Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

# Cyber Security Risks and Challenges in Supply Chain

Om Pal
Ministry of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex, New Delhi

Bashir Alam
Department of Computer Engineering,
Jamia Millia Islamia, New Delhi

***Abstract:*** Traditional data security practices are not much helpful if any hardware or software component of the system is built to send the inner data to outside of the system or leave the back door open for intruders intentionally. This kind of back door entry may be restricted if proper inspection of the network components, monitoring of supply chain steps, history check of network component suppliers is done properly. To address the above issues, there is need of standard cyber security practice frameworks, cyber security guidelines in supply chain management to mitigate the cyber security risks in the supply chain of the network components. In this paper, need of cyber security practice framework, Strategies, Road Map and solutions to resolve the threats of Cyber security in supply chain are discussed and analyzed.

**Keywords:** Cyber security in supply chain, Cyber security risks in supply chain, cyber security practices, cyber security risks.

## 1. INTRODUCTION

In today's scenario electronic devices are integral part to everyday life, to the critical infrastructures, and to defense system. These electronics devices are built up through semiconductor integrated circuits. For example, smart phones, laptop computers and tablets, aircraft flight controls, the financial system, the power grid, automobile antilock braking etc. These devices can be trusted only if the chips are free of hidden malicious circuits which may be inserted during the design or manufacturing process of the chips [4].

Huawei introduced a mechanism for selection of the supplier through the list of 100 cyber-security requirements. The list of cyber security requirements basically covers 11 key areas: standards and processes, strategy governance and control, human resources, laws and regulations, verification, research and development, manufacturing, third-party supplier management, issue, delivering services securely, audit and defect and vulnerability resolution. At the time of supplier, organizations should explore the each area in details for detailed requirements [1, 2, 5, 6, 20].

Physical supply chain management present numerous risks during the phases of the chain. In cyber world also, supply chain plays an important role. If any cyber security equipment is supplied through supply chain then there are cyber security risks during the phases of supply chain. If any risk is detected after the delivery of the equipment then it is tough to detect the exact step of supply chain or sole responsible person to the damage occurred due to delivery of faulty equipment [7, 16, 17, 18].

The attacking technology like virus inclusion in software or hardware is on rise so, any hardware Trojans may be inserted in any phase of the supply chain for the purpose of hacking [3]. There are various types of hardware attacks which includes the following-

- Manufacturing backdoors may be created for malware or other penetrative purposes. Backdoors may be embedded in radio-frequency identification (RFID) chips and memories.
- Unauthorized access of protected memory
- Inclusion of faults for causing the interruption in the normal behavior of the equipment.
- Hardware tampering by performing various invasive operations
- Through insertion of hidden methods, the normal authentication mechanism of the systems may be bypassed.

Above hardware attacks may pertain to various devices or systems like:

- Network systems
- Authentication tokens and systems
- Banking systems
- Surveillance systems
- Industrial control systems
- Communication infrastructure devices

Most of us do not bother about the risks of the supply chain, genuineness of supplier, trustiness of the manufacturing process etc. But we generally mean cyber security only the network security and data protection. It may be firewalls, intrusion detection, secure and trained workforce, secure network design, social engineering etc.

But our assumption fails if one of the components is faulty in our network. If any component of the network is built to send the data outside of the network then general information assurance practices do not help too much. As many companies get supply of the components from the contractors before the final assembly so, consumer may not be able to find who built the particular component of his/her device. Authenticity of the supplied component is also doubtful if the contractor is not a reputed contractor or he/she did not follow the manufacturing standards. Therefore, the efficient management of the supply chain of the cyber security products is the necessity and this is also the need for the cyber security program. If compromised components are prevented from entering in the network then it will improve the overall cyber security and reliability of the product would be also increased [8, 9, 10, 11].

Cyber supply chain risks cannot be handled through Information Technology tool only. Cyber supply chain risks touch sourcing of product, management of vendors, transportation security, supply chain continuity and quality

and other functions across the organization and needs a coordinated effort to address the risk issues. Cyber security in supply chain is a multi dimensional problem which include management of supply chain, Quality and production assurance standards, manufacturing process standards, IT problem etc[12, 13, 14, 15,21].

