The Impact of Emerging Technologies and Trends in Network Security on Cybersecurity: Identifying Risks and Benefits for Organizations.

Jeggo Paolo V. DyCok

Jdyco001@odu.edu

Old Dominion University

CYSE250: Cybersecurity Networking and Programming

Hind AlDabagh

April 23, 2023

Abstract

This essay explores the impact of emerging technologies and trends on cybersecurity, allocation of authority and responsibility for policymaking, and challenges and opportunities presented by blockchain, AI (Artificial Intelligence), and malware attacks. Governments' interpretation and prioritization of policy problems determine which governing jurisdiction is assigned and which actors are responsible for policy decisions. Emerging technologies and trends can create new policy concerns that shift or expand the target population and enforcement authority bestowed on existing regulatory structures. Blockchain's encryption and security are its core strengths, but its technical complexity may inadvertently increase cybersecurity risks. AI may represent the potential future of many business processes, but most organizations are not prepared enough for a full-blown AI program. Malware attacks remain a significant concern for cybersecurity experts, who are constantly developing new countermeasures to ensure the confidentiality, integrity, and availability of digital and information technologies. Confidentiality is used to prevent the disclosure of information to unauthorized individuals or systems, integrity prevents any modification or deletion in an unauthorized manner, and availability assures that the systems responsible for delivering, storing, and processing information are accessible when needed and by those who need them.

Key Words: cybersecurity, blockchain, AI, malware attacks, encryption, crypto assets, firewalls, anti-virus software.

How do emerging technologies and trends in network security impact cybersecurity, and what potential risks and benefits do they present for organizations?

Introduction

Cybersecurity has become an increasingly important issue in today's digital landscape, with emerging technologies and trends in network security posing new challenges and vulnerabilities. As technology continues to advance, the allocation of authority and responsibility for policymaking plays a critical role in regulating and protecting against cybersecurity threats. Blockchain and AI offer new opportunities for security, but also present new risks and challenges that require careful consideration. Malware attacks remain a significant concern for cybersecurity experts, who are constantly developing new countermeasures to ensure the confidentiality, integrity, and availability of digital and information technologies. In this essay, we will explore the impact of emerging technologies and trends on cybersecurity, examine the allocation of authority and responsibility for policymaking, and discuss the challenges and opportunities presented by blockchain, AI, and malware attacks.

Understanding of The Topic

The fast-paced growth of technology poses a significant challenge for institutions to comprehend and address the policy implications, as highlighted by Lewallen (2020). Governments' interpretation and prioritization of policy issues determine governing jurisdictions and actors responsible for making policy decisions. Cybersecurity is a complex issue that spans multiple jurisdictions within regulatory institutions, leading to the allocation of authority to determine which actors are involved and how they define the problem. This has a significant impact on how risks are assessed, and the range of regulatory responses considered.

New technologies like blockchain and artificial intelligence (AI) have the potential to revolutionize the way businesses operate and interact with different sectors, leading to new ties between governance and industries. However, incorporating new technologies into existing systems can create cybersecurity risks due to technical complexity and lack of experience in connecting these tools with other enterprise resource planning tools. Organizations must ensure the confidentiality, integrity, and availability of digital and information technologies while being

aware of malware, which can breach cybersecurity efforts. The traditional perimeter defense model, which relies on firewalls and anti-virus software, may not be adequate to protect against modern malware attacks that can penetrate multiple internal networks.

In summary, cybersecurity is not limited to specific technology tools or platforms but is also connected to how different technology systems and platforms interact with each other. As new technologies continue to emerge, practitioners in accounting functions and other sectors must be prepared to adapt to changing cybersecurity concerns and risks to preserve the confidentiality, integrity, and availability of digital and information technologies.

Results and Findings

Emerging technologies and trends in network security have a significant impact on cybersecurity. According to Lewallen (2020), new technologies can come up and change faster than institutions can even understand them. This means that governments have to decide which governing jurisdiction they assign to cybersecurity issues, and which actors are responsible for making policy decisions. As Lewallen (2020) puts it, "Cybersecurity is a technology-driven problem that involves multiple jurisdictions within regulatory institutions, and the allocation of authority determines which actors are engaged, how those actors define the issue at hand, and how the range of considered regulatory responses is weighed." This highlights the importance of understanding the different aspects of network security and how they affect cybersecurity policies.

