

Ethical Considerations in Cybersecurity: Analyzing Supply Chain Attacks, Ransomware, and Open-Source Vulnerabilities

Ebone McCoy

*Capitol Technology University, Washington DC, USA
emccoy@captechu.edu*

Abstract: The increasing reliance on digital infrastructure and rapid expansion of cloud computing have significantly amplified cybersecurity risks. Although technical solutions to these challenges are being developed, the ethical implications of these risks are often overlooked. This study investigates the ethical dimensions of modern cybersecurity challenges, particularly in the context of high-profile cyberattacks such as SolarWinds (2020), Colonial Pipeline (2021), and the Log4j vulnerability (2021). These incidents underscore the moral responsibilities of organizations in securing their software supply chains, protecting personal data, and mitigating the broader social impact of cybercrime. This paper explores the role of ethical frameworks, such as deontological ethics, utilitarianism, and virtue ethics, in shaping cybersecurity policies and proposes actionable recommendations for integrating these ethical principles into cybersecurity strategies. By examining these threats through an ethical lens, this study aims to provide actionable insights for organizations, policymakers, and cybersecurity professionals to create more responsible and resilient digital environments.

Keywords: Cybersecurity Ethics, Privacy, Ransomware, Supply Chain Attacks, Software Vulnerabilities, Ethical Hacking, Zero Trust, Ethical Responsibility

Introduction

The rapid expansion of digital technology has resulted in unprecedented cybersecurity challenges. As software systems become more integrated and complex, cyberattacks are becoming increasingly sophisticated, with far-reaching consequences. High-profile breaches, such as the SolarWinds attack (2020), Colonial Pipeline ransomware incident (2021), and Log4j vulnerability (2021), have exposed critical weaknesses in security practices, often revealing a disregard for ethical responsibility in safeguarding systems and data (Camacho, 2024). These events highlight the ethical implications of cybersecurity practices, including the moral responsibility of organizations to protect sensitive information, ensure privacy, and maintain public trust (Bayya, 2022).

Despite technological advancements, cybersecurity professionals and organizations often face ethical dilemmas in managing risks, prioritizing security measures, and balancing operational efficiency with privacy concerns. As cybersecurity risks evolve, so must the ethical frameworks that guide the response strategies. Cybersecurity professionals must adopt a multidimensional framework that includes moral, ethical, and socio-economic responsibilities in addition to technical and operational considerations (Onwubiko & Ouazzane, 2022). Emerging technologies have transformed industries to be more effective and collaborative but have also increased dependencies on these platforms, which can cause extensive harm if exploited or hacked, raising ethical concerns. (Dhirani et al., 2023)

This study explores the intersection of ethics and cybersecurity, emphasizing the role of ethical decision-making in mitigating the risks posed by supply chain attacks, ransomware, and open-source vulnerabilities.

Problem Statement

Recent high-profile cyber incidents, such as the SolarWinds supply chain attack (2020), Colonial Pipeline ransomware attack (2021), and Log4j vulnerability (2021), have highlighted significant security gaps in modern software development, supply chain management, and access control

practices (Sam 2023; Ofte & Katsikas 2024; Alboqmi & Gamble 2025). Despite advancements in cybersecurity technologies, these attacks demonstrate that vulnerabilities persist in critical systems, often due to poor security practices and the lack of proactive risk management (Kurniawan, 2023). These breaches have severe implications not only for organizations, but also for society at large, affecting public trust, national security, and economic stability. (Sam, 2023).

The key issue lies in understanding why these vulnerabilities continue to exist, despite the proliferation of advanced cybersecurity tools and frameworks. (Kurniawan, 2023). Organizations often fail to adopt holistic, ethical security practices that go beyond mere compliance with regulatory requirements (Lee, 2021; Taylor & Whitty, 2023). Traditional security approaches that focus on reactive responses to attacks are increasingly inadequate for addressing evolving threats (Bold, et al., 2022). There is a need to explore how organizations can better integrate advanced ethical cybersecurity strategies, such as zero-trust architecture, AI-driven threat detection, and proactive incident response plans to prevent, detect, and mitigate cyber risks (Kang et al., 2023; Aryal, 2024; Taherdoost et al., 2025). This context of persistent vulnerabilities and ethical oversights underscores the necessity to investigate ethical frameworks in cybersecurity.

