

## Chapter 4

# Cyber Threat Migration: Perpetuating in the Healthcare Sector and Agriculture and Food Industries

**Minhaj Akhtar Usmani**

*Era University, India*

**Kainat Akhtar Usmani**

*Integral University, India*

**Adil Kaleem**

*NCS Group, Australia*

**Mohammad Samiuddin**

*University of Technology and Applied Sciences, Oman*

### **ABSTRACT**

*'Globalization,' 'industrialization,' 'cyber connectivity,' 'digitalization,' and 'e-commerce' are not fantasy words in today's era. They all amalgamated towards the growth and development of every sector in the country. But as on other side of the coin, cyber security is on the verge of serious threats in digital world. The danger posed by cyber security threats in today's world cannot be understated. The health sector, agriculture, and food and beverage industries are no exemptions. As they all are inter-related, they manage an array of assets, including infrastructure, applications, managed and unmanaged endpoints, mobile devices, and cloud services, all of which can be attacked. Information and cyber security are trending topics. As the security risk is scooping high, different organizations should take steps forward to protect themselves. This chapter focuses on the frightening hikes in incidences of cyber-attacks, and also focuses on major cyber security approaches to minimize the risk of cyber breaches and making these industries flourish like never before.*

### BACKGROUND

In the quest for digitalization, India has become an easy target for cyber-attacks due to poor cyber security. Today, numerous organizations are plagued by cyber-attacks that are advanced, persistent, and which can wreck both operations and reputation of companies, including food companies, agriculture sector and healthcare sector. Companies manage an array of assets, including infrastructure, applications, managed and unmanaged endpoints, mobile devices, and cloud services, all of which can be attacked. Just Food cyber security dashboard tracks data and information on cyber security in the food industry.

In many ways, the risks from cyber threats are no different than the safety risks that food companies mitigate every day. The same practices used to identify and address food-processing risks, such as foreign materials and pathogens, can apply to protecting data essential for processing. These practices call for evaluating the threats, assessing the likelihood of occurrences, and establishing programs for mitigation.

The security risks to food data fall into a few categories: theft, public exposure, data corruption or loss, and data manipulation or falsification. Assessing the likelihood of attack in each category requires identifying malicious actors and how each might benefit from an attack. Is the actor a foreign agent, cyber-criminal, disgruntled employee, a competitive spy, or extremist food activist? How would a bad actor benefit from stealing, exposing, manipulating, or corrupting data? (Woehl, 2022)

### BASIC TERMS AND DEFINITIONS

Before analyzing deep into the facts and findings related to cyber threats and cyber security it is mandatory to get acquainted with some basic terminology and definitions associated to them.

#### Cyber Security

Computer security, cyber security, or information technology security (IT security) is the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide. (Schatz *et al.*, 2017)

Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance. (Kianpour *et al.*, 2021) (Stevens, 2018)

#### Categories of Cyber Security

The 3 major types of cyber security are network security, cloud security, and physical security. The operating systems and network architecture make up the network security. It can include network protocols, firewalls, wireless access points, hosts, and servers.

Cyber security can be further categorized into five distinct types:

1. **Critical infrastructure security.** Critical infrastructure protection is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation.

22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:  
[www.igi-global.com/chapter/cyber-threat-migration/325546?camid=4v1](http://www.igi-global.com/chapter/cyber-threat-migration/325546?camid=4v1)

## Related Content

---

### Investigating the Connection between Awareness and Internet Non-Use

Carol Ting (2015). *International Journal of Information Communication Technologies and Human Development* (pp. 39-57).

[www.igi-global.com/article/investigating-the-connection-between-awareness-and-internet-non-use/143758?camid=4v1a](http://www.igi-global.com/article/investigating-the-connection-between-awareness-and-internet-non-use/143758?camid=4v1a)

### Local Search Applications and Urban Public Space: Interfacing Networked Individualism and Tangible Urbanism

Florian Fischer (2014). *International Journal of Technology and Human Interaction* (pp. 31-47).

[www.igi-global.com/article/local-search-applications-and-urban-public-space/114590?camid=4v1a](http://www.igi-global.com/article/local-search-applications-and-urban-public-space/114590?camid=4v1a)

### Dichotomous Radial Basis Tanimoto Network to Predict Delivery Mode in Maternal Care Domain

Kavitha Kannan and Balasubramanian Thangavel (2021). *International Journal of Information Communication Technologies and Human Development* (pp. 92-104).

[www.igi-global.com/article/dichotomous-radial-basis-tanimoto-network-to-predict-delivery-mode-in-maternal-care-domain/302105?camid=4v1a](http://www.igi-global.com/article/dichotomous-radial-basis-tanimoto-network-to-predict-delivery-mode-in-maternal-care-domain/302105?camid=4v1a)

### Healthcare Education: Integrating Simulation Technologies

Eva M. Frank (2018). *Handbook of Research on Human Development in the Digital Age* (pp. 163-182).

[www.igi-global.com/chapter/healthcare-education/186215?camid=4v1a](http://www.igi-global.com/chapter/healthcare-education/186215?camid=4v1a)