**International Journal of Multidisciplinary Research and Development**
**www.allsubjectjournal.com**
**ISSN Online: 2349-4182 ISSN Print: 2349-5979**
**Received: 09-10-2023, Accepted: 25-10-2023, Published: 11-11-2023**
**Volume 10, Issue 11, 2023, Page No. 73-78**

# Understanding cybersecurity in the digital age: Systematic literature review

**Bader Lafi Almutairi[1], Omar Lafi Almutairi[2]**
[1] Department of Accounting, College of Business Administration, International University of Science and Technology in Kuwait, Al-Ardiya, Kuwait
[2] Ministry of Electricity, Water & Renewable Energy, Kuwait

**Abstract**
This study aims to provide a systematic literature review for understanding cybersecurity in the digital age. As technology continues to advance, so do the sophistication and frequency of cyber threats. The digital age has brought about a complex and evolving cyber threat landscape, encompassing a wide array of threats, including malware, phishing, ransomware, and advanced persistent threats. These threats are constantly evolving, requiring a proactive and adaptive cybersecurity approach. The increasing interconnectivity of devices, networks, and systems heightens the potential impact of cyber threats. A single vulnerability can have cascading effects across various sectors, highlighting the need for comprehensive cybersecurity strategies. Human error remains a significant factor in cybersecurity breaches, emphasizing the importance of education, training, and promoting a culture of security within organizations and society at large. Moreover, governments and international bodies are continually enhancing cybersecurity regulations to enforce compliance and encourage a higher standard of cybersecurity across industries. Compliance with these regulations is critical to maintaining trust and avoiding legal repercussions.

**Keywords:** Understanding cybersecurity, Systematic literature, digital age

## Introduction

In today's interconnected world, where information flows seamlessly across digital networks, the importance of cybersecurity cannot be overstated. As our reliance on technology grows, so does the need to safeguard our digital assets from a myriad of threats (De Arroyabe *et al*., 2023) [11]. Cybersecurity, a dynamic and ever-evolving field, plays a crucial role in protecting individuals, organizations, and nations from the potential harms of the digital landscape. At its core, cybersecurity encompasses the practices, technologies, and processes designed to safeguard computer systems, networks, and data from unauthorized access, attacks, and damage. It is a multidisciplinary field that combines elements of computer science, risk management, and law to create a robust defense against an ever-expanding array of cyber threats (Alsharida *et al*., 2023) [5].

The increasing digitization of our daily lives has made cybersecurity a cornerstone of our collective safety and privacy. From personal information stored on our devices to critical infrastructure powering nations, virtually every aspect of modern society relies on secure and resilient digital systems. A breach in cybersecurity can have far-reaching consequences, ranging from financial loss and identity theft to national security threats (Carley, 2020) [8]. As we continue to navigate the complexities of the digital age, a proactive and comprehensive approach to cybersecurity is essential. Whether on an individual or organizational level, understanding and implementing robust cybersecurity measures are paramount to fostering a secure and resilient digital ecosystem. Only through collective awareness, continuous learning, and technological innovation can we effectively mitigate the risks posed by cyber threats and ensure a safer digital future (Taherdoost, 2022) [33].

## Key Concepts

- **Confidentiality:** Ensuring that sensitive information is accessible only to authorized individuals or systems.
- **Integrity:** Maintaining the accuracy and reliability of data by protecting it from unauthorized tampering or alteration.
- **Availability:** Ensuring that systems and data are consistently accessible and operational, minimizing downtime and disruptions.
- **Authentication:** Verifying the identity of users and systems to prevent unauthorized access.
- **Authorization:** Granting appropriate access permissions based on authenticated identities.
- **Encryption:** Securing data by converting it into a code that can only be deciphered with the proper keys.
- **Challenges and Evolving Threat Landscape:** The landscape of cybersecurity is in constant flux, with cyber threats becoming more sophisticated and diverse. From ransomware attacks to social engineering tactics, cybersecurity professionals must stay ahead of the curve to effectively protect against emerging threats. The interconnected nature of global networks also means that collaboration and information sharing are critical in developing effective defense strategies.