Purpose of Study

This study aims to investigate persistent cybersecurity vulnerabilities and evaluate the ethical and practical shortcomings of current approaches to securing software development processes, supply chains, and critical infrastructure. Through this examination, this study seeks to provide actionable recommendations for improving cybersecurity resilience and addressing the ethical responsibilities of organizations in protecting sensitive data and systems from emerging threats. This study begins by identifying the ethical challenges in cybersecurity, then examines specific high-profile incidents to illustrate these challenges in real-world contexts.

Literature Review

The literature on cybersecurity often focuses on technical solutions to cyber threats, but less attention is given to the ethical implications of these threats. Recent cyberattacks have raised critical questions regarding the ethical responsibilities of organizations in securing their digital assets and protecting users' privacy.

Precautionary Principle

The precautionary principle is a risk management strategy that advocates for ethical preventive action in the face of uncertainty, aiming to minimize potential harm to human health or the environment even when scientific evidence is inconclusive (Dhirani et al., 2023). In the realm of cybersecurity, this principle underscores the importance of proactively addressing potential threats before they materialize. For instance, organizations are encouraged to implement advanced security measures and conduct regular vulnerability assessments to safeguard against emerging cyber threats (Camacho, 2024). This proactive stance is crucial in mitigating risks associated with sophisticated cyberattacks, such as supply chain compromises and ransomware incidents (Beerman et al., 2023).

Applying the precautionary principle in cybersecurity involves recognizing the ethical responsibility of organizations to protect sensitive information and maintain public trust. High-profile breaches, such as the SolarWinds attack in 2020 and the Colonial Pipeline ransomware incident in 2021, have highlighted the consequences of inadequate security practices (Beerman et al., 2023). These events emphasize the need for organizations to adopt a precautionary approach by strengthening their security protocols and ensuring the integrity of their software supply chains (Camacho, 2024). By doing so, they can prevent potential harm to users and the broader society, aligning with ethical frameworks that prioritize the well-being of stakeholders (Dhirani et al., 2023).

Prospect theory

Prospect theory, developed by Kahneman and Tversky, describes how individuals assess potential losses and gains, often valuing losses more heavily than equivalent gains (Kahneman & Tversky, 1979). In cybersecurity, this theory can explain ethical decision-making behaviors related to risk management and investment in security measures. Organizations may exhibit loss aversion by overemphasizing the potential negative outcomes of cyber threats, leading to either excessive caution or underinvestment in necessary security protocols due to the fear of incurring costs without immediate benefits (Kozhuharova et al., 2022).

Understanding prospect theory is essential for developing effective cybersecurity strategies that balance the perceived risks and rewards. By acknowledging cognitive biases such as loss aversion, organizations can design policies that encourage rational investment in security measures, even when immediate benefits are not apparent (Kozhuharova et al., 2022). This approach ensures a more resilient cybersecurity posture, as it aligns ethical decision-making processes with the actual risk landscape rather than subjective perceptions influenced by cognitive biases (Kahneman & Tversky, 1979).

Just Culture Model

The Just Culture model promotes an organizational environment that encourages the reporting of errors and near-misses without fear of punitive action, thereby enhancing safety and accountability (Hidayatulloh & Rahman, 2025). In the context of cybersecurity, adopting a Just Culture fosters an atmosphere where professionals feel empowered to disclose vulnerabilities and mistakes, facilitating continuous learning and systemic improvements (Nasir et al., 2024). By focusing on understanding the root causes of security incidents rather than assigning individual blame, organizations can ethically develop more effective strategies to prevent future breaches and enhance overall security posture (Hidayatulloh & Rahman, 2025).

Implementing a Just Culture in cybersecurity involves establishing clear distinctions between human errors, at-risk behaviors, and reckless actions, allowing for appropriate responses to each (Nasir et al., 2024). This framework not only improves incident reporting but also contributes to building trust within the organization, leading to more robust and proactive cybersecurity practices (Hidayatulloh & Rahman, 2025). By fostering an ethical environment where employees are encouraged to share information about potential security issues without fear of retribution, organizations can better identify systemic weaknesses and address them effectively (Nasir et al., 2024).

