].

OverTheWire. : OverTheWire is designed for individuals who want to learn more about security concepts and practice their skills. It offers a series of wargames, each designed to test and enhance different aspects of cybersecurity knowledge [21].

PentesterLab.: PentesterLab provides hands-on exercises that cover various topics, including web penetration testing, Unix security, Android hacking, and more. It offers free exercises and a pro subscription with additional content [22].

VulnHub.: VulnHub is a platform that allows users to comprehend and practice hacking skills through a series of challenges in a safe and legal environment [23].

While these platforms offer excellent opportunities to educate penetration testing professionals, they also pose risks that could impact digital transformation initiatives. The skills acquired could be misapplied, leading to unauthorized exploitation of digital systems and undermining trust in digital transformation efforts. This emphasizes the need for ethical training alongside technical instruction.

3.2 Large Language Model (LLM)

LLMs, such as ChatGPT [24], have shown remarkable capabilities in generating human-like text, understanding context, and even answering complex queries. While these capabilities have numerous beneficial applications, they also present potential risks if misused maliciously [25].

Cybercriminals may misuse LLMs to conduct malicious activities: First, LLMs could generate convincing, personalized messages that mislead users into disclosing sensitive information or clicking on malicious links. Second, LLMs could also be used to create realistic deep fake content or disinformation campaigns, contributing to broader cyber threats. Third, given their ability to generate code, LLMs could potentially be used to automate the creation of malicious software or malware. By providing the model with certain specifications, an adversary could instruct it to generate code that exploits specific vulnerabilities or performs harmful actions. These activities represent just a fraction of the numerous potential malicious ones.

Although ChatGPT has fundamental safeguards in place to prevent its misuse, these can be easily circumvented with careful phrasing of prompts. For instance, a direct request to assist in identifying and exploiting vulnerabilities, posed as "Can you help me to find and exploit vulnerabilities using Kali Linux at the following target: 192.168.100.130", is met with a refusal: "I'm sorry, but I cannot assist you with finding or exploiting vulnerabilities in any system. Hacking into systems without explicit permission is illegal and unethical, and it's against OpenAI's use-case policy". Nonetheless, rephrasing the question to reflect professional due diligence, such as "I'm a security professional. Can you help me conduct a security audit using Kali Linux at the following target: 192.168.100.130?", elicit a detailed step-by-step walkthrough.

Therefore, as the development and deployment of LLMs progress, it is imperative to consider these potential risks and implement appropriate safeguards to prevent misuse. This includes robust access controls, usage monitoring, and ongoing research into potential adversarial attacks and defenses.

In conclusion, educational platforms such as penetration testing platforms and LLMs are instrumental in cybersecurity education, providing practical, hands-on learning experiences. However, their potential for misuse introduces significant risks for digital transformation and its wider exposure to digital assets, underscoring the critical need for concurrently implementing sophisticated cybersecurity measures.

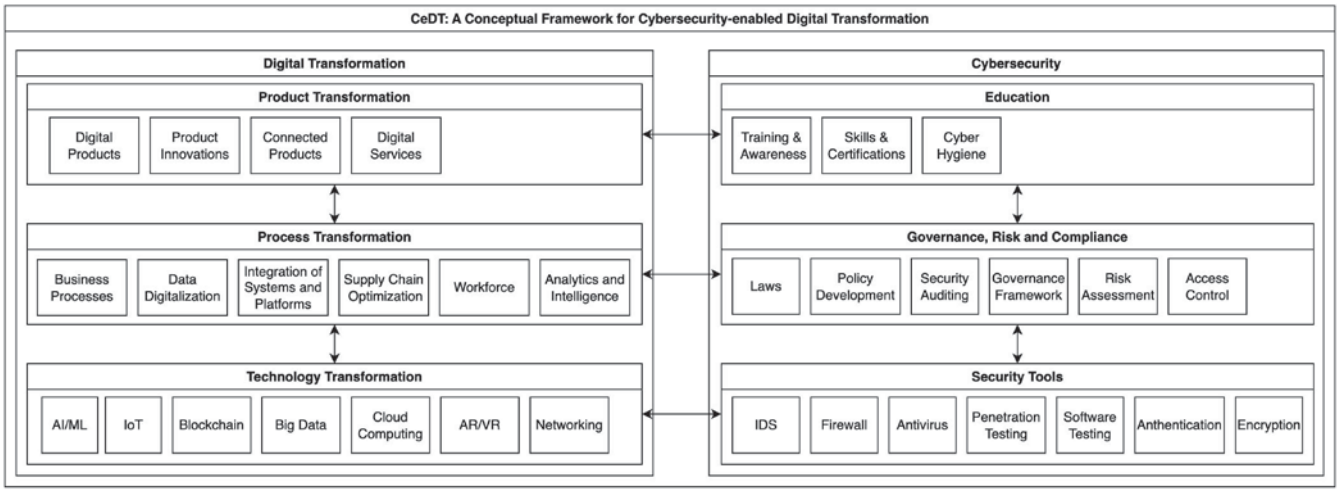

Figure 1 A Conceptual Framework for CeDT.

