Journal of Information Technology Management
ISSN-OnLine: 2980-7972
University of Tehran

Artificial Intelligence and the Evolving Cybercrime Paradigm: Current Threats to Businesses

GholamReza Zandi

Universiti Kuala Lumpur, Business School, Malaysia. E-mail: zandi@unikl.edu.my

Nor Azam Yaacob*

*Corresponding author, Universiti Kuala Lumpur, Business School, Malaysia. E-mail: norazam@unikl.edu.my

Mazilena Tajuddin

Universiti Kuala Lumpur, Business School, Malaysia. E-mail: mazilena@unikl.edu.my

Nik Khadijah Nik Abdul Rahman

Universiti Kuala Lumpur, Business School, Malaysia. E-mail: nikkhadijah@unikl.edu.my

Abstract

This paper provides a comprehensive overview of the evolving Artificial Intelligence (AI) threat to cybersecurity, emphasizing the urgent need for finance leaders and cybersecurity professionals to adapt their strategies and controls to effectively combat AI-powered scams and cyber-attacks. The study delves into the specific ways in which AI is being used maliciously in cybercrime, such as enhanced phishing and Business Email Compromise (BEC) attacks, the creation of synthetic media including deepfakes, targeted attacks, automated attack strategies, and the availability of black-market AI tools on the dark web. Furthermore, it highlights the critical need for enhanced cybersecurity strategies and international cooperation to combat cyber threats effectively. The findings of this study provide valuable insights for finance leaders, cybersecurity professionals, policymakers, and researchers in understanding and addressing the challenges posed by generative AI in the cyber threat landscape.

Keywords: Artificial Intelligence, Cybersecurity, Phishing, Business Email

Journal of Information Technology Management, 2024, Vol. 16, Issue 4, pp. 162-170
Published by the University of Tehran, College of Management
doi: https://doi.org/ 10.22059/jitm.2024.99505
Article Type: Research Paper

Received: June 16, 2024
Received in revised form: July 25, 2024
Accepted: September 30, 2024
Published online: October 16, 2024

Introduction

The current threat landscape in cybersecurity is characterized by a significant increase in cyber incidents and financial losses, with the proliferation of artificial intelligence (AI) tools further exacerbating the risks. Global cybercrime costs are projected to grow by 15% annually, reaching USD 10.5 billion by 2025. Additionally, Australian businesses have reported substantial losses, with millions of dollars being lost to payment redirection schemes in 2022, as reported by the Australian Competition and Consumer Commission (ACCC). The percentage growth of cyber-attacks in Australia is also noteworthy, with a 73% increase in the number of attacks (Eftsure, 2024) year-on-year. These figures underscore the escalating financial impact of cybercrime and the pressing need for organizations to bolster their cybersecurity defenses.

Cybersecurity threats have become a paramount concern for organizations and governments worldwide, as the frequency, sophistication, and impact of cyberattacks (Yamin et al., 2021) continue to escalate. In recent years, the evolution of cyber threats has exposed vulnerabilities across various sectors, leading to significant financial, operational, and reputational damage. The increasing reliance on digital infrastructure (Turk et al., 2022) has amplified the potential for cyberattacks to disrupt critical services and business operations, highlighting the urgent need for robust cybersecurity measures. This introduction delves into recent high-profile cyberattacks in Malaysia, the United States, and Europe, examining their implications and estimating the business losses incurred.

One notable cyber-attack in Malaysia involved the country's largest media company, Media Prima Berhad, which fell victim to a ransomware attack in November 2018. The attackers demanded a ransom of 1,000 Bitcoins, equivalent to approximately USD 6.3 million at the time. This incident not only disrupted the company's operations (Satyapanich et al., 2020) but also underscored the vulnerabilities in the media industry's cybersecurity defenses. The financial losses extended beyond the ransom demand, encompassing operational downtime, remediation costs, and potential reputational damage, cumulatively amounting to millions of dollars. This attack highlighted the critical need for Malaysian organizations to enhance their cybersecurity resilience against increasingly sophisticated threats.