Ethical Implications of Cybersecurity Threats

Cybersecurity threats such as supply chain attacks, ransomware, and vulnerabilities in open-source software not only endanger organizations security but also raise fundamental ethical concerns (Krivokapić et al., 2023). For instance, the SolarWinds attack, which compromised the software used by thousands of organizations worldwide, illustrates the moral responsibility of companies to ensure the integrity of their software supply chains. The Colonial Pipeline ransomware attack further emphasizes the consequences of weak security practices, such as inadequate access control mechanisms, which directly impacted critical infrastructure and public resources.

Ethical considerations in cybersecurity go beyond technical failures to encompass privacy, fairness, and corporate responsibility. For instance, organizations that neglect user data security or prioritize efficiency over security contribute to the erosion of public trust and the exploitation of vulnerable populations (Spanca & Salihu, 2024). These challenges underscore the importance of integrating ethical frameworks into cybersecurity practices to ensure responsible decision-making in response to emerging threats (Kozhuharova et al., 2022). This review of ethical frameworks underscores the complexity of integrating ethical

considerations into cybersecurity practices. Despite extensive discussion in literature, there remains a gap in practical application, which this study aims to address through its methodology.

Ethical Frameworks in Cybersecurity

Ethical considerations in cybersecurity typically revolve around three major schools of thought: deontological ethics, utilitarianism, and virtue ethics. (Manjikian, 2017; Loi & Christen, 2020). Each provides a different lens through which organizations can evaluate and mitigate risks. Together, these frameworks underline the necessity of embedding ethical decision-making in cybersecurity strategies (Kozhuharova et al., 2022).

- **Deontological Ethics:** Deontological ethics assert that organizations are morally obligated to follow specific duties, such as ensuring the security of systems and user privacy (Kim et al., 2021). This framework supports the principle that cybersecurity measures should be implemented as a matter of moral duty regardless of potential consequences. Ensuring that software updates are free from malicious code should be viewed as a moral obligation (Kim et al., 2021).
- **Utilitarianism:** Utilitarianism evaluates actions based on their consequences, aiming to maximize overall well-being and reduce harm (Dupuis & Renaud, 2020). In cybersecurity, utilitarian principles can justify investments in advanced security measures if they significantly reduce the overall harm caused by cyberattacks, such as data breaches or ransomware attacks (Rajamäki & Hämäläinen, 2021; Reddy Piduru, 2021). However, balancing the costs of security measures with their potential benefits is crucial (Loi & Christen, 2020).
- **Virtue Ethics:** Virtue ethics emphasizes the character and intentions of the individuals involved in decision-making (Ohlhorst, 2023). In cybersecurity, this framework emphasizes the moral character of professionals and their commitment to responsible practices (Nasir et al., 2024). Virtue ethics advocate for integrity and moral accountability in cybersecurity professionals and organizations. For example, promptly reporting vulnerabilities, even if it harms an organization's reputation, demonstrates integrity (Hidayatulloh & Rahman, 2025).

Methodology

This study employed a historical analysis research approach to analyze recent cyberattacks through an ethical lens. This research draws on case studies, industry reports, and scholarly literature to assess the ethical implications of cybersecurity practices. By integrating moral philosophy with cybersecurity frameworks, this study aims to provide a comprehensive understanding of how ethical principles can guide the development of robust and responsible cybersecurity strategies.

Case Studies and Ethical Analysis

1. SolarWinds Supply Chain Attack (2020): The SolarWinds attack was a supply chain breach that compromised the security of over 18,000 organizations globally. Ethical lapse occurred when SolarWinds failed to ensure the integrity of their software development process, allowing malicious code to be inserted into its widely used Orion software. From a deontological perspective, SolarWinds had a moral obligation to secure its systems. From an ethical perspective, the attack raises serious concerns regarding corporate responsibility for securing third-party software. This oversight violated the trust of clients, who assumed that their software was secure. This breach underscores the ethical obligation of companies to ensure the security of their supply chains and to prevent the exploitation of vulnerabilities that could have widespread consequences.

