Impact and Social Meaning of Cybersecurity

Isaiah Bagwell-Goines

Professor Bowman

Old Dominion University

Introduction

In this digital age, the interconnectedness of mankind and technology has become ever prevalent. As such, assessing the state and importance of cybersecurity-related technologies is vital. Cybersecurity, being a vague and mysterious topic for most, entails more than just codes and algorithms used to protect our devices. Instead, cybersecurity involves much simpler and well-known measures to prevent security breaches and potential cyber-attacks—developing security or, more specifically, cybersecurity frameworks and adopting risk management strategies. By employing these practices carefully, the state of cybersecurity within an infrastructure can thrive as it is incumbent upon a strong foundation for not only the reputation of the business but also the data and privacy of its customers. In addition, knowing how a cybersecurity system can be breached to show its detrimental effects fully displays its value and importance in society. Also, delving into the hackers' perspective and motives to properly mitigate the potential of becoming victims of their often malicious and selfish acts will add to cybersecurity's meaning and importance. Thus, these are essential aspects regarding cybersecurity-related technologies and their overall impact on society.

Cybersecurity Framework

First, in cybersecurity, a framework is a set of standards and best practices that serve as a basis for creating, implementing, and examining systems or processes (Framework for Improving Critical Infrastructure Cybersecurity, 2018). As such, it acts as a guide or model to assist companies in effectively achieving objectives or results regarding the level or tier of cybersecurity. The NIST framework is a heavily followed guideline for managing and preventing cybersecurity risk, consisting of the following core topics: Identify, Protect, Detect, Respond, and Recovery. To start, "identify” involves the organization identifying potential risks to security

and assessing the assets that may need better protection. "Protect" means implementing safety procedures or safeguards against potential physical or cybersecurity-related risks. "Detect" and "Respond" involve the detection of cybersecurity incidents and their associated effects as well as the timely response to such incidents to transition to the final portion of the NIST framework, "Recovery," which includes the recovery of the everyday operations and potential assets that may or may not have been compromised to the said threat. As a result, organizations may create a structured approach for maintaining and enhancing cybersecurity risk assessment and mitigation by adhering to these five basic guidelines. Businesses may customize the NIST Cybersecurity Framework to fit various needs and risk profiles since it offers a versatile and scalable structure that can be used with other frameworks, allowing for better cybersecurity integrity and a more robust, more up-to-date framework profile. Thus, frameworks are helpful as they are blueprints for companies to combat cybersecurity risks based on their needs and niches.

Risk Management

Moreover, risk management is a crucial component of safeguarding cybersecurity-related technologies. Risk management involves identifying potential sources of risk and vulnerabilities to an organization's technology and physical security. The need to secure cyber-related technology from cyber-attacks is crucial due to the real threats of security breaches by human error and criminal activity like hacking and espionage. For organizations to protect their operational technology and, perhaps, your data and assets, companies must identify and manage risks in their digital infrastructures and physical environments. Practices like mandatory reporting, monitoring, and cybersecurity training can improve transparency and help address cybersecurity risks within a company. According to IBM, a company that specializes in cyber-

related technology, "The average savings for organizations that use security AI and automation extensively is USD 1.76 million compared to organizations that don't" (IBM, 2023).

In addition, the impacts of a security breach on a company include financial loss, reputational or operational damage, data loss or compromise, loss of life due to safety risks, and mistrust in industries. Financial loss concerns the costs associated with cybersecurity attacks that may result in data recovery, legal fees, and software replacement/recovery. Operational damage or disruption is caused by a cyber-attack leading to downed systems, delay, financial loss, and reputational damage to the company. Data loss or compromise also affects the company's reputation and finances, as data recovery can be costly. Data is one of the more critical assets to safeguard, as a security breach can expose sensitive or potentially classified information, customer data, and even trade secrets. Finally, lives can be lost because of a breach that suffers the same consequences as the others, with the added severity of legal fees and loss of personnel. These are critical potential consequences in a breach due to a lack of risk management.

Moreover, organizations' readiness levels for cybersecurity risks and risk management strategies vary greatly. Some businesses invest significantly in comprehensive cybersecurity measures, such as ongoing risk assessments, staff training, and deploying cutting-edge security systems. Others, on the other hand, might not devote enough resources or be unaware of how the danger landscape is changing. Thus, it depends on the company's value/level of cybersecurity within the business on the individual level. Regardless, companies would be wise to invest more financially into this aspect of business as technology progresses.

The Need for Cybersecurity/Hacker's Perspective

Finally, hackers use malicious code they create or download to facilitate malicious cyber-attacks. The motive for these attacks varies from reputation, financial gain, acts of terrorism, etc.; the book *Electric Grid Security and Resilience* (2016) addresses this and provides multiple examples of hacker tools and malicious code that continuously evolve as technology progresses. Some examples include automated toolkits, viruses, rootkits, logic bombs, worms, and others that would naturally be detrimental to a computer system once infected. To mitigate the associated risks concerning malicious code used by hackers, the widespread and careful monitoring of computer systems should be done regularly. However, it is also worth noting that there is not perfectly safe or "impossible to hack" software or hardware, though increasing physical security and enforcing risk mitigation tactics would combat the opportunities for a cybersecurity event. In addition, as hackers improve their methods and tools for employing malicious software into computers, so do antivirus and malware analysis software. A recent study consisted of researcher S. Arshad Hashmi (2023) analyzing the Android OS for viruses and malware through AI detection and machine learning (ML) deep learning (DL) to which he noted:

> ML and DL malware identification and categorization methods might help cyber forensic investigators curb the spread of malicious software. Applying DL methods helps safeguard applications. DL approaches have addressed cybersecurity issues, including intrusion detection, malware classification and identification, phishing and spam detection, and spam recognition. (p. 650)

To keep up with new hacking methods and the creation of different and more powerful malware, we must employ proper cyber safeguards, data handling, and risk mitigation tactics and adapt to

new cyber threats. Thus, hacking and malicious code are closely associated, and awareness of these methods stresses cyber-related technologies' significance.

Conclusion

To summarize, cybersecurity is a broad and critical part of our digital era, involving a variety of safeguards and technology to protect against possible cyber-attacks. Businesses and organizations may strengthen their defenses and reduce the risks associated with cybersecurity incidents by developing comprehensive strategies such as the NIST Cybersecurity Framework and using risk management methods. Cybersecurity attacks can have severe ramifications, including financial loss, reputational harm, and lost data, emphasizing the significance of proactive protection measures. Furthermore, knowing hackers' motivations and tactics gives insight into the always-changing nature of cybersecurity threats. By remaining aware and utilizing emerging technologies such as AI and machine learning for malware detection and prevention, we can adapt to new cyber threats and strengthen our cybersecurity protection. Thus, the interdependence of humanity and technology ultimately highlights the impact of cyber-related technology and the requirement for solid cybersecurity procedures to protect people and companies in an increasingly digitalized environment.

References

Hashmi, S. A. (2023). Malware Detection and Classification on Different Dataset by Hybridization of CNN and Machine Learning. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(6s), 650-667.

IBM. (2024). Cost of a data breach 2023. Retrieved from https://www.ibm.com/reports/data-breach

ICF. (2016). Retrieved from https://energy.gov/epsa/downloads/electric-grid-security-and-resilience-establishing-baseline-adversarial-threats