CHAPTER 2

Emerging Cybersecurity Risks

1. Impact of Emerging Cybersecurity Risks & Digital Transformation

With the growing digital shift, there has been a surge in sophisticated cyber threats too. We are also witnessing new and creative approaches taken by threat actors to take advantage of weaknesses in both technology and human behaviour. Some of this year's Most Dangerous Emerging Cybersecurity Threats include Social Engineering Attacks, Cryptojacking, and Supply Chain Attacks. These attacks threaten not just individuals, but larger incidents like this one can represent huge threats to the economy and to global cybersecurity. This digital shift is reshaping industries and everyday life, increasing interconnectivity and the dependence on digital platforms for communication, commerce, and information sharing[50].

The Most Dangerous Emerging Cybersecurity Threats

The latest cybersecurity threats such as advanced phishing attacks and AI-based scams, as well as ransomware attacks involving double extortion techniques are considered the most dangerous cybersecurity threat. Additionally, a rapid rise in IoT (Internet of Things) and supply chain related vulnerabilities have left enterprises more exposed than any time before to breaches that can expose sensitive data and disrupt crucial functions.

[50] Marc van Zadelhoff, "The Biggest Cybersecurity Threats Are Inside Your Company," *Harvard Business Review*, September 19, 2016

Social Engineering Attacks

They are measured on how many people they can get to slip the line and how much money they can make. The information can be used in imitating as an organization to access sensitive information, which could also be examples of such attacks: Phishing, Pretexting and baiting etc so, it is essential for an organization to train its employees to recognize and respond to these type of attacks[51].

Cryptojacking

Cryptojacking refers to a nefarious act whereby cybercriminals leverage a victim's computing resources without their knowledge or permission in order to mine cryptocurrency.[52] The use of such software not only significantly hampers system performance and results in higher energy consumption for the user, but it also brings forth the increasing call for solid cybersecurity mechanisms to authenticate mechanism that can detect unauthorized use of devices, and the need to protect oneself from malicious array of programs that hog system resource.

Supply Chain Attacks

Supply chain attacks exploit weaknesses in the ecosystem of suppliers and third-party vendors used by organizations, enabling malicious actors to gain access bypassing protections. Infiltrating a trusted partner's infrastructure allows attackers to access sensitive data, or to deploy malicious software to all organizations linked to a trusted partner, reinforcing the need to secure links in the supply chain against such attacks[53].

2. Social Engineering Attacks Overview

Social engineering attacks rely on human aspects rather than technological failures. Perpetrators exploit psychological vulnerabilities to trick individuals into revealing personal information, clicking on malicious links, or granting unauthorized access. These assaults are increasing in sophistication, making them some of the gravest cybersecurity threats we face.

Cybercriminals resort to various psychological tactics to manipulate their victims. They can include tactics such as creating urgency, fear, or adding incentives to drive

[51] Fabian Muhly, Jennifer Jordan, and Robert B. Cialdini, "Your Employees Are Your Best Defense Against Cyberattacks," *Harvard Business Review*, August 30, 2021,

[52] Mike Chapple, CC Certified in Cybersecurity Study Guide (Wiley Publishing 2024), 181

[53] Kiran Sridhar, Daniel Ralph, and Jennifer Copic, "3 Strategies to Secure Your Digital Supply Chain," *Harvard Business Review*, August 9, 2021