2. Colonial Pipeline Ransomware Attack (2021): The Colonial Pipeline Attack in April 2021, disrupted approximately 45 % of fuel supplies in the U.S. East Coast (Beerman et al., 2023). The attack exploited weak security controls, including the failure to implement multi-factor authentication (MFA) on critical VPN accounts (Mittal, 2024). This incident highlights the ethical responsibility of organizations in implementing stringent access control measures, particularly in critical infrastructure. From a broader ethical perspective, this attack demonstrates how security failures can disproportionately affect vulnerable populations, particularly those reliant on critical infrastructure.

3. Log4j Vulnerability (2021): The Log4j vulnerability, disclosed on December 10, 2021, exposed a critical flaw in the widely used open-source logging library, affecting millions of systems globally (Hiesgen et al., 2024). This zero-day exploit allowed attackers to execute remote code (RCE) on vulnerable systems (Hiesgen et al., 2024). The issue primarily stems from two ethical challenges: the governance of open-source software and the frequent absence of oversight in its deployment by organizations (Precious, 2025). Open-source software carries inherent ethical responsibilities for both developers and organizations.

The Log4j incident calls for stronger ethical guidelines for the management and oversight of open-source dependencies. Developers must ensure transparent and secure coding practices, while organizations must vet the software thoroughly before deploying it in critical systems (IBM, n.d.). Organizations adopting virtue ethics should exhibit foresight and accountability, proactively patching vulnerabilities rather than waiting for exploits to emerge (Feng & Lubis, 2022). Ethically grounded oversight mechanisms and tighter regulation over third-party software libraries could have mitigated the chaos caused by this vulnerability (IBM, n.d.).

Emerging Ethical Issues in Cybersecurity

The intersection of cybersecurity and emerging technologies such as artificial intelligence, Ransomware-as-a-Service (RaaS), and quantum computing introduces complex ethical issues that require careful consideration. While offering enhanced capabilities, these technologies also present new challenges related to bias, accountability, and potential misuse (Kulothungan, 2024).

Artificial Intelligence in Cybersecurity

AI-driven cybersecurity tools offer significant advantages in terms of threat detection and incident response. However, they also raise ethical concerns regarding bias, fairness, and accountability (Ilieva & Stoilova, 2024). Algorithmic bias in AI systems can lead to discriminatory outcomes, emphasizing the need for ethical guidelines to ensure transparency and prevent unfair practices (Blancaflor et al., 2024). To mitigate these risks, the adoption of AI should prioritize fairness, accountability, transparency, data privacy concerns and address potential biases (Blancaflor et al., 2024).

Ransomware-as-a-Service (RaaS)

The proliferation of RaaS platforms has significantly lowered the barrier to entry for cybercriminals, leading to a surge in ransomware attacks (Singh et al., 2024). This trend poses significant ethical concerns regarding the responsibilities of technology providers hosting these platforms. RaaS platforms enable even individuals with limited technical skills to launch sophisticated attacks, highlighting the ethical implications of providing the tools for such malicious activities (Gyimah et al., 2024).

Quantum Computing

The development of quantum computing poses a significant future ethical challenge by potentially undermining traditional encryption methods. Quantum computers can break current

encryption algorithms, threatening the privacy and security of sensitive information (Singh et al., 2024). To address this, there is a need to develop and implement quantum-resistant cryptographic solutions to safeguard digital communications and data integrity in the quantum era (Seiler, 2024).

Conclusion and Recommendations

As cyber threats continue to evolve, it is essential for cybersecurity practices to be grounded in ethical decision-making. This paper emphasizes the need for organizations to adopt ethical frameworks in their cybersecurity strategies. Organizations must prioritize the moral responsibility of securing software supply chains, protecting user privacy, and ensuring public trust. Furthermore, greater investment in cybersecurity education and training is critical for bridging the skills gap and fostering a culture of ethical responsibility within the cybersecurity profession.

Cybersecurity intricately interweaves technological safeguards with moral imperatives, emphasizing the need for ethical responsibility at every level. Many organizations are recognizing the need for enhanced cybersecurity measures, such as network segmentation and multi-factor authentication, to protect against evolving ransomware attacks (Elete, 2024). The cases of SolarWinds, Colonial Pipeline, and Log4j vividly illustrate the grave ethical lapses that exacerbate societal harm when organizations prioritize short-term operational efficiencies over robust security. Adopting ethical frameworks such as deontological, utilitarian, and virtue ethics is not merely an advisable strategy but a moral imperative in safeguarding public trust, privacy, and critical infrastructure. If organizations commit to proactive ethical cybersecurity practices, including zero-trust architecture, responsible use of AI, and rigorous supply chain security, they can mitigate technical risks and uphold their moral duty to society. Ethical stewardship is essential for fostering a secure and trustworthy digital ecosystem in this rapidly evolving cyber landscape.