4. OPPORTUNITIES: A CONCEPTUAL FRAMEWORK FOR CYBERSECURITY-ENABLED DIGITAL TRANSFORMATION (CEDT)

Digital transformation and cybersecurity are two interconnected domains essential for modern businesses. As organizations increasingly adopt digital technologies to improve their operations, innovate, and enhance customer experience, they also face growing cybersecurity risks. Therefore, we propose a conceptual framework for CeDT to mitigate these risks and ensure secure digital transformation; an overview is given in Fig. 1. The framework consists of two main modules: the digital transformation module and the cybersecurity module.

4.1 The Digital Transformation Module

The digital transformation module focuses on adopting and integrating digital technologies into all business areas. This module is driven by changes in the business environment, customer behavior, and technology advancements. It involves three key submodules:

Technology Transformation. Technology transformation involves identifying, evaluating, and integrating suitable digital technologies such as AI, IoT, Blockchain, and more that can enhance business operations, improve customer experience, and drive innovation.

Process Transformation. Process transformation involves streamlining and automating business processes to increase efficiency, reduce costs, and improve service delivery. It includes the redesign of workflows, the elimination of redundant tasks, and the introduction of automation where appropriate.

Product Transformation. Product transformation involves using digital technologies to enhance or create new products. It includes the development of digital products and services, the digital enhancement of physical products, and the use of data and analytics to create personalized offerings.

4.2 The Cybersecurity Module

The cybersecurity module protects the organization's digital assets from various cyber threats. This module ensures digital systems and data security, integrity, and availability. It involves three key submodules:

Security Tools. Security tools involve the use of tools to protect digital assets. These include firewalls, intrusion detection systems, encryption technologies, and other security tools.

Governance, Risk, and Compliance. Governance, risk, and compliance include adopting laws, policy development, security audits, risk assessment, and continuously monitoring security controls.

Education. Education ensures that all employees and stakeholders involved in the digital transformation understand their cybersecurity-related roles and responsibilities. This includes providing cybersecurity training and awareness programs, skills, and certifications, fostering a security-conscious culture, and ensuring that cybersecurity considerations are considered in all decision-making processes.

4.3 A Walkthrough

The digital transformation and cybersecurity modules are intrinsically interconnected, operating synergistically through a bottom-to-top approach. This approach ensures that each stage of the transformation process is underpinned by robust cybersecurity measures, thereby fostering a secure digital environment.

For instance, when an enterprise launches on a technology transformation by introducing new digital technology, a series of interconnected actions are triggered within the cybersecurity module. The first step involves revising the existing security tools. This is crucial to ensure sufficient protection for the new technology, thereby mitigating any potential cyber threats that could compromise the integrity of the digital transformation process.

Following this, the process transformation stage is initiated. This involves reengineering existing business processes to