## Historical Evolution of Cybersecurity

The history of cybersecurity is like a thrilling novel with constant plot twists. It all began in the early days of computing when security concerns were limited to physical access controls. As technology advanced, so did the threats. Let me take you on a brief journey through the historical evolution of cybersecurity (Dawson *et al*., 2021) [10].

**1. 1950s-1960s: The Dawn of Computers**
The concept of cybersecurity didn't exist, but early computers faced threats like physical theft or espionage.

**2. 1970s: Birth of Hacking**
As computers became more interconnected, the first hackers emerged. Notably, the term "hacker" was more benign, referring to those who explored the limits of systems.

**3. 1980s: Malicious Software Emerges**
The '80s saw the rise of computer viruses and malware. The infamous Morris Worm in 1988 was a wake-up call, highlighting the vulnerability of interconnected systems.

**4. 1990s: Internet Explosion**
The internet boom brought new opportunities and challenges. Cybersecurity efforts intensified with the development of firewalls and antivirus software.

**5. Early 2000s: Rise of Cybercrime**
Cybercrime became more organized and sophisticated. The infamous Code Red and Nimda worms wreaked havoc, emphasizing the need for better cybersecurity practices.

**6. Mid-2000s: A Focus on Compliance**
Regulatory frameworks like HIPAA and Sarbanes-Oxley mandated better data protection practices. The Payment Card Industry Data Security Standard (PCI DSS) also emerged.

**7. 2010s: Advanced Persistent Threats (APTs)**
Nation-state cyberattacks, such as Stuxnet, highlighted the emergence of APTs. Cybersecurity became a major concern for governments and corporations alike.

**8. Present and Beyond: Cloud, IoT, and AI**
The current landscape is marked by the challenges of securing cloud environments, the proliferation of Internet of Things (IoT) devices, and the use of Artificial Intelligence (AI) in cyber attacks and defense.

Throughout this evolution, cybersecurity has transitioned from a reactive approach to a more proactive and risk-based strategy. It's a continuous cat-and-mouse game between defenders and attackers, with each technological advancement opening new possibilities and challenges (Afenyo & Caesar, 2023) [1].

**Current and potential cyber threats**
Cyber threats continue to evolve and pose significant risks to individuals, businesses, governments, and organizations worldwide. The following discussion shows the current cyber threats and potential cyber threats based on historical trends and known risks up to this point.

**1. Current cyber threats**
Ransomware Attacks: Ransomware attacks involve encrypting a victim's data and demanding a ransom for decryption keys. The threat actors threaten to permanently delete or publish the data if the ransom is not paid. Ransomware attacks have been a pervasive and growing threat, targeting organizations of all sizes, including critical infrastructure, healthcare, government agencies, and educational institutions (Papakonstantinou, 2022) [25]. Phishing and Social Engineering: Phishing attacks remain a prevalent threat where cybercriminals use deceptive emails, messages, or phone calls to trick individuals into revealing sensitive information like passwords, credit card details, or login credentials. Social engineering techniques are often combined with phishing to manipulate individuals into performing specific actions) Almansoori, Al-Emran & Shaalan, 2023) [4].
Supply Chain Attacks: Attackers target the software supply chain to compromise widely used applications or systems. By injecting malware or vulnerabilities into the software development process, they can distribute malicious updates to unsuspecting users (Sebastian, 2023) [29]. Zero-Day Exploits: Zero-day vulnerabilities are software vulnerabilities that are unknown to the vendor and, therefore, have no patch available. Exploiting these vulnerabilities allows attackers to compromise systems and networks, often with severe consequences (Turk *et al*., 2022) [35].
Advanced Persistent Threats (APTs): APTs are sophisticated, long-term cyberattacks carried out by well-funded and organized threat actors, often state-sponsored. APTs focus on stealing sensitive data, conducting espionage, or disrupting critical infrastructure (Wylde *et al*., 2022) [37]. IoT and OT (Operational Technology) Vulnerabilities: The proliferation of Internet of Things (IoT) devices and the convergence of IT and OT networks have expanded the attack surface. Insecure IoT and OT devices present opportunities for attackers to exploit vulnerabilities and gain unauthorized access to critical systems (Hepfer & Powell, 2020) [17].