Recommendations

1. **Policy and Procedure Considerations:** Privacy and security policies should be developed to protect individual rights and ensure fairness.
2. **Adopt Comprehensive Ethical Frameworks:** Organizations should explicitly integrate ethical frameworks such as deontology (emphasizing moral duties), utilitarianism (focusing on outcomes), and virtue ethics (highlighting character and moral integrity) into their cybersecurity strategies to ensure that decisions balance technical efficacy and moral accountability.
3. **Embed Ethical Decision-Making Training:** Regularly train cybersecurity professionals and organizational leaders in ethical decision-making, focusing on the broader societal implications of cybersecurity practices and emphasizing moral responsibilities over short-term operational gains.
4. **Implement Zero-Trust Security Architecture:** Employ a zero-trust security model that strictly controls and continuously verifies user access and system interactions, thereby preventing unauthorized access and reducing vulnerabilities from internal and external threats.
5. **Utilize Ethical AI Governance:** Establish clear ethical guidelines and oversight committees to govern the deployment and operation of AI-based cybersecurity systems, ensuring transparency, accountability, fairness, and the mitigation of biases.
6. **Strengthen Supply Chain Integrity:** Develop rigorous oversight and verification processes for software and technology providers, mandating regular security audits and ethical compliance assessments to prevent vulnerabilities similar to those exploited in the SolarWinds and Log4j cases.

7. **Prioritize Long-Term Security Investment:** Shift organizational perspectives from immediate cost-benefit analyses towards long-term security investments, thereby reducing susceptibility to breaches such as the Colonial Pipeline attack that exploited weak short-term security measures.
8. **Cultivate a Just Culture:** Promote an organizational culture in which employees feel empowered to report vulnerabilities, errors, or unethical cybersecurity practices without fear of reprisal, fostering continuous improvement and robust risk management.
9. **Integrate Cyber Ethics into Corporate Values:** Cybersecurity ethics are clearly defined as an organizational core value, aligning security policies with broader corporate social responsibility commitments to uphold public trust, safeguard privacy, and protect critical infrastructure.
10. **Continuous Risk Assessment and Ethical Audits:** Regularly perform ethical cybersecurity audits alongside technical evaluations to identify emerging ethical risks, proactively address potential security gaps, and ensure alignment with evolving ethical standards.
11. **Foster Collaborative Stakeholder Engagement:** Actively involves diverse stakeholders, including customers, policymakers, community representatives, and technical experts, in discussions on cybersecurity strategies and ethical considerations, reinforcing a shared responsibility for maintaining a secure and trustworthy digital environment.

References

- Alboqmi, R., & Gamble, R. F. (2025). Enhancing Microservice Security Through Vulnerability-Driven Trust in the Service Mesh Architecture. *Sensors*, 25(3), 914. <https://doi.org/10.3390/s25030914>
- Aryal, N. (2024). *Evaluating Context-aware, Continuous and Device Authentication for Zero Trust Architecture Adoption: A Quantitative Study among IT Professionals*. <https://search.proquest.com/openview/96499e601529b5156a8b952804c17b9d/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y>
- Bayya, A. K. (2022). Advocating Ethical Data Management and Security. In *International Journal of Scientific Research in Computer Science Engineering and Information Technology* (p. 396). <https://doi.org/10.32628/cseit225541>
- Beerman, J., Falter, Z., Bhunia, S., & Berent, D. (2023, May 1). A review of Colonial Pipeline ransomware attack. *Proceedings of the 2023 IEEE/ACM International Symposium on Cluster, Cloud, and Internet Computing (CCGrid)*. <https://doi.org/10.1109/CCGRIDW59191.2023.00017>
- Blancaflor, E. B., Eleccion, F. G., Ferry, F. L., & Oplado, J. P. (2024, August). Ethical use of AI for cybersecurity and facing digital threats in the Philippines. In *Proceedings of the 2024 IEEE 7th International Conference on Computer and Communication Engineering Technology (CCET)*. IEEE. <https://doi.org/10.1109/CCET62233.2024.10837790>
- Bold, R., Al-Khateeb, H., & Ersotelos, N. (2022). Reducing False Negatives in Ransomware Detection: A Critical Evaluation of Machine Learning Algorithms. *Applied Sciences*, 12(24), 12941. <https://doi.org/10.3390/app122412941>
- Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, 3(1), 143–154. <https://doi.org/10.60087/jaigs.v3i1.75>
- Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors*, 23(3), 1151. Multidisciplinary Digital Publishing Institute. <https://doi.org/10.3390/s23031151>
- Dupuis, M., & Renaud, K. (2020). Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology*, 23(3), 265–284. <https://doi.org/10.1007/s10676-020-09560-0>
- Elete, T. (2024). Impact of ransomware on industrial control systems in the oil and gas sector: Security challenges and strategic mitigations. *Computer Science & IT Research Journal*. <https://doi.org/10.51594/csitjr.v5i12.1759>
- Feng, S., & Lubis, M. (2022). Defense-in-depth security strategy in Log4j vulnerability analysis. *Proceedings of the 2022 International Conference on Advancement in Data Science, E-Learning and Information Systems (ICADEIS)*. IEEE. <https://doi.org/10.1109/ICADEIS56544.2022.10037384>