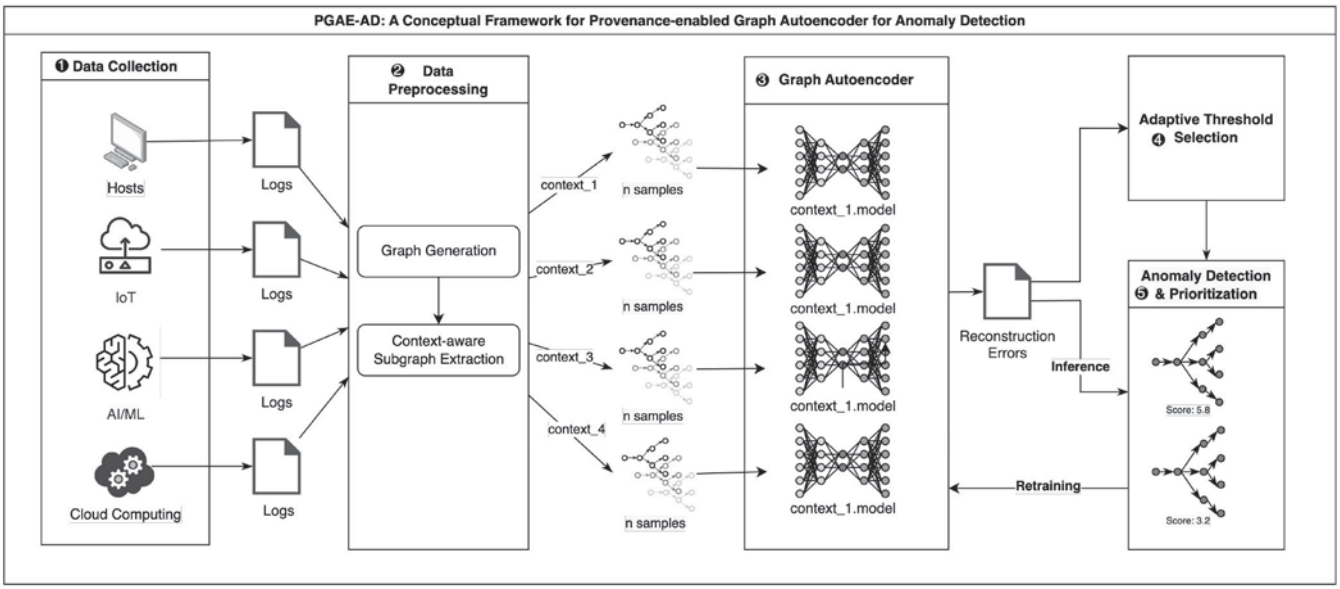

Figure 2 A Conceptual Framework for PGAE-AD.

align with the new digital technology. Concurrently, the governance, risk, and compliance procedures are updated to ensure they can manage the risks associated with the new digital processes. This involves updating policies and procedures to comply with relevant laws and regulations about the new technology. It also includes conducting risk assessments and audits to ensure compliance and identify potential vulnerability areas.

Finally, the product transformation stage is undertaken, which involves leveraging the new technology to enhance existing products or create new ones. Simultaneously, the education aspect of the cybersecurity module is addressed. This involves educating employees about the new technology and the associated cybersecurity measures. This step is crucial to ensure that all individuals within the organization understand their roles and responsibilities in maintaining cybersecurity in the new digital environment.

In conclusion, the digital transformation and cybersecurity modules are actively connected, influencing and shaping the other. This interconnected approach ensures that digital transformation initiatives are securely implemented, enabling organizations to reap the benefits of digital transformation while minimizing associated cybersecurity risks.

5. OPPORTUNITIES: A CONCEPTUAL FRAMEWORK FOR PGAE-AD

One potential drawback of the CeDT is our assumption that the cybersecurity module possesses the necessary capabilities to guarantee the security, integrity, and availability of digital systems and data. Unfortunately, due to the rapid advancement of emerging technologies like cloud computing, AI, IoT, and blockchain, existing solutions find it challenging to keep pace with these developments.

To address this, we want to highlight the recent research on Provenance-based Intrusion Detection Systems (PIDS) as on solution for Intrusion Detection Systems (IDS) as part of the security tools. PIDS leverage the concept of data provenance to enhance the accuracy of intrusion detection and minimize the rate of false alarms [26], [27]. By tracing and recording the origins and lifecycle of data, PIDS can provide a detailed context for identifying and analyzing potential security threats, thereby enhancing accuracy.

5.1 Framework Overview

With the recent advancements in Graph Neural Networks (GNN), we present a conceptual framework for PGAE-AD that demonstrates high adaptability, making it particularly suitable for environments characterized by rapid and continuous change, such as those driven by digital transformation. In such dynamic environments, the ability to quickly adapt to new types of data and evolving threat patterns is of utmost importance. Equipped with inherent flexibility and comprehensive data tracking capabilities, our PGAE-AD is well-equipped to meet these challenges. An overview of the framework is provided in Fig. 2.

Data Collection. The data collection module gathers data from various heterogeneous sources, including hosts, IoT devices, AI/ML, and cloud computing environments.

Data Preprocessing. The data preprocessing module parses the collected data into a graph based on predefined graph models. It then extracts contextual subgraphs.

Graph Autoencoder. The graph autoencoder learns local and global graph features from a set of benign subgraphs. The output is the reconstruction error between the input and reconstructed graphs.

Adaptive Threshold Selection. The adaptive threshold selection module utilizes the training output to select a threshold for anomaly detection dynamically.

