Chapter 27
Security Framework for Supply-Chain Management

Kathick Raj Elangovan
Concordia University, Canada

ABSTRACT

In recent times, cyber-attacks have been a significant problem in any organization. It can damage the brand name if confidential data is compromised. A robust cybersecurity framework should be an essential aspect of any organization. This chapter talks about the security framework for cyber threats in supply chain management and discusses in detail the implementation of a secure environment through various controls. Today, a systematic method is used for handling sensitive information in an organization. It includes processes, people, and IT systems by implementing a risk management method. Distinct controls dedicated to different levels of domains, namely human resources, access control, asset management, cryptography, physical security, operations security, supplier relations, acquisition, incident management, and security governance are provided. Companies, contractors, and any others who are part of the supply chain organization must follow this security framework to defend from any cyber-attacks.

BACKGROUND

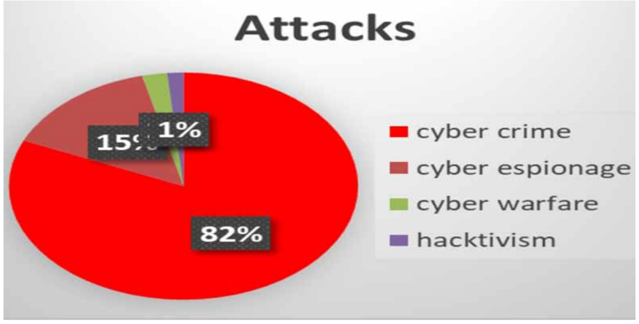
Cybersecurity threats pose a significant risk to any organization. According to 2018 average time to detect a breach takes up to 197 days (Ponemon, 2018) This can impact business, brand name, reputation, and revenue. To address this issue in supply chain-based organization and to enhance the cybersecurity, a security framework implementation is developed. A supply chain is a system of organizations, people, activities, information, and resources involved in moving a product or service from supplier to customer (Wikipedia, 2019a). The framework focuses on process, business drivers, people, and IT systems management by implementing a risk management approach.

DOI: 10.4018/978-1-6684-3698-1.ch027

Setting the Stage

Cybercriminals infiltrate into an organization to steal sensitive information. Cyber breach is the worst nightmare in the Information Technology world. A few impacts are damage to the brand name, litigation, financial losses, and data theft (Ponemon, 2018). As of 2016 cyber-attack have caused loss of around $ 450 billion to the international economy and it's on the rise every year. The primary motivation in attack scenario as shown in Figure 1. Cybercrime-related attacks top the charts when it comes to the different motivation behind the attacks (Appendix 1).

Figure 1. Attack coverage
Source: (Passeri, 2018)



SOLUTION APPROaCH

In recent days, the cyber-attacks towards supply chain management (SCM) have been very successful. Attackers target a weak or less secure member in a supply chain to gain access to the organization. Some of the weaker networks are mentioned below in Figure 2. one of the main reasons for the successful attack is no awareness about security in the organization and its vendors and everyone in the supply chain. Attackers use this to phish emails of the employees and send malware to infect the machines and infiltrate into the network to steal sensitive information. Attackers can request ransoms by encrypting essential data for an exchange of decryption key.

To fix these cyber risks, a security framework is required. A pure knowledge of security concerns, business processes distinct from the use of technology is needed. Every organization has its unique methods and tools to achieve the results reported by its framework. However, in this paper, This Paper propose one single security framework that must be followed by the organization and the companies in its supply chain. As described in Figure 3, The framework will follow five continuous and concurrent function or can be called a cybersecurity life cycle (Identity, Protect, Detect, Respond, Recover) (NIST, 2019). This process is used to identify, assess and manage cybersecurity risk in the environment proactively.