**2. Potential cyber threats**
**AI-Powered Attacks:** As artificial intelligence (AI) and machine learning (ML) technologies advance, cybercriminals may leverage them to enhance attacks, evade detection, and automate targeted attacks (Stobert *et al*., 2020) [32]. 5G Network Vulnerabilities: The rollout of 5G networks introduces new security challenges, such as increased attack surface, higher data speeds, and potential vulnerabilities in network architecture and protocols (Garcia-Perez *et al*., 2023) [14].

**Quantum Computing Threats:** Quantum computing could render current encryption algorithms obsolete, posing a significant threat to data privacy and security. However, it's important to note that quantum-resistant cryptographic techniques are being developed to mitigate this risk (Coenraad *et al*., 2020) [9]. Deepfakes and Synthetic Media: Deepfake technology could be used to create convincing false audio and video content, enabling social engineering attacks and misinformation campaigns (Coenraad *et al*., 2020) [9]. Cyber-Physical Attacks: With the increased integration of technology in critical infrastructure (e.g., power grids, transportation systems), the potential for cyber-physical attacks, where digital compromises impact physical systems, is a growing concern (Jacob, Peters & Yang, 2020) [19].

To stay ahead of these threats, organizations and individuals should maintain strong cybersecurity measures, including regular software updates, employee training, multi-factor authentication, and a robust incident response plan. Additionally, collaboration between industry, government, and international organizations is crucial to effectively address and mitigate these evolving cyber threats (Goupil *et al*., 2022) [15].

**Cybersecurity Frameworks and Standards**

Cybersecurity frameworks and standards provide guidelines, best practices, and structured approaches to help organizations manage and improve their cybersecurity posture. These frameworks aim to assist in identifying, protecting, detecting, responding to, and recovering from cyber threats and vulnerabilities. Here are some prominent cybersecurity frameworks and standards:

**NIST Cybersecurity Framework (CSF):** Created by the National Institute of Standards and Technology (NIST) in the United States, this framework provides a risk-based approach to managing cybersecurity. It emphasizes identifying, protecting, detecting, responding to, and recovering from cybersecurity risks (Awang *et al*., 2022) [6]. ISO/IEC 27001: This international standard specifies requirements for an Information Security Management System (ISMS). It provides a systematic approach for managing sensitive information and ensuring security, encompassing people, processes, and technology (Sleeman, Finin, & Halem, 2021) [31].

**CIS Controls:** The Center for Internet Security (CIS) Controls offers a prioritized set of actions for organizations to improve their cybersecurity posture and resilience against common cyber threats. It focuses on basic and advanced cybersecurity practices (Alahmari & Duncan, 2020) [2]. COBIT (Control Objectives for Information and Related Technologies): COBIT is a framework developed by ISACA, providing a comprehensive governance and management framework that aligns IT objectives with business goals. It helps organizations in effective governance and control of information and technology (Burrell, 2020) [7].

PCI DSS (Payment Card Industry Data Security Standard): PCI DSS is a standard that applies to organizations that handle cardholder information. It provides requirements for securing payment card transactions and ensuring the protection of cardholder data (Alferidah & Jhanjhi, 2020) [3]. HIPAA (Health Insurance Portability and Accountability Act): HIPAA sets the standard for protecting sensitive patient data. It outlines security and privacy rules to safeguard electronic protected health information (ePHI) within the healthcare industry (Reeves, Calic & Delfabbro, 2023) [26]. GDPR (General Data Protection Regulation): GDPR is a European Union regulation that focuses on data protection and privacy for individuals. It imposes strict requirements on how organizations collect, process, and handle personal data (Sarker *et al*., 2020) [28].