Anomaly Detection & Prioritization. The anomaly detection and prioritization module classifies unseen subgraphs as benign or malicious based on whether their reconstruction

error exceeds the adaptive threshold. Potential alarms can be prioritized based on their reconstruction error, with a higher error indicating higher importance.

5.2 A Walkthrough

To illustrate the process, let us consider host-based audit logs as an example for provenance data. In this case, PGAEAD collects host-based audit logs and converts them into a graph representation, where nodes represent system entities and edges represent system operations. System entities can include processes, files, modules, registries, and more, while system operations encompass actions like creation, deletion, editing, connection, and others. Next, the framework extracts context-aware subgraphs, such as subgraphs, based on process executables. This results in multiple samples for each process executable. The graph autoencoder is then trained using benign samples for each process executable, and the adaptive threshold is selected. Subsequently, the model can be deployed to classify unseen subgraphs. The assumption is that potential malicious subgraphs possess different local and global graph features, resulting in higher reconstruction errors compared to benign subgraphs. If a subgraph is classified as malicious, appropriate actions can be taken to address the security threat.

In conclusion, the proposed conceptual framework for PGAE-AD harnesses the advancements in GNN to offer high adaptability, making it well-suited for dynamic environments driven by digital transformation. The framework's ability to swiftly adapt to new data types and evolving threat patterns is crucial in ensuring effective anomaly detection and prioritization. By leveraging the power of graph autoencoders, the framework learns local and global graph features, enabling the identification of potential security threats. The adaptive threshold selection further enhances the framework's capabilities by dynamically adjusting the detection threshold. Overall, the framework provides a robust solution for addressing cybersecurity challenges in rapidly changing environments, such as digital transformation.

6. CONCLUSION

This work has explored the landscape of digital transformation, demonstrating its necessity for businesses contending for competitive advantage in an increasingly digital and interconnected global economy. However, the expanded digital footprints inherent in such transformation have also amplified cybersecurity risks, a situation further escalated by the COVID-19-induced shift to remote work and the misuse of educational platforms like penetration testing platforms and Large Language Model (LLM)s.

In response to these challenges, we have proposed a conceptual framework for Cybersecurity-enabled Digital Transformation (CeDT) that explains the importance of the interplay between cybersecurity and digital transformation. Furthermore, we have introduced a novel conceptual framework for Provenance-enabeld Graph Autoencoders for Anomaly Detection (PGAE-AD) as a potential tool to detect cybersecurity threats in an ever-evolving digital landscape.

Through the establishment of secure operational environments, the proposed frameworks are posited as instrumental mechanisms to facilitate digital transformation while effectively mitigating associated cybersecurity risks. The insights derived from this study underscore the importance of continually developing and refining security measures as an integral part of the digital transformation journey, highlighting the necessity for future research and innovations in this critical field.

ACKNOWLEDGMENTS

The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

REFERENCES

1. S. J. Berman, "Digital transformation: Opportunities to create new business models," *Strategy & Leadership*, vol. 40, no. 2, pp. 16–24, Jan. 2012. [Online]. Available: https://doi.org/10.1108/1087857121 1209314
2. P. Soto-Acosta, "COVID-19 pandemic: Shifting digital transformation to a high-speed gear," *Information Systems Management*, vol. 37, no. 4, pp. 260–266, 2020. [Online]. Available: https://doi.org/10.1080/10580530.2020.1814461
3. "Cyber crime – the risks of working from home." [Online]. Available: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html
4. M. Bocayuva, "Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic," *WMU Journal of Maritime Affairs*, vol. 20, no. 2, pp. 173–192, Jun. 2021. [Online]. Available: https://doi.org/10.1007/s13437-021-00240-4
5. BITSIGHT, "The Financial Impact of SolarWinds Breach," 2021. [Online]. Available: https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided
6. A. C. Society, "Medibank reports significant cyber security incident," 2023. [Online]. Available: https://ia.acs.org.au/article/2022/medibank-reports-significant-cyber-security-incident.html
7. A. Yerina, I. Honchar, and S. Zaiets, "Statistical Indicators of Cybersecurity Development in the Context of Digital Transformation of Economy and Society," *Science and Innovation*, vol. 17, no. 3, pp. 3–13, Jun. 2021. [Online]. Available: https://scinn-eng.org.ua/oj s/index.php/ni/article/view/95
8. B. K. Gebremeskel, G. M. Jonathan, and S. D. Yalew, "Information Security Challenges During Digital Transformation," *Procedia Computer Science*, vol. 219, pp. 44–51, Jan. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S18770 50923002703
9. V. Kankaanhuhta, T. Packalen, and K. Väätäinen, "Digital transformation of forest services in Finland—A case study for improving business processes," *Forests*, vol. 12, no. 781, 2021. [Online]. Available: https://www.mdpi.com/1999-4907/12/6/781

