Journal of Academic Inquiry and Knowledge Volume 2024 (3) 71-79
ISBN 979-8-9888908-1-2

THE ECONOMIC THREAT OF CYBER ATTACKS AND SECURITY STRATEGIES

Yidong Jin

Los Angeles, CA, USA

The Economic Threat of Cyber Attacks and Security Strategies

Technology has become entrenched in people's lives and is being adopted in many ways. This is known as *digitalization* (Zimon & Kasprzyk, 2021). People and businesses have become increasingly reliant on computers and technologies. However, with this increased reliance comes a greater risk of cyber-attacks (Singh & Kumar, 2020). Although the rise of technology has benefited society, it has also increased the risk and potential damage of cyber-attacks, posing a dangerous threat to individuals, companies, and supply chains.

What are Cyber-Attacks?

Cyber-attacks are digital attacks that seek to disrupt, destroy, and gain profits from attacking a system, enterprise, or individual (Green, 2016). Cyber-attacks have always been a huge threat, but they have become more so as technology becomes more integrated into society. Cyber-attacks have a wide range of targets, from individuals to companies and supply chains. Cyber-attacks come in many forms, with any of them as effective as the others.

Cyber-attacks most commonly use one of the following methods: malware, phishing, passwords, SQL injections, denial of service, insider threats, and man-in-the-middle (Nathwani,

2023). *Malware* is malicious software designed to seek and harm a person's data. (Buriro, 2023). Malware includes viruses, worms, trojan horses, ransomware, spyware, and adware (Nathwani, 2023). *Phishing* uses deceptive websites to steal a person's data and personal information. The disguised website tricks users into revealing personal data (Rao & Pais, 2018). *Password attacks* involve using software to continuously guess passwords until they guess the right one (Nathwani, 2023). *SQL injections*, on the other hand, specifically target the SQL (Structured Query Language) database. SQL is a programming language that is used to manage information. SQL injections manipulate the database to steal sensitive information such as usernames and passwords (Nathwani, 2023). *A Denial of Service (DoS*) attack overloads a website, application, or network by creating a large amount of traffic, making the system unresponsive and eventually crashing (Nathwani, 2023). It reduces bandwidth, disrupting and preventing access to a service from users (Lau et al., 2000). While cyber-attacks are caused by an outside hacker, an *insider threat* originates within a company (Nathwani, 2023). An employee or trusted individual triggers the attack by exposing the company to cyber-attacks. Finally, a *man-in-the-middle attack* seeks to intercept communication between two groups and eavesdrop on the information that is spread (Nathwani, 2023).

A hacker's motive behind cyber-attacks is to steal sensitive information and data, primarily for financial gain. Hackers also steal intellectual property and confidential information (Srinivas et al., 2019) and sell the information for profit on online forums (Holt, 2013).

Cyber-Attack Harm

Companies and organizations suffer much harm from cyber-attacks. Cyber-attacks cause digital harm by disrupting, stealing, and corrupting digital assets (Green, 2016). This can minimize or even destroy a company's digital assets. Digital assets and operations can be lost,

exposed, leaked, and stolen (Agrafiotis et al., 2018). This can slow a company's operations and even halt them altogether.

A cyber-attack's disruption of operations diminishes the company's ability to do business and gain profit. The drop in revenue and profit can lead to a subsequent fall in stock prices and reduce the company's value. Not to mention, hackers can outright steal the company's financial resources through cyber-attacks (Agrafiotis et al., 2018).

In addition, repairing the damages caused by cyber-attacks can be very expensive. Companies may pay investigation costs, public relations response expenses, and extortion payments (Agrafiotis et al., 2018). Finally, along with repair costs, companies may have to pay regulatory and compensation fines (Agrafiotis et al., 2018). Larger companies lose an average of 3.8 million USD to 16.8 million USD (Taddeo, 2019), and cyber-attacks have cost the global economy about 445 billion USD annually (Samtani et al., 2017).

Finally, cyber-attacks create reputational harm. Most notably, a company can suffer significant damage to its public perception after being hit with a cyber-attack (Agrafiotis et al., 2018). The attacks suggest a security weakness that engenders distrust and damages the company's relationship with its customers, suppliers, and investors (Agrafiotis et al., 2018).