**FFIEC Cybersecurity Assessment Tool:** Developed by the Federal Financial Institutions Examination Council (FFIEC), this tool assists financial institutions in identifying risks and assessing their cybersecurity preparedness based on inherent risk and maturity control (Nwankpa & Datta, 2023) [23]. FAIR (Factor Analysis of Information Risk): FAIR is a framework for understanding, analyzing, and quantifying information risk in financial terms. It enables organizations to make more informed risk management decisions (Sarker *et al*., 2020) [28]. AICPA SOC Framework (System and Organization Controls): AICPA's SOC framework provides guidelines for reporting on controls at service organizations relevant to security, availability, processing integrity, confidentiality, and privacy (Nwankpa & Datta, 2023) [23].

Organizations should choose a cybersecurity framework or standard based on their specific industry, regulatory requirements, risk profile, and organizational needs. Often, a combination of these frameworks is used to develop a comprehensive and effective cybersecurity strategy. Additionally, compliance with these frameworks may be mandatory in certain industries or regions to meet legal and regulatory obligations.

**Government and Cybersecurity**

Government and cybersecurity are closely intertwined, as governments play a critical role in securing their nations' digital infrastructure, sensitive information, and overall cyberspace. Here's an overview of the relationship between government and cybersecurity, including their roles, responsibilities, challenges, and strategies:

**1. Government Roles and Responsibilities in Cybersecurity**

Governments create laws and regulations to govern cybersecurity practices, standards, and penalties for cybercrimes. These policies guide organizations and individuals in safeguarding digital assets. Protecting national security is a primary concern. Governments work to defend critical infrastructure, military assets, and government systems from cyber threats, which could have severe implications for a nation's safety and stability. On the other hand, governments facilitate collaboration and information sharing between various stakeholders, including public and private sectors, academia, international organizations, and other nations. This cooperation strengthens collective defense against cyber threats (Singh *et al*., 2023) [30].

Governments establish cybersecurity incident response teams and law enforcement agencies to investigate cyber incidents, prosecute cybercriminals, and provide assistance to affected entities. Governments educate the public on cybersecurity best practices, potential threats, and how to stay safe online. This helps create a cyber-literate population that can contribute to national cybersecurity. Moreover, governments invest in research and development to advance cybersecurity technologies, techniques, and strategies to stay ahead of evolving cyber threats (Lee & Chua, 2023) [22].

**2. Challenges in Government Cybersecurity**

Cyber threats are constantly evolving and becoming more sophisticated, challenging governments to keep pace with new attack vectors and techniques. Adequate funding is essential for robust cybersecurity measures, but budget constraints can limit the government's ability to implement and maintain effective cybersecurity programs. There is a shortage of skilled cybersecurity professionals. Governments need to invest in training programs and initiatives to bridge the skills gap. Cyber threats often transcend borders, requiring international cooperation and coordination. Governments must work together to combat cyber threats effectively. Balancing cybersecurity measures with individual privacy rights is a challenge. Governments need to strike a delicate balance to protect citizens' privacy while enhancing cybersecurity (Kianpour, Kowalski & Øverby, 2021) [21].

**3. Strategies for Effective Government Cybersecurity:**

- **Public-Private Partnerships:** Foster collaboration between the government and private sector to share threat intelligence, best practices, and resources to strengthen the overall cybersecurity posture.
- **Regular Risk Assessments:** Continuously assess and identify cybersecurity risks to prioritize actions and allocate resources effectively.
- **Education and Awareness:** Invest in public awareness campaigns and educational programs to enhance cybersecurity knowledge and encourage responsible online behavior.
- **International Cooperation:** Collaborate with other countries to share threat intelligence, harmonize regulations, and coordinate efforts to mitigate global cyber threats.
- **Incentives for Compliance:** Provide incentives for organizations and individuals to comply with cybersecurity regulations and best practices, encouraging a culture of security.
- **Investment in Research and Innovation:** Fund research and innovation in cybersecurity to stay ahead of evolving threats and foster technological advancements.