In the United States, the Colonial Pipeline ransomware (Beerman et al., 2023) attack in May 2021 stands out as a stark example of the potential impact of cyber threats (Dion, 2011) on critical infrastructure. The attack led to a six-day shutdown of the pipeline, which supplies nearly half of the East Coast's fuel. The disruption caused widespread fuel shortages, panic buying, and significant economic repercussions. Colonial Pipeline reportedly paid a ransom of $4.4 million to the cybercriminal group DarkSide, though the FBI later recovered a portion of the ransom. The estimated business losses due to the operational disruption and subsequent economic impact were substantial, running into hundreds of millions of dollars. This incident

emphasized the vulnerability of critical infrastructure to cyber threats and the far-reaching consequences of such attacks.

Europe has also experienced significant cyberattacks, with the 2017 NotPetya (Dwyer, 2023; Ren et al., 2020) attack serving as a prominent example. Originating as a state-sponsored attack targeting Ukraine, NotPetya quickly spread globally, affecting numerous multinational companies. In Europe, Danish shipping giant Maersk was severely impacted, with the attack causing an estimated loss of USD300 million due to disrupted operations and the cost of restoring its IT systems. The pharmaceutical company Merck, based in Germany, also suffered significant disruptions, with financial losses estimated at around USD 870 million. These incidents underscored the transnational nature of cyber threats and the extensive economic damage they can inflict on major corporations.

The financial and operational impacts of these cyberattacks highlight the critical need for enhanced cybersecurity strategies and international cooperation to combat cyber threats (Valkenburg & Bongiovanni, 2024) effectively. As cybercriminals continue to develop more sophisticated methods, organizations must adopt proactive measures to safeguard their digital assets and infrastructure. This includes investing in advanced cybersecurity technologies, fostering a culture of security awareness, and implementing comprehensive incident response plans. Additionally, governments and regulatory bodies must collaborate to establish robust cybersecurity frameworks and standards, ensuring a unified approach to mitigating cyber risks on a global scale.

Additionally, the escalating threat landscape of cybersecurity presents significant challenges for businesses and critical infrastructure worldwide. Recent high-profile cyberattacks in Malaysia, the United States, and Europe underscore the potential for substantial financial losses and operational disruptions. By examining these incidents, it becomes evident that a concerted effort is required to enhance cybersecurity resilience, involving not only technological advancements but also strategic collaborations and regulatory measures. Addressing these threats (Slapničar et al., 2022) necessitates a comprehensive and proactive approach, ensuring that organizations are equipped to navigate the complex and ever-evolving cyber threat landscape.

Literature Review

Artificial Intelligence (AI)

Artificial Intelligence (AI) is a broad field of computer science that focuses on creating systems capable of performing tasks that typically require human intelligence. These tasks include understanding natural language, recognizing patterns, solving problems, and making decisions. AI systems can be designed to learn from data and improve their performance over time without being explicitly programmed for every task. Machine learning, a subset of AI, employs algorithms and statistical techniques to enable computers to learn from data and

make predictions or decisions. Generative AI is a specific type of AI that uses machine learning techniques to generate entirely new content, such as text, images, or sound, which was not part of the original training dataset.

AI Threat to Cybersecurity

AI presents a dual-edged sword in the realm of cybersecurity. While it offers powerful tools for defenders to protect systems and data, it also provides cybercriminals with advanced capabilities to launch more sophisticated attacks. Several ways in which AI is being used maliciously:

Enhanced Phishing and BEC Attacks: AI, particularly Large Language Models (LLMs) like ChatGPT, is being used to craft more convincing phishing (Teichmann, 2023) emails and Business Email Compromise (BEC) attacks. By eliminating grammatical errors and mimicking natural language, AI-generated messages are harder (Guembe et al., 2022; Manoharan & Sarker, 2024) to detect, leading to increased success rates for cybercriminals.