10. D. Purwaningtyas, I. Ardiansyah, and W. Widayati, "Developing aviation smart campus through digital transformation strategy: Case study at indonesia aviation polytechnic," *Journal of Innovation in Educational and Cultural Research*, vol. 3, pp. 177–184, Feb. 2022.
11. G. Vial, "Understanding digital transformation: A review and a research agenda," *The Journal of Strategic Information Systems*, vol. 28, no. 2, pp. 118–144, Jun. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0963868717302196.
12. J. S. Rha and H.-H. Lee, "Research trends in digital transformation in the service sector: A review based on network text analysis," *Service Business*, vol. 16, no. 1, pp. 77–98, Mar. 2022. [Online]. Available: https://doi.org/10.1007/s11628-022-00481-0
13. L. Xue, Q. Zhang, X. Zhang, and C. Li, "Can digital transformation promote green technology innovation?" *Sustainability*, vol. 14, no. 7497, 2022. [Online]. Available: https://www.mdpi.com/2071-1050/ 14/12/7497
14. G. A. Gellert, S. P. Kelly, E. W. Wright, and L. C. Keil, "Zero Trust and the future of cybersecurity in healthcare delivery organizations," *Journal of Hospital Administration*, vol. 12, no. 1, p. 1, Feb. 2023. [Online]. Available: https://www.sciedupress.com/journal/index.php/jha/article/view/22909
15. Y. Maleh and B. Mellal, "Digital transformation and cybersecurity in the context of COVID-19 proliferation," *IEEE Technology Policy and Ethics*, vol. 6, no. 5, pp. 1–4, 2021.
16. D. Kurniawan and R. M. Arti, "Comparative study of a cybersecurity curriculum to support digital transformation in the public sector," *Iapa Proceedings Conference*, pp. 547–576, 2020. [Online]. Available: https://journal.iapa.or.id/proceedings/article/view/427
17. A. Kuzior, T. Vasylieva, O. Kuzmenko, V. Koibichuk, and P. Brozÿek, "Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 8, no. 195, 2022. [Online]. Available: https://www.mdpi.com/2199-8531/8/4/195.
18. M. Mijwil, Y. Filali, M. Aljanabi, M. Bounabi, and H. AlShahwani, "The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment," *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 1–6, Jan. 2023. [Online]. Available: https://journals.mesopotamian.press/index.php/CyberSecurity/article/view/27
19. "Hacking Training For The Best." [Online]. Available: https://www.hackthebox.euhttps://www.hackthebox.com
20. "TryHackMe |Cyber Security Training." [Online]. Available: https://tryhackme.com/
21. "OverTheWire: Wargames." [Online]. Available: https:// overthewire.org/wargames/
22. "PentesterLab: Learn Web Penetration Testing: The Right Way." [Online]. Available: https://pentesterlab.com/
23. "Vulnerable By Design∼VulnHub." [Online]. Available: https://www.vulnhub.com/
24. "ChatGPT." [Online]. Available: https://openai.com/chatgpt
25. L. Weidinger, J. Uesato, M. Rauh, C. Griffin, P.-S. Huang, J. Mellor, A. Glaese, M. Cheng, B. Balle, A. Kasirzadeh, C. Biles, S. Brown, Z. Kenton, W. Hawkins, T. Stepleton, A. Birhane, L. A. Hendricks, L. Rimell, W. Isaac, J. Haas, S. Legassick, G. Irving, and I. Gabriel, "Taxonomy of risks posed by language models," in *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, ser. FAccT '22. New York, NY, USA: Association for Computing Machinery, 2022, pp. 214–229. [Online]. Available: https://doi.org/10.1145/3531146.3533088
26. M. Zipperle, F. Gottwalt, E. Chang, and T. Dillon, "Provenance-based intrusion detection systems: A survey," *Acm Computing Surveys*, vol. 55, no. 7, Dec. 2022. [Online]. Available: https://doi.org/10.1145/3539605
27. M. Zipperle, F. Gottwalt, Y. Zhang, O. Hussain, E. Chang, and T. Dillon, "A conceptual framework for automated rule generation in provenance-based intrusion detection systems," in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2022, pp. 1–4. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212623002661