Government involvement in cybersecurity is essential to protect national interests, critical infrastructure, and citizen data. Collaboration, regulation, education, and international cooperation are key pillars in building a resilient and secure cyberspace.

**Future Trends in Cybersecurity**

Predicting precise future trends in cybersecurity is challenging due to the evolving nature of technology and the rapidly changing threat landscape. However, we can discuss potential trends based on patterns and emerging technologies. AI and Machine Learning in Cybersecurity: AI and machine learning will continue to play a crucial role in identifying and mitigating cyber threats. These technologies can enhance threat detection, automate responses, and improve overall security posture by analyzing large volumes of data to identify patterns and anomalies (Franco, Granville & Stiller, 2023) [13].

**Zero Trust Architecture (ZTA):** Zero Trust Architecture is gaining momentum, focusing on continuous verification and not trusting anything inside or outside the organization's perimeters. It's about authenticating and authorizing users and devices regardless of their location, emphasizing strict access control and data segmentation (Offner *et al*., 2020) [24]. Quantum-Safe Cryptography: With the potential arrival of quantum computers that can break current encryption algorithms, there's a growing emphasis on developing and adopting quantum-resistant or quantum-safe cryptographic algorithms to ensure data security in the post-quantum era (Trumbach *et al*., 2023) [34].

**5G Security:** As 5G networks become more widespread, cybersecurity will need to adapt to the unique challenges and vulnerabilities that come with the increased speed, capacity, and interconnectedness. Ensuring the security and privacy of data transmitted over 5G networks will be a priority (Wong *et al*., 2022) [36]. Edge Computing Security: Edge computing brings processing closer to data sources, reducing latency and improving performance. However, this decentralization introduces security concerns, and cybersecurity measures will need to adapt to secure the distributed infrastructure and devices at the edge of the network (Hong & Furnell, 2021) [18].

**Cloud Security Enhancements:** Cloud adoption will continue to rise, necessitating advancements in cloud security technologies and practices. This includes better authentication and access control mechanisms, encryption, and data privacy measures to ensure secure cloud usage (Ham, 2021) [16]. Biometric Authentication and Behavioral Analysis: Biometric authentication and behavioral analysis technologies will gain traction as more secure methods of verifying identities. This can include fingerprint recognition, facial recognition, keystroke dynamics, and other biometric and behavioral patterns for authentication (Formosa, Wilson & Richards, 2021) [12]. Supply Chain Security: Cybersecurity will increasingly focus on securing the supply chain, ensuring that third-party vendors and partners meet specific security requirements to mitigate the risk of attacks through the supply chain (Rohan *et al*., 2021) [27]. Regulatory Compliance and Privacy Concerns: Stricter regulations regarding data privacy and protection will continue to be introduced worldwide. Compliance with these regulations, such as GDPR, CCPA, and others, will be a priority for organizations to avoid legal consequences. Cybersecurity Skills and Workforce Development: The demand for skilled cybersecurity professionals will remain high. Efforts to bridge the cybersecurity skills gap will continue, focusing on training and education programs to cultivate a competent and diverse cybersecurity workforce (Kavak *et al*., 2021) [20].

**Conclusion and Recommendations**

In the rapidly evolving digital age, cybersecurity has become a paramount concern for individuals, organizations, and governments. As technology continues to advance, so do the sophistication and frequency of cyber threats. The digital age has brought about a complex and evolving cyber threat landscape, encompassing a wide array of threats, including malware, phishing, ransomware, and advanced persistent threats (APTs). These threats are constantly evolving, requiring a proactive and adaptive cybersecurity approach. The increasing interconnectivity of devices, networks, and systems heightens the potential impact of cyber threats. A single vulnerability can have cascading effects across various sectors, highlighting the need for comprehensive cybersecurity strategies.