Synthetic Media: Generative AI is used to create synthetic media, including deepfakes, which are realistic forgeries of audio, video, or images. These can be used to impersonate individuals, such as executives, and issue fraudulent instructions (Gao et al., 2009; Kingdon, 2004), undermining trust within organizations and supply chains.

Targeted Attacks: AI helps threat actors analyze large datasets of stolen personal information to identify the most vulnerable targets. This allows for more efficient and effective attacks, as cybercriminals can focus their efforts on those who are likely to fall for their scams.

Automated Attack Strategies: AI can automate the process of finding vulnerabilities, writing malicious code (Chen et al., 2004), and developing new attack strategies. This not only speeds up the attack process but also allows cybercriminals to stay ahead of defensive measures.

Black-Market AI Tools: On the dark web, AI tools are available that lack the guardrails of mainstream AI services. These can be used for unethical purposes, such as creating honeypots or deceptive technologies to lure and exploit unsuspecting victims.

In response to these threats, finance leaders need to develop a unified cybercrime strategy, strengthen anti-fraud controls (Lau & Ooi, 2016; Moyes, 2007), routinely pressure-test their controls, and double down on security hygiene. Additionally, they should incorporate a synthetic media incident response strategy to prepare for and respond to AI-powered scams effectively.

Methodology

The qualitative study employed in this study will examine threats and opportunities from Artificial Intelligence for corporation cybersecurity utilizing recent literature, expert opinions,

and case studies. The approach is designed to make it easier to conduct a methodical investigation of AI applications concerning many cybersecurity aspects, such as threat identification, vulnerability assessment, incident response, and predictive analysis.

1. Case Studies: This involves analyzing real-world case studies and use cases demonstrating the application of AI technology in cybersecurity settings. It includes examining effective deployments, challenges encountered, and lessons learned from employing AI-driven defenses against cyberattacks.
2. Expert Interviews: This involves interviewing professionals in the field, AI practitioners, and cybersecurity experts to gain firsthand insights into the applications and implications of AI in cybersecurity. Additionally, questionnaires or surveys will be sent out to gather opinions from stakeholders who are using or implementing AI-driven cybersecurity solutions.
3. Framework Evaluation: This involves assessing current approaches and frameworks for integrating AI into cybersecurity procedures. A critical evaluation of the SWOT (strengths, weaknesses, opportunities, and threats) of AI-driven cybersecurity techniques will be conducted to identify best practices and potential areas for development.

Through the rigorous application of these methods, the goal is to provide valuable insights into safeguarding security responses, offer input for policymakers, raise public awareness, and foster collaboration and information sharing among researchers in this field.

Results

This study provides a comprehensive overview of the AI threat to cybersecurity, particularly focusing on the proliferation of generative AI and its implications for financial risk management.

AI's Impact on the Cyber Threat Landscape: The key highlight is that AI is reshaping the cyber threat landscape by equipping cybercriminals with powerful capabilities and altering concepts of evidence and truth. It emphasizes that the rapid evolution of AI is outpacing existing laws, regulations, and societal norms, raising concerns about a potential "post-trust future."

AI's Role in Cybercrime: This study underscores that AI is assisting both defenders and attackers, with cybercriminals having access to the same AI tools and technologies. It points out that generative AI capabilities are increasing the efficiency, reach, and scale of existing scams and cyber-attacks, posing significant challenges for finance professionals.

Specific Applications of AI in Cybercrime: This research delves into specific applications of generative AI in cybercrime, such as the use of Large Language Models (LLMs) and chatbots to refine phishing tactics and Business Email Compromise (BEC) attacks (Iasiello, 2014). It also highlights the potential use of AI to develop multi-persona phishing tactics and synthetic media, including deep fakes (Camacho, 2024), for impersonation and manipulation.

Challenges and Risks: Another aspect discussed here is an outline of the challenges and risks posed by AI-powered cyber threats, including the need for finance leaders to adopt (Beerman et al., 2023) to a new reality and the potential for cybercriminals to capitalize on new technology. It also emphasizes the importance of understanding how AI capabilities can be used against finance professionals and the need to upgrade laws and institutions to address unforeseen AI advances.