- Gyimah, F. O., Ofori-Mensah, E., Boowuo, H., & Aggrawal, S. (2024, October). *Friend or foe? AI and the evolving landscape of Ransomware-as-a-Service (RaaS)*. In *Proceedings of the 2024 Cyber Awareness and Research Symposium (CARS)* (pp. 1–5). IEEE. <https://doi.org/10.1109/CARS61786.2024.1077871>
- Hidayatulloh, S., & Rahman, A. B. A. (2025). Balancing Cybersecurity Policies and Institutional Ethics: A Legal and Cultural Perspective on Higher Education Frameworks. *Revista De Gestão Social E Ambiental*, 19(1), e010788. <https://doi.org/10.24857/rgsa.v19n1-049>
- Hiesgen, R., Wählich, M., Schmidt, T. C., & Nawrocki, M. (2024). The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability. *IEEE Transactions on Network and Service Management*, 1. <https://doi.org/10.1109/tnsm.2024.3440188>
- IBM. (n.d.). What is the Log4j vulnerability? *IBM*. Retrieved March 14, 2025, from <https://www.ibm.com/think/topics/log4j>
- Ilieva, S., & Stoilova, K. (2024). Challenges of AI-driven cybersecurity. In *Proceedings of the 2024 XXXIII International Scientific Conference on Electronics and Telecommunications (ET)* (pp. 1-5). IEEE. <https://doi.org/10.1109/ET63133.2024.10721572>
- Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263–291. <https://doi.org/10.2307/1914185>
- Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. *Entropy*, 25(12), 1595. <https://doi.org/10.3390/e25121595>
- Kim, B., Williams, T., Zhu, Q., Phillips, E., & Wen, R. (2021). *Robots as Moral Advisors*. 10–18. <https://doi.org/10.1145/3434074.3446908>
- Kołodziej, J., & Repetto, M. (2022). *Cybersecurity of Digital Service Chains*. springer. <https://doi.org/10.1007/978-3-031-04036-8>
- Kozuharova, D., Kirov, A., & Al-Shargabi, Z. (2022). Ethics in cybersecurity: What are the challenges we need to be aware of and how to handle them? In J. Kołodziej & M. Repetto (Eds.), *Cybersecurity of digital service chains* (pp. 202–221). Springer. https://doi.org/10.1007/978-3-031-04036-8_9
- Kurniawan, K. (2023). " *Improving Cybersecurity through Semantic Log Monitoring, Analysis and Attack Reconstruction*. <https://phaidra.univie.ac.at/open/o:1633094>
- Krivokapić, D., Nikolić, A., & Živković, I. (2023). *Capacities of Western Balkan Economies (and Their Public Sectors) to Respond to Ransomware Attacks***. 1508–1514. <https://doi.org/10.23919/mipro57284.2023.10159856>
- Lee, W.W. (2021). *Hexa-Dimension Metric, Ethical Matrix, and Cybersecurity*. <https://www.igi-global.com/chapter/hexa-dimension-metric-ethical-matrix-and-cybersecurity/260203>
- Loi, M., & Christen, M. (2020). *Ethical Frameworks for Cybersecurity* (pp. 73–95). springer. https://doi.org/10.1007/978-3-030-29053-5_4
- Manjikian, M. (2017). *Cybersecurity Ethics*. routledge. <https://doi.org/10.4324/9781315196275>
- Mittal, M. (2024). Colonial Pipeline Cyberattack Drives Urgent Reforms in Cybersecurity and Critical Infrastructure Resilience. *International Journal of Oil, Gas and Coal Engineering*, 12(5), 106–119. <https://doi.org/10.11648/j.ogce.20241205.11>
- Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. *Spectrum of Engineering Sciences*, 2(3), 420–454. Retrieved from <https://sesjournal.com/index.php/1/article/view/56>
- Ofte, H.J., Katsikas, S. (2024). Paralyzed or Compromised: A Case Study of Decisions in Cyber-Physical Systems. In: Moallem, A. (eds) *HCI for Cybersecurity, Privacy and Trust*. HCII 2024. Lecture Notes in Computer Science, vol 14729. Springer, Cham. https://doi.org/10.1007/978-3-031-61382-1_9
- Ohlhorst, J. (2023). Engineering virtue: constructionist virtue ethics. *Inquiry, ahead-of-print*(ahead-of-print), 1–20. <https://doi.org/10.1080/0020174x.2023.2238293>
- Onwubiko, C., & Ouazzane, K. (2022). Multidimensional Cybersecurity Framework for Strategic Foresight. In *International Journal on Cyber Situational Awareness* (Vol. 6, Issue 1, p. 46). <https://doi.org/10.22619/ijcsa.2021.100137>
- Precious, O. (2025). National critical infrastructure protection via supply chain security in the United States of America. *International Journal of Science and Research Archive*, 14(1), 1379–1386. <https://doi.org/10.30574/ijrsra.2025.14.1.0082>
- Rajamäki, J., & Hämäläinen, H. (2021). Ethics of Cybersecurity and Biomedical Ethics: Case SHAPES. *Information & Security: An International Journal*, 50, 103–116. <https://doi.org/10.11610/isij.5002>
- Reddy Piduru, B. (2021). Ethical Hacking and Penetration Testing: Accessing Cybersecurity Defenses in the Digital Age. *International Journal of Science and Research (IJSR)*, 10(3), 1944–1949. <https://doi.org/10.21275/sr24127124555>
- Sam, D. (2023). *The Impact of System Outages on National Critical Infrastructure Sectors: Cybersecurity Practitioners' Perspective*. <https://search.proquest.com/openview/9b29e82ec8cf652436b65608c9c442ab/1?pq-origsite=gscholar&cbl=18750&diss=y>