Supply Chain Risks

In the bigger economic arena, cyber-attacks can significantly impact supply chains. Just one company being attacked by a cyber-attack can create distrust and panic among the entire chain, from supplier to customer. Relationships among many companies and businesses can crumble due to the economic and reputational damage that cyber-attacks can cause. Thus, a singular cyber-attack can create a domino effect, destroying economies.

Cyber-attacks can intercept and manipulate design specifications and alterations before the final product is finished and brought to customers.

> For instance, design specification establishes the contractual agreement of a final product deliverable after the system requirements have been captured in a software development process. The threat actor could deliberately insert a code to manipulate data, especially in software that is bought off the shelf, to prevent the product from achieving the organizational goal. (Yeboah-Ofori & Islam, 2019).

In general, this manipulation would cause harm to both the suppliers and the customers as the suppliers receive reputational and financial damage while customers are not given the right product.

Existing Cyber Security

Because of the enormous economic damage cyber-attacks can cause, there is a need for extensive cyber security, and security measures are created to provide a level of protection against cyber-attacks (Kumar et al., 2022). Existing security measures used against cyber-attacks include cloud security, critical infrastructure security, data loss prevention (DLP), application security, information security, network security, Internet of Things (IoT) security, operational security, endpoint security, website security, big data security, and blockchain security (Perwej et al., 2021).

Cloud security protects cloud-based data storage by providing users with data, network, and service security. *Critical infrastructure* security is security for critical infrastructures, including electricity grids, water purification systems, traffic lights, shopping malls, hospitals, and more (Perwej et al., 2021). *Data Loss Prevention* (DLP) prevents data loss by detecting potential data breaches. DLP does this through monitoring, detecting, and blocking sensitive

data. On the other hand, *application security* is used during all the stages of developing an application. It includes hardware, software, and procedures to help strengthen security (Perwej et al., 2021). Like DLP, *information security* helps protect data on a wider spectrum. It protects all types of information from unwanted access whenever it travels from one device to another (Perwej et al., 2021). Moreover, while cyber security deals with outside dangers, *network security* deals with internal protection (Perwej et al., 2021). Next, *Internet of Things (IoT)* security protects physical devices that use IoT from hackers by using a secure network (Perwej et al., 2021). The Internet of Things uses devices with sensors and processing abilities that can connect and exchange data with other devices that use IoT, making them vulnerable to hackers. *Operational security* protects the operations of systems and processes through 5 steps. These steps include identifying important information, threat analysis, vulnerability analysis, risk assessment, and deploying effective countermeasures (Perwej et al., 2021). Equally important, *endpoint security* protects and prevents risks from using devices such as phones and computers (Perwej et al., 2021). *Website security* is used to protect websites from cyber-attacks. *Big data security* can detect and add that extra layer of protection against cyber-attacks (Perwej et al., 2021). And finally, *blockchain security* decentralizes data storage (Perwej et al., 2021). This reduces the chances of a single point of risk and failure.

New Methods of Protection

Even with all the already existing cyber security, 51% of businesses with 1,000 or more employees have reported facing at least one cyber-attack (Perwej et al., 2021). That number is only increasing as entities dive deeper into digitalization. Hence, new solutions are needed to combat the growing dangers of cyber-attacks. Artificial intelligence has recently been implemented into cyber security, but it is still very limited due to its newness and ongoing

evolution. Artificial intelligence is used against cyber-attacks by classifying malware, detecting intrusions, and directly combating them (Li, 2018). There is great potential for using artificial intelligence to combat cyber security as AI keeps developing.

Companies, especially smaller ones, should maintain correct cyber security practices to ensure protection, as most hackers target smaller companies. They are considered the weakest link in supply chains as they often do not have adequate protection measures (Urciuoli et al., 2013). These practices include security tests, secure coding practices, appropriate authentication and authorization, and logging and monitoring activities. It is necessary to run regular tests to ensure there are no holes or flaws in cyber security (Nathwani, 2023). Next, security practices should be integrated into the code at every step and process. These practices include using secure coding frameworks, avoiding insecure coding practices, and using source code analysis tools (Nathwani, 2023). Appropriate authentication and authorization are also crucial as they help prevent access to certain resources. It helps ensure that only authorized users can access these resources (Nathwani, 2023), which also helps prevent data leaks. Finally, logging and monitoring help keep track of the system at all times. They help detect suspicious behavior, such as traffic, user logins, and system events (Nathwani, 2023).

