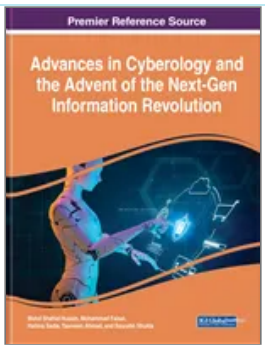

Cyber Threats in Agriculture and the Food Industry: An Indian Perspective

Harish Chandra Verma (/affiliate/harish-chandra-verma/445833/), Saurabh Srivastava (/affiliate/saurabh-srivastava/445834/), Tasneem Ahmed, Nayyar Ali Usmani

Source Title: Advances in Cyberology and the Advent of the Next-Gen Information Revolution (/book/advances-cyberology-advent-next-gen/311443)

Pages: 14

DOI: 10.4018/978-1-6684-8133-2.ch006

Abstract

A cyber threat is a harmful act meant to steal, corrupt, or undermine an organization's digital stability. At present cyber threats in agriculture and food industry is a rising concern because farming is becoming more dependent on computers and Internet access. The attacks that fall under this category include denial of service attacks, computer viruses. Growing food demand and shortage of skilled labours have necessitated for the adoption of digital agriculture. The major challenge is to prevent it from cyber threats for successful implementation. As ransomware hackers are increasingly likely to target food supply chain, the food industry is experiencing an increase in cyber-security threats, which might result in business interruptions. Due to the fragile nature of the food supply, the entire food sector needs to be protected . In this chapter, major issue on cyber threats, challenges of cyber-security, some notable cyber-attacks, and cyber-security solutions for the food/agriculture industry are discussed in detail.

Chapter Preview

Top

Introduction

Globally, India is one of the major countries in the agriculture sector and agriculture is the primary source of livelihood for about 58% of India's population. Agriculture is considered the backbone of the Indian economy. It has helped the Indian economy in several ways: providing food, a source of national income, a Source of employment generation, accumulation of the National Capital, provides raw materials for industries.Similarly, according to the United Nations (UN), the world population is expected to exceed 9 billion by 2050 (Roser, 2020; Godfray et al., 2010). According to the United Nations Food and Agriculture Organization, such a rise in population necessitates an increase in food production of about 70%. Many digital devices such as smartphones, various sensors, global position systems (GPSs), robotics, and drones could be utilised to extract valuable data analysis and make effective decisions to increase food production with less human resources and intervention (Adel et al., 2022). A criminal act that destroys data, steals data, or otherwise harms digital infrastructure is considered a cyber security concern.Cybersecurity is a multidisciplinary domain consisting of cybersecurity, bio-security, and cyber-physical security (Fountas et al., 2015).

The digitalization of agriculture is an ongoing process that causes an increasing number of agricultural systems to be connected through the Internet (Adel et al., 2022). Because farming is becoming more dependent on computers and Internet connectivity, cyber security in the agriculture and food industry is a growing problem. Digital agriculture is not immune to cyber-attacks, which can range from controlling the heating and ventilation system of a greenhouse to controlling a drone used for spraying crops (Adel et al., 2022). The issue has received major research attention in recent years when the agro-technology