Human error remains a significant factor in cybersecurity breaches, emphasizing the importance of education, training, and promoting a culture of security within organizations and society at large. Governments and international bodies are continually enhancing cybersecurity regulations to enforce compliance and encourage a higher standard of cybersecurity across industries. Compliance with these regulations is critical to maintaining trust and avoiding legal repercussions. On the other hand, rapid technological advancements, such as artificial intelligence

(AI), blockchain, and the Internet of Things (IoT), offer both opportunities and challenges. Leveraging these technologies to bolster cybersecurity while mitigating associated risks is crucial.

**Recommendations**

- Conduct regular and thorough risk assessments to identify vulnerabilities and potential threats.
- Develop a comprehensive cybersecurity strategy tailored to the organization's specific risks, industry, and technological environment.
- Implement continuous cybersecurity training for all employees to enhance their understanding of cyber threats and best practices.
- Foster a culture of cybersecurity awareness and responsibility within the organization.
- Implement a multi-layered defense strategy, including firewalls, intrusion detection systems, encryption, and access controls, to mitigate potential risks.
- Regularly update and patch systems and software to address known vulnerabilities.
- Develop and regularly test an incident response plan to efficiently and effectively respond to cyber incidents.
- Establish robust disaster recovery mechanisms to minimize downtime and data loss in case of a cyber-attack.
- Foster collaboration among industry stakeholders, government agencies, and international bodies to share threat intelligence and best practices.
- Encourage information sharing regarding cyber incidents to enhance collective preparedness and response.
- Prioritize data privacy and protection, ensuring compliance with relevant data protection laws and regulations.
- Implement encryption and access controls to safeguard sensitive information.
- Continuously monitor networks and systems for potential threats and anomalous activities.

Finally, safeguarding the digital age requires a holistic and proactive approach, encompassing technology, education, regulation, and collaboration. By prioritizing cybersecurity and implementing these recommendations, we can collectively work towards a more secure and resilient digital landscape.

**References**


1. Afenyo M, Caesar LD. Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management*,2023:*236*:106493.
2. Alahmari A, Duncan B. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, 2020, 1-5. IEEE.
3. Alferidah DK, Jhanjhi NZ. Cybersecurity impact over bigdata and iot growth. In *2020 International Conference on Computational Intelligence (ICCI)*, 2020, 103-108). IEEE.
4. Almansoori A, Al-Emran M, Shaalan K. Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Applied Sciences*,2023:*13*(9):5700.
5. Alsharida RA, Al-rimy BAS, Al-Emran M, Zainal A. A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 2023, 102258.
6. Awang N, Ganthan A, Samy LN, Hassan NH, Maarop N, Perumal S. Implementation of SARIMA algorithm in understanding cybersecurity threats in university network. *Journal of Positive School Psychology*,2022:*6*(3):8442-8451.
7. Burrell DN. Understanding the talent management intricacies of remote cybersecurity teams in covid-19 induced telework organizational ecosystems. *Land Forces Academy Review*,2020:*25*(3):232-244.
8. Carley KM. Social cybersecurity: an emerging science. *Computational and mathematical organization theory*,2020:*26*(4):365-381.
9. Coenraad M, Pellicone A, Ketelhu DJ, Cukier M, Plane J, Weintrop D. Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. *Simulation & Gaming*,2020:*51*(5):586-611.
10. Dawson M, Bacius R, Gouveia LB, Vassilakos A. Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review*,2021:*26*(1):69-75.
11. De Arroyabe IF, Arranz CF, Arroyabe MF, de Arroyab, JCF. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security*,2023:*124:*102954.
12. Formosa P, Wilson M, Richards D. A principlist framework for cybersecurity ethics. *Computers & Security*,2021:*109*:102382.
13. Franco MF, Granville LZ, Stiller B. CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 2023, (1-6). IEEE.
14. Garcia-Perez A, Cegarra-Navarro JG, Sallos MP, Martinez-Caro E, Chinnaswamy A. Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*,2023:*121*:102583.
15. Goupil F, Laskov P, Pekaric I, Felderer M, Dürr A, Thiesse F. Towards understanding the skill gap in cybersecurity. In *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education*,2022:1:477-483.
16. Ham JVD. Toward a better understanding of "cybersecurity". *Digital Threats: Research and Practice*,2021:*2*(3):1-3.
17. Hepfer M, Powell TC. Make cybersecurity a strategic asset. MIT Sloan Management Review,2020:*62*(1):40-45.
18. Hong Y, Furnell S. Understanding cybersecurity behavioral habits: Insights from situational support. Journal of Information Security and Applications,2021:57:102710.
19. Jacob J, Peters M, Yang TA. Interdisciplinary cybersecurity: Rethinking the approach and the process. In National Cyber Summit (NCS) Research Track. Springer International Publishing, 2020, 61-74.
20. Kavak H, Padilla JJ, Vernon-Bido D, Diallo SY, Gore R, Shetty S. Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*,2021:*7*(1):tyab005.

