Chapter 4
Industry 5.0 and Cyber Crime Security Threats

Lila Rajabion
SUNY Empire State College, USA

ABSTRACT

Cybersecurity is the act of protecting networks, programs, and systems against various hostile and digital assaults. Subset of a security program, it defends cyberspace from escalating assaults and dangers that result in significant damage to resources like finances, information, and applications. Hackers are increasingly targeting firms in the financial and industrial sectors, particularly for the purpose of stealing sensitive data. As a result, many business leaders are turning to cybersecurity to meet their company's security demands and prevent its precious assets from falling into the wrong hands. When it comes to safeguarding software and hardware against unauthorized access and intrusion, cyber assaults play a critical role. The security measure makes use of several security approaches, such as cybersecurity software, access control systems, antivirus and malware security programs, firewalls, and program upgrades, among all system users.

INTRODUCTION

Cybersecurity is the act of protecting networks, programs, and systems against various hostile and digital assaults. The subset of a security program defends cyberspace from escalating assaults and dangers that significantly damage resources like finance, information, and applications. Hackers are increasingly targeting firms in the financial and industrial sectors, mainly to steal sensitive data (Lezzi, Lazoi, & Corallo, 2018). As a result, many business leaders are turning to cybersecurity to

DOI: 10.4018/978-1-7998-8805-5.ch004

meet their company's security demands and prevent its precious assets from falling into the wrong hands.

When it comes to safeguarding software and hardware against unauthorized access and intrusion, cyber assaults play a critical role. The security measure uses several security approaches, such as cybersecurity software, access control systems, antivirus and malware, firewalls, program upgrades, intrusion detections, and raising security awareness among all system users. As a result of these changes, cybersecurity is now seen as the most robust modern-day defense against digital threats.

Research Objectives

This study's goal was to create new information and reinforce existing knowledge, so it may be shared with other students and the public. Furthermore, to guarantee that students and researchers thoroughly understand the subject, it provides concise explanations of various ideas and procedures and their advantages, hazards, and tactics. The primary aims of this study are to:

- explore the past, present, and potential futures of the cybersecurity sector, identifying which cyberattacks are more widespread; and
- explore the benefits of hyperconnected systems for Cybersecurity for Industry 5.0.

Literature Review

According to Randall and Kroll (2018) study, millions of pieces of personally identifiable information have been stolen from large and small companies across the globe, including the healthcare and government sectors. As a result, several sectors have resorted to cybersecurity to prevent data breaches and theft, secure trade secrets, maintain regulatory compliance, protect sensitive information, and facilitate and enhance corporate operations.

The industrial sector has had to contend with cybersecurity issues for several years, including hackers and malicious intrusions into industrial control systems. These disturbances influence product quality, brand reputation, sales income, market globalization, and the safety of employees.

Industries must modify their business processes and prevent issues influencing their businesses to reduce these damaging interruptions and implement appropriate security procedures. Modern technologies like mobile computing and the Internet of Things have aided strategic decision-making to deter cyber threats, attacks, and vulnerabilities (Lezzi et al., 2018). As a result, these technologies provided industrial control systems with security strategies that enhanced cybersecurity.