Text

Description automatically generated

Department of Information Science, University of North Texas

INF0 5737: Information and Cyber Security

Nayana Pampapura Madali

**The commercial impact of cyber risk on the Internet of Things (IoT)**

**Group Project Members**: Vijay Raj Pathani (11609155), Praveen Kumar Maddineni (11601302)

Cyber risk refers to the possibility of monetary loss, reputational harm, or other unfavorable outcomes resulting from a data breach or other cyber security event. The Internet of Things (IoT) is used by most businesses to increase productivity and create new revenue streams. Since more and more devices are becoming online, the number of cyberattacks has increased. Up from $2.1 trillion in 2019, Juniper Research estimates that the cost of data breaches will reach $5 trillion by 2024. Many businesses are concerned about the damage to their brand that may result from a cyber-attack. As many as 43% of UK businesses worry that a cyberattack may hurt their image. Disruption to operations (31%), followed by financial loss (34%). The legal repercussions of a data leak are another issue. Fines for the EU's General Data Protection Regulation (GDPR) violations might amount to more than 4% of a company's annual global revenues. Companies may change their stock value due to cyber assaults (Swapnil, 2021). After the 2017 data breach, shares of Equifax fell by 15%. To mitigate the impact of a cyber-attack, businesses may get cyber insurance, implement stringent security measures, and provide employees with cyber security training.

The business effect of cyber risk in IoT may be linked to CISSP themes. CISSP helps firms identify IoT dangers and how to minimize them. CISSP can help develop secure IoT environments and react to and recover from issues. Most of these devices have inadequate security and allow hackers to access the larger network (Swapnil, 2021). We must avoid cyber security threats from IoT devices as the sector adapts. Cyber security is the method to overcome our difficulties. Some of these technologies are attackable. Risk analysis is part of a strong security plan (Swapnil, 2021).

Furthermore, it safeguards networks, computers, servers, devices, gadgets and data from threats. Adopting a solid cyber security measure is a problem today because attackers are increasingly clever, and there are more gadgets than humans; using a framework will show you where you have the largest security risk compared to the rest of the firm (Swapnil, 2021). If the cloud architecture is appropriately designed, the cloud instance's security is maintained, and cloud-to-thing communication is ensured, cloud technologies may lessen cyber threats.

IoT provides new methods for organizations to produce value, connection and data exchange, creates opportunities for data to explore new things, and has its own few difficulties. In this procedure, IOT Security assesses and ranks risk. IoT Security evaluates and ranks risk at four levels: devices, profiles, sites, and organizations. A continual risk assessment identifies weaknesses and threats (Swapnil, 2021). For cyber hazards, we suggest the NIST Cyber Security Framework. Various ratings show the danger in different parts of your network. The NIST Cyber Security Framework (NIST CSF) is the gold standard for cyber-security programs. Garage door openers and deactivating the house alarm are examples of smart homes (Swapnil, 2021). If simply the garage door opener is hacked, the whole alarm system might be disabled. Home gadgets, including TVs, thermostats, home alarms, door locks, smart houses, and garage door openers, present a variety of entry points for hackers to breach IoT systems and acquire client information.

Furthermore, this aligns with my interest since cyber security is vital now that more machines are networked, and more entities support security standards and best practices. A thousand "small things" on the network, from sensors to 3D printers, became an alternative for invaders to concentrate on high-profile control systems (Alkhudhayr et al., 2019). Lack of confidence leads to a lack of organization-wide security and cyber risk awareness. ("Deloitte Cyber and Dragos Share Top IoT Cyber Risks - Press...") The amount of cyber-attacks, data breaches, and total damage caused by insecure IoT devices is rising since firms do not realize the extent of the issue (Alkhudhayr et al., 2019). The cloud enhances cyber security but raises IoT cyber dangers. IoT's real-time data increases the cyber danger.

Finally, any firm may use a few essential risk management concepts to limit the commercial effect of cyber risk on the Internet of Things (IoT). First, know the organization's most valuable assets and what dangers may attack them. After understanding its assets and dangers, the business must establish a strategy to secure them and react to occurrences. This strategy should be adapted to the organization's requirements and revised as needed (Alkhudhayr et al., 2019). Ensure that all workers understand the organization's cyber security rules and procedures. By implementing these actions, enterprises may reduce IoT cyber risk.

**References**

Swapnil, S. (2021). *cyber security and internet of things - researchgate*. Cyber security and the internet of things. Retrieved October 24, 2022, from <https://www.researchgate.net/publication/351576013_Cyber_Security_and_Internet_of_Things>

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information security: A review of information security issues and Techniques. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. <https://doi.org/10.1109/cais.2019.8769504>