Conclusion

The rise of technology has led to an increased frequency and damage of cyber-attacks, harming individuals, companies, and supply chains. Cyber-attacks come in many forms and can steal personal information from individuals, cause economic and reputational damage to companies, and create major disruptions in supply chains. However, we can mitigate and even prevent cyber-attacks by maintaining secure cyber practices and using new technological advances, such as artificial intelligence, to advance cyber security.

References

Agrafiotis, Ioannis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, and David Upton. "A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate." *Journal of Cybersecurity* 4, no. 1 (January 1, 2018): tyy006. https://doi.org/10.1093/cybsec/tyy006.

Buriro, Attaullah, Abdul Baseer Buriro, Tahir Ahmad, Saifullah Buriro, and Subhan Ullah. "MalwD&C: A Quick and Accurate Machine Learning-Based Approach for Malware Detection and Categorization." *Applied Sciences* 13, no. 4 (January 2023): 2508. https://doi.org/10.3390/app13042508.

Green, James A., ed. *Cyber Warfare: A Multidisciplinary Analysis*. Routledge Studies in Conflict, Security and Technology. London New York: Routledge, Taylor & Francis Group, 2016.

Holt, Thomas J. "Exploring the Social Organisation and Structure of Stolen Data Markets." *Global Crime* 14, no. 2–3 (May 1, 2013): 155–74. https://doi.org/10.1080/17440572.2013.787925.

Kumar, Lokesh, Nikhil Singhal, Mudit Agarwal, Mukul Kumar, and Jaivardhan Bhardwaj. "Effect of a Cyber Attack on a Company's Economic Performance," n.d.

Lau, F., S.H. Rubin, M.H. Smith, and L. Trajkovic. "Distributed Denial of Service Attacks." In *Smc 2000 Conference Proceedings. 2000 Ieee International Conference on Systems, Man and Cybernetics. "cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions" (Cat. No.0*, 3:2275–80 vol.3, 2000. https://doi.org/10.1109/ICSMC.2000.886455.

Li, Jian-hua. "Cyber Security Meets Artificial Intelligence: A Survey." *Frontiers of Information*

Technology & Electronic Engineering 19, no. 12 (December 1, 2018): 1462–74. https://doi.org/10.1631/FITEE.1800573.

Nathwani, Sneha. "IMPLEMENTATION OF TECHNIQUES TO AVOID CYBER ATTACKS" 11, no. 2 (2023).

Perwej, Dr.Yusuf, Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar, and Anurag Kumar Jaiswal. "A Systematic Literature Review on the Cyber Security." *International Journal of Scientific Research and Management* 9, no. 12 (December 2021): 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04.

Rao, Routhu Srinivasa, and Alwyn Roshan Pais. "Detection of Phishing Websites Using an Efficient Feature-Based Machine Learning Framework." *Neural Computing and Applications* 31, no. 8 (August 1, 2019): 3851–73. https://doi.org/10.1007/s00521-017-3305-0.

Samtani, Sagar, Ryan Chinn, Hsinchun Chen, and Jay F. Nunamaker Jr. "Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence." *Journal of Management Information Systems* 34, no. 4 (October 2, 2017): 1023–53. https://doi.org/10.1080/07421222.2017.1394049.

Singh, Sakshi, and Suresh Kumar. "THE TIMES OF CYBER ATTACKS," n.d.

Srinivas, Jangirala, Ashok Kumar Das, and Neeraj Kumar. "Government Regulations in Cyber Security: Framework, Standards and Recommendations." *Future Generation Computer Systems* 92 (March 1, 2019): 178–88. https://doi.org/10.1016/j.future.2018.09.063.

Taddeo, Mariarosaria. "Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity." *Minds and Machines* 29, no. 2 (June 1, 2019): 187–91. https://doi.org/10.1007/s11023-019-09504-8.

Urciuoli, Luca, Toni Männistö, Juha Hintsa, and Tamanna Khan. “Supply Chain Cyber Security – Potential Threats.” *Information & Security: An International Journal* 29 (2013): 51–68. https://doi.org/10.11610/isij.2904.

Yeboah-Ofori, Abel, and Shareeful Islam. “Cyber Security Threat Modeling for Supply Chain Organizational Environments.” *Future Internet* 11, no. 3 (March 2019): 63. https://doi.org/10.3390/fi11030063.

Zimoń, Michał, and Rafał Kasprzyk. *Digital Revolution and Cyber Threats as Its Consequence*, 2021.