In summary, these findings provide insights into the evolving AI threat to cybersecurity, emphasizing the urgent need for finance leaders to think creatively, stay informed, and implement technology-driven processes to combat the growing challenges posed by generative AI in the cyber threat landscape.

Conclusion

The proliferation of generative artificial intelligence (AI) has significantly enhanced the capabilities of cybercriminals, leading to a rapidly evolving and multifaceted threat landscape. As generative AI technologies become more sophisticated and accessible, cybercriminals are increasingly leveraging these tools to launch more effective, precise, and complex attacks. This study emphasizes the urgent need for finance leaders and cybersecurity professionals to adapt their strategies and controls to effectively combat AI-powered scams and cyber-attacks. The traditional methods of cybersecurity are proving inadequate against the backdrop of these advanced AI-driven threats, necessitating a paradigm shift in how organizations approach their security measures.

Generative AI enables cybercriminals to automate the creation of malicious content, such as phishing emails, deepfake videos, and fake social media profiles, with unprecedented realism and scale. These AI-generated attacks can deceive even the most vigilant users, making it easier for cybercriminals to steal sensitive information, spread disinformation, or disrupt operations. The increasing sophistication of these attacks means that organizations must continuously evolve their defenses to keep pace with the threat landscape. Cybersecurity professionals must not only detect and respond to these threats but also anticipate and mitigate potential future risks.

The financial impact of cybercrime is escalating at an alarming rate. According to various studies, the global cost of cybercrime is expected to reach trillions of dollars annually. These costs include not only direct financial losses but also reputational damage, regulatory fines, and the costs associated with incident response and recovery. For finance leaders, the stakes are higher than ever. They must ensure that their organizations have robust cybersecurity frameworks in place to protect against these evolving threats. This involves investing in advanced cybersecurity technologies, such as AI-driven threat detection systems, as well as training employees to recognize and respond to cyber threats.

Moreover, the challenges posed by AI-powered cyber threats require finance leaders to think creatively and strategically. Traditional risk management approaches may no longer be sufficient in this new landscape. Finance leaders need to stay informed about the latest developments in AI and cybersecurity and be proactive in adopting new technologies and methodologies. This might involve collaborating with cybersecurity experts, participating in industry forums, and staying abreast of regulatory changes. By doing so, they can better understand the risks and opportunities associated with generative AI and make informed decisions about how to protect their organizations.

Implementing technology-driven processes is also crucial in addressing the growing threats posed by generative AI. Automated threat detection and response systems, powered by machine learning and AI, can help organizations quickly identify and mitigate cyber threats before they cause significant damage. These systems can analyze vast amounts of data in real-time, identifying patterns and anomalies that may indicate a cyber-attack. Additionally, AI can be used to simulate potential attack scenarios, allowing organizations to test their defenses and identify vulnerabilities.

However, technology alone is not enough. Organizations must also foster a culture of cybersecurity awareness and resilience. This involves educating employees about the latest cyber threats and encouraging them to adopt best practices in their daily activities. Regular training sessions, phishing simulations, and cybersecurity drills can help reinforce the importance of cybersecurity and ensure that employees are prepared to respond to potential threats.

In conclusion, the rise of generative AI has fundamentally changed the cybersecurity landscape, presenting new challenges and opportunities for finance leaders and cybersecurity professionals. To effectively combat AI-powered scams and cyber-attacks, organizations must adapt their strategies, invest in advanced technologies, and foster a culture of cybersecurity awareness. By doing so, they can protect their assets, reputation, and bottom line from the escalating threat of cybercrime. The financial impact of cybercrime underscores the pressing need for robust cybersecurity defenses, and the challenges posed by AI-powered threats highlight the importance of staying informed and proactive in this rapidly evolving landscape.

