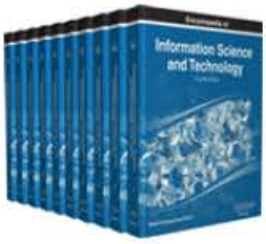

Concept and Practices of Cyber Supply Chain in Manufacturing Context

Anisha Banu Dawood Gani (Universiti Sains Malaysia, Malaysia) and Yudi Fernando (Universiti Malaysia Pahang, Malaysia)

Source Title: Encyclopedia of Information Science and Technology, Fourth Edition
 | Pages: 11
DOI: 10.4018/978-1-5225-2255-3.ch460

Abstract

The objective of this chapter is to discuss the concept and practices of cyber supply chain (CSC) in manufacturing context. Technological advancements are drastically transforming manufacturing industry, which in turn drives the need for a digitally integrated supply chain. While CSC has its share of benefits, it is also vulnerable to cyber threats. In order to mitigate the risks, a comprehensive security measures must be undertaken in the areas of technology, organization, governance, and culture, and integrate them into the company's established risk management processes. To ensure a resilient CSC, all members of the supply chain network must play a role to protect their respective systems from potential breach.

Chapter Preview

Background

Manufacturing is one of the leading industries of the global economy and is projected to undergo a major transformation driven by power of digitalization. Manufacturing industry's share of GDP has remained stable over the last 40 years. According to United Nations Industrial Development Organization (UNIDO), the total contribution of the entire manufacturing sector to GDP, measured as manufacturing value added (MVA), reached an all-time high of $9,228 billion in 2014. The MVA of developing and emerging industrial economies (DE IEs) for the same year increased 2.4 times from 2000, while their GDP doubled (UNIDO, 2015). Inarguably, manufacturing remains a key driving force of overall economic growth globally.

UNIDO Director General, Mr. Li Yong recognized that the technological change shall become one of the main drivers of long-term growth for the industry:

"In the coming decades, radical innovations such as the mobile internet, the Internet of Things and cloud computing are likely to revolutionize production processes and enhance living standards, particularly in developing countries", he envisioned.

These rising trends are promising evidence that the digitalization of manufacturing industry will dramatically transform the way companies operate in many areas – from Research & Development (R&D) efficiency and faster product launches to supply chain improvements, better operations services and more efficient processes. Oliver Wyman, one of the leading management consultancies in the world, predicts that the global annual margin impact of digital industry across discrete manufacturing in 2030 could be an estimated US$1.4 trillion (Oliver Wyman, 2016).

Key Terms in this Chapter

Digitalization: Use of digital technologies to change a business model.

Security: Free from danger and threats.

Risk Management: Procedure to avoid and minimize risks.

Cybercrime: Any crime that is facilitated or committed using a computer, network, or hardware device.

Cyber Supply Chain: An end to end integration of supply chain over secured and intricate digital network.

Supply Chain Integration: Coordination within a supply chain using integrated system.

Cybersecurity: Mechanism to fend off cyber crime.