Chapter 3
CyberSecurity Essentials for Industry 5.0

Mahmoud Numan Bakkar
https://orcid.org/0000-0003-4637-4035
Institute of Applied Technology, Abu Dhabi Vocational Education and Training Institute, UAE

ABSTRACT

Currently, hacking threats have increased exponentially because of the massive integration of technology into our daily life practices. Hackers are usually known for their advanced programming skills. They utilize these skills in challenging old systems and work on breaking them to test their capabilities and achieve their desire or motivation. The terminology of cybercrime evolved with the current industry's 4.0 and 5.0 revolutions and the changing of cybersecurity domains. This book chapter will discuss the different types of attacks in the industry 5.0 Era. Show examples of industrial cybersecurity attacks, Industry 5.0 cybersecurity vulnerabilities, and issues.

INTRODUCTION

Hacking threats have increased exponentially because of the massive integration of technology into our daily life practices. Hackers are usually known for their advanced programming skills. They utilize these skills in challenging old systems and work on breaking them to test their capabilities and achieve their desire or motivation. The terminology of cybercrime evolved with the current industry 4.0 and 5.0.0 revolutions and the changing of cybersecurity domains. The cybersecurity domain developed through the Internet enables companies to collect users' data such as names, backgrounds, friends, jobs, interests, travels, and locations. Internet

DOI: 10.4018/978-1-7998-8805-5.ch003

evaluations created many global domains for data, such as Google, for the fact that many people in the world use and have Google accounts, and it is available on 80% of mobile devices around the globe (Academy, 2022)

Facebook is also considered an enormous cybersecurity domain, fed with many personal data entered by users. In addition, the LinkedIn network of professional employees and employers is all connected through one network. Those domains, in addition to the industry's four technologies, such as the Internet of Things (IoT), Cyber-Physical Systems, Smart manufacturing, smart factories, cloud computing, and Artificial Intelligence, all created a demand for cybersecurity measures to protect the environment from being attacked and compromised for specific harmful actions. Industry 5.0 Cybersecurity Essentials emphasizes business continuity and risk management; more white and gray hat hackers are needed in the upcoming Industry 5.0. Having white hat hackers could reduce the vulnerability of the industrial systems; however, it may add more cost to the production line to create a fort line against the black hat hackers and the organized hackers, Script. Moreover, kiddies, black hackers, and organized hackers could have cyber motivation for their crimes, such as financial gain (Academy, 2022).

The first CyberSecurity Essential threat for Industry 5.0 is cyber criminals, who are either insiders such as employees, contractors, or outsiders such as hackers (black, white, grey) and organized attackers (Hacktivist, Terrorist, State-Sponsored). They are working towards financial gain; they can work on cracking passwords and sending malware and viruses to steal financial information, such as credit cards or any information that can be sold for high earnings. Cybercrime countermeasures varied based on data sensitivity and value. However, the current practices start with a system that alerts the victims early before the attack occurs using the honey bots and using shared knowledge and expertise of attacks, such as maintaining a vulnerability database that keeps the records of the national common vulnerability and exposures (CVE) (Academy, 2022)—also sharing intelligence, in addition, having laws information security management standards (ISM) such as ISO /IEC 27000 (Academy, 2022).

Databases are the primary concern of companies in the industry 5.0 Era. Medical, finance, education, and private and personal records can be the primary targets for cybercriminals. The second threat is the internet manufacturing infrastructure (IMI); many organizations use cloud computing technologies, so attacks such as DNS spoofing redirect the domain names to the attack's computer. Also, packet sniffing can be used to steal sensitive transmitted data such as credit cards, passwords, and attacks such as man in the middle can be used for packet forgery. In addition to attacking systems that control the manufacturing industry, for example, supervisory control and data acquisition (SCADA), an attack on industry needs such as telecommunication, logistical systems, transportation, electrical systems, and power providers. In the