21. Kianpour M, Kowalski SJ, Øverby H. Systematically understanding cybersecurity economics: A survey. *Sustainability*,2021:*13*(24):13677.
22. Lee CS, Chua YT. The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, 2023, 00111287231180093.
23. Nwankpa JK, Datta PM. Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security*,2023:*130*:103266.
24. Offner KL, Sitnikova E, Joiner K, MacIntyre CR. Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*,2020:*35*(4):556-585.
25. Papakonstantinou V. Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? *Computer Law & Security Review*,2022:*44:*105653.
26. Reeves A, Calic D, Delfabbro P. Generic and unusable" 1: Understanding employee perceptions of cybersecurity training and measuring advice fatigue. *Computers & Security*,2023:*128*:103137.
27. Rohan R, Funilkul S, Pal D, Chutimaskul W. Understanding of human factors in cybersecurity: A systematic literature review. In *2021 International Conference on Computational Performance Evaluation (ComPE*, 2021, 133-140). IEEE.
28. Sarker IH, Kayes ASM, Badsha S, Alqahtani H, Watters P, Ng A. Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*,2020:*7*:1-29.
29. Sebastian G. A descriptive study on metaverse: Cybersecurity risks, controls, and regulatory framework. *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)*,2023:*15*(1):1-14.
30. Singh T, Johnston AC, D'Arcy J, Harms PD. Stress in the cybersecurity profession: a systematic review of related literature and opportunities for future research. *Organizational Cybersecurity Journal: Practice, Process and People*, 2023.
31. Sleeman J, Finin T, Halem M. Understanding cybersecurity threat trends through dynamic topic modeling. *Frontiers in big Data*,2021:*4*:601529.
32. Stobert E, Barrera D, Homier V, Kollek D. Understanding cybersecurity practices in emergency departments. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, 1-8.
33. Taherdoost H. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*,2022:*11*(14):2181.
34. Trumbach CC, Payne DM, Walsh K. Cybersecurity in business education: The 'how to'in incorporating education into practice. *Industry and Higher Education*,2023:*37*(1):35-45.
35. Turk Ž, de Soto BG, Mantha BR, Maciel A, Georgescu A. A systemic framework for addressing cybersecurity in construction. *Automation in Construction*,2022:*133:*103988.
36. Wong LW, Lee VH, Tan GWH, Ooi KB, Sohal A. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*,2022:*66*:102520.
37. Wylde V, Rawindaran N, Lawrence J, Balasubramania R, Prakash E, Jayal A, *et al*. Cybersecurity, data privacy and blockchain: a review. *SN Computer Science*,2022:*3*(2):127.