The three main ways that emerging technologies and trends affect cybersecurity, according to Lewallen (2020), are: first, a new technology may create a new policy concern that shifts or expands the target population and resulting enforcement authority bestowed on existing regulatory structures. Second, a new technology in one sector may change the way business and policy are conducted in other sectors, which creates new ties between governance of the different industries. Third, through the adoption or mimicking of existing technologies across economic and social sectors and across geographic boundaries, different governing arrangements and jurisdictions designed to address different issues find themselves faced with similar challenges.

Blockchain technology has significant implications for cybersecurity, as it is recognized for enhancing security through its transparency, immutability, and decentralization features.

However, as discussed by Smith (2020), the technical complexity of blockchain and the lack of experience in integrating it with other enterprise resource planning tools may increase cybersecurity risks. The potential of blockchain technology to provide a secure and reliable data storage system cannot be understated, but the risks associated with it must be taken seriously. The integration of blockchain technology with other systems must be approached with caution to avoid any vulnerability in the security of the entire system. Additionally, the verification of the custody and provenance of crypto assets, which is closely related to blockchain technology, is critical to building a comprehensive cybersecurity framework. (Smith 2020) It can help mitigate the risks associated with fraudulent activities, data breaches, and cyber-attacks. Therefore, it is crucial to recognize the importance of blockchain technology and its potential risks and implement appropriate security measures to ensure cybersecurity.

Jang-Jaccard and Nepal (2014) assert that cybersecurity concerns are critical in preserving confidentiality, integrity, and availability of any digital and information technologies. "Confidentiality is used to prevent the disclosure of information to unauthorized individuals or systems, integrity prevents any modification or deletion in an unauthorized manner, and availability assures that the systems responsible for delivering, storing, and processing information are accessible when needed and by those who need them." The majority of perimeter defense mechanisms, such as firewalls and anti-virus software, utilize the perimeter defense strategy to put a wall outside all internal resources to safeguard everything inside from any unwanted intrusion from outside. As Jang-Jaccard and Nepal (2014) state, Perimeter defense is a security strategy that focuses on protecting the boundary of a network from external threats, and it includes mechanisms such as firewalls, intrusion detection systems, and virtual private networks. They also emphasize the importance of employing both perimeter and internal defense mechanisms to protect the confidentiality, integrity, and availability of digital and information technologies, stating that "comprehensive security solutions for the protection of the networks, hosts, and applications should be put in place to mitigate the risk of threats.

Conclusion

In conclusion, emerging technologies and trends in network security have a significant impact on cybersecurity. New technologies may create new policy concerns that shift or expand the target population and resulting enforcement authority bestowed on existing regulatory structures. Additionally, the integration of new technologies into existing systems can create cybersecurity risks due to technical complexity and lack of experience in connecting these tools with other enterprise resource planning tools. Blockchain's encryption and security are its core strengths, but its technical complexity may inadvertently increase cybersecurity risks. AI may represent the potential future of many business processes, but most organizations are not prepared enough for a full-blown AI program. Malware attacks remain a significant concern for cybersecurity experts who are constantly developing new countermeasures to ensure the confidentiality, integrity, and availability of digital and information technologies. It is crucial for organizations to ensure the confidentiality, integrity, and availability of digital and information technologies while being aware of malware and other cybersecurity threats, as the traditional perimeter defense model may not be enough to protect against modern attacks. As new technologies continue to emerge, practitioners in various sectors must be prepared to adapt to changing cybersecurity concerns and risks to preserve the confidentiality, integrity, and availability of digital and information technologies.

References

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Lewallen, J. (2020). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance*, *15*(4), 1035–1052. https://doi.org/10.1111/rego.12341

Smith, S. S. (2020). Emerging technologies and implications for financial cybersecurity. *International Journal of Economics and Financial Issues*, 27–32. https://doi.org/10.32479/ijefi.8844