- Seiler, G. (2024). Quantum Computing and the Future of Encryption. *Scholarly Review Journal, SR Online: Showcase* (Winter 2024/2025). <https://doi.org/10.70121/001c.127168>
- Singh, R., Singh, S., & Singh, A. (2024, June). *REvil Ransomware*. Paper presented at the 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET), <https://doi.org/10.1109/ICICET59348.2024.10616279>
- Singh, A., Rana, A., Kumar, Y., Yadav, P., Tripathi, N., & Bhargava, A. (2024). Overcoming quantum hardware challenges: Navigating the landscape of quantum computing. *Proceedings of the 7th International Conference on Software and Systems Engineering (IC3SE)*, 7, 1904–1911. <https://doi.org/10.1109/ic3se62002.2024.10593317>
- Spanca, F., & Salihu, A. (2024). *Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation in the Digital Age*. 1–8. <https://doi.org/10.1109/icecce63537.2024.10823432>
- Taherdoost, H., Le, T.-V., & Slimani, K. (2025). Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review. *Cryptography*, 9(1), 17. <https://doi.org/10.3390/cryptography9010017>
- Taylor, J., & Whitty, M. (2023). An Exploration of the Awareness and Attitudes of Psychology Students Regarding Their Psychological Literacy for Working in the Cybersecurity Industry. *Psychology Learning & Teaching*, 23(2), 298-314. <https://doi.org/10.1177/14757257231214612>