Acknowledgments

Thanks to all of the co-authors of this article for their willingness to share and contribute knowledge to carry out this study successfully.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A Review of Colonial Pipeline Ransomware Attack. *Proceedings - 23rd IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing Workshops, CCGridW 2023*, 8–15. https://doi.org/10.1109/CCGridW59191.2023.00017

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

Chen, H., Chung, W., Xu, J. J., Wang, G., Qin, Y., & Chau, M. (2004). Crime data mining: a general framework and some examples. *Computer*, *37*(4), 50–56.

Dion, M. (2011). Corruption, fraud and cybercrime as dehumanizing phenomena. *International Journal of Social Economics*, *38*(5), 466–476. https://doi.org/10.1108/03068291111123156

Dwyer, A. C. (2023). Cybersecurity's grammars: A more-than-human geopolitics of computation. *Area*, *55*(1), 10–17. https://doi.org/10.1111/area.12728

Eftsure. (2024). *Cybersecurity Guide for CFOs*. *7th edition*.

Gao, S., Xu, D., Wang, H., & Green, P. (2009). Knowledge-based anti-money laundering: a software agent bank application. *Journal of Knowledge Management*, *13*(2), 63–75.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. In *Applied Artificial Intelligence* (Vol. 36, Issue 1). Taylor & Francis. https://doi.org/10.1080/08839514.2022.2037254

Iasiello, E. (2014). Is cyber deterrence an illusory course of action? *Journal of Strategic Security*, *7*(1), 54–67. https://doi.org/10.5038/1944-0472.7.1.5

Kingdon, J. (2004). AI fights money laundering. *Intelligent Systems, IEEE*, *19*(3), 87–89.

Lau, C. K., & Ooi, K. W. (2016). A case study on fraudulent financial reporting: Evidence from Malaysia. *Accounting Research Journal*, *29*(1). https://doi.org/10.1108/ARJ-11-2013-0084

Manoharan, A., & Sarker, M. (2024). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *International Research Journal of Modernization in Engineering Technology and Science*, *March*. https://doi.org/10.56726/irjmets32644

Moyes, G. D. (2007). Audit Techniques & Inventory Fraud Detection In Accounting Information Systems. *Review of Business Information Systems (RBIS)*, *1*(1), 63–76.

Ren, A. L. Y., Liang, C. T., Hyug, I. J., Brohi, S. N., & Jhanjhi, N. Z. (2020). A three-level ransomware detection and prevention mechanism. *EAI Endorsed Transactions on Energy Web*, *7*(26), 1–7. https://doi.org/10.4108/eai.13-7-2018.162691

Satyapanich, T., Ferraro, F., & Finin, T. (2020). Casie: Extracting cybersecurity event information from text. *AAAI 2020 - 34th AAAI Conference on Artificial Intelligence*, 8749–8757. https://doi.org/10.1609/aaai.v34i05.6401

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*(January 2021). https://doi.org/10.1016/j.accinf.2021.100548

Teichmann, F. (2023). Ransomware attacks in the context of generative artificial intelligence—an experimental study. *International Cybersecurity Law Review*, *4*(4), 399–414. https://doi.org/10.1365/s43439-023-00094-x

Turk, Ž., Sonkor, M. S., & Klinc, R. (2022). Cybersecurity assessment of bim/cde design environment using cyber assessment framework. *Journal of Civil Engineering and Management*, *28*(5), 349–364. https://doi.org/10.3846/jcem.2022.16682

Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: a systematic literature review. *Computers and Security*, *139*(December 2023), 103708. https://doi.org/10.1016/j.cose.2024.103708

Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, *57*, 1–35. https://doi.org/10.1016/j.jisa.2020.102722

Bibliographic information of this paper for citing:

Zandi, GholamReza; Yaacob, Nor Azam; Tajuddin, Mazilena & Nik Abdul Rahman, Nik Khadijah (2024). Artificial Intelligence and the Evolving Cybercrime Paradigm: Current Threats to Businesses. *Journal of Information Technology Management*, 16 (4), 162-170.
https://doi.org/10.22059/jitm.2024.99505