## 2. CYBER SECURITY PRACTICES AT SUPPLIER'S END:

Companies are using the questionnaire to evaluate the security practice standards followed by suppliers. Using the appropriate set of questions, companies determine how much security practices are risky of their supplier's. Following are some questions which are being used for making the questionnaire-

(i) Whether design process is documented?
(ii) Is the design process of software or hardware product Repeatable?
(iii) How vendor deal the existing and emerging vulnerabilities? How vendor is capable to address new vulnerabilities?
(iv) What kind of standards are being used by vendor to manage and monitor manufacturing, assembling, testing processes?.
(v) How is code quality is tested?
(vi) What techniques, procedures and approaches are being used for protection and detection of malware.
(vii) How "tamper proofing" of products is done? What are methods for closing the backdoors?
(viii) Whether all process are documented properly and audition is conducted as per standards?
(ix) What kind of access controls are in place.
(x) How customer's data is protected?
(xi) What are the encryption mechanism?
(xii) How much is the retention period for data?
(xiii) What is the policy for data destruction when the partnership is dissolved?
(xiv) Whether background checks are performed for employees? If yes then how frequently?
(xv) What kind of security practices are followed.
(xvi) Whether there is proper cyber security check list for upstream and downstream suppliers? How is adherence to check list?
(xvii) Whether proper security checks are performed for the distribution process?
(xviii) What is the selection criteria for selecting the distribution channels?
(xix) What is the mechanism to disposed off the counterfeit component?
(xx) How does vendor assure the security of the process, product, service etc. throughout the product life cycle?

## 3. SUPPLY CHAIN MANAGEMENT TIERS

Supply chain management tiers describe the level of any organization in terms of the familiarity of the organization with risk free SCM. Organizations may be categorized in different levels according the risk free standards, rules, capability of countering the SCM risk, assessment of SCM risk and capability of repeatability of the secure practice. SCM implementation tiers may be categorized in four categories-

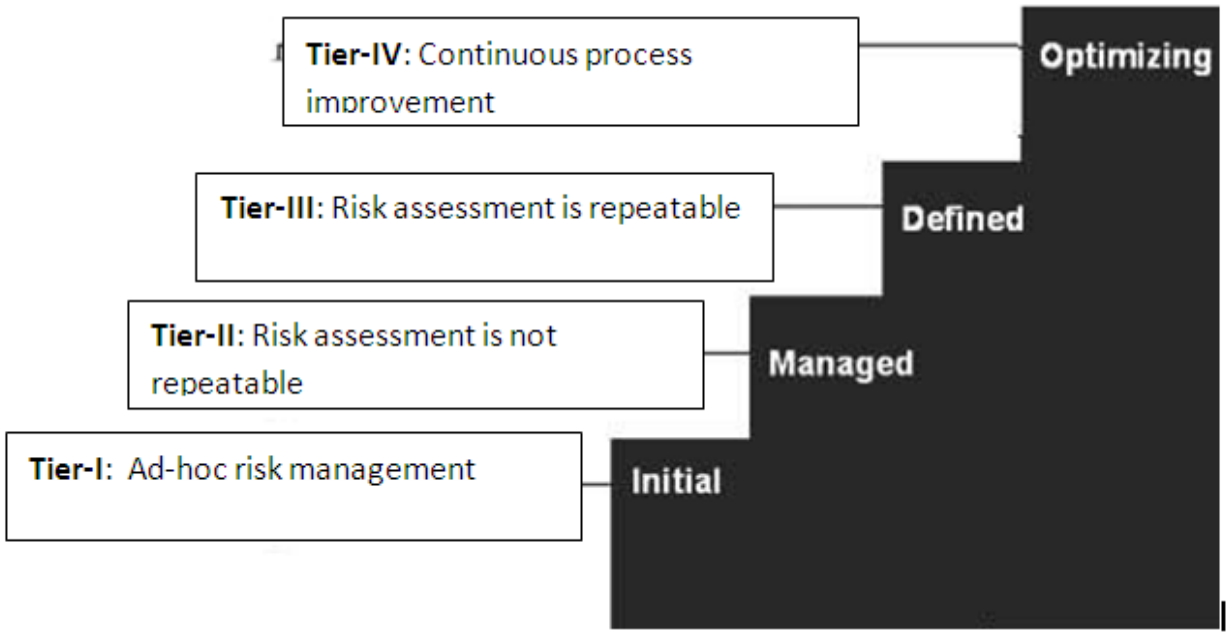


**Fig 1**. SCM Tier Implementation

(i) **Tier-I**: In this tier, security related practices are not well designed. In these type of organizations, secure SCM practices are partially followed. In case of any observed risk in SCM, it is counter down on ad-hoc basis.

(ii) **Tier-II:** In this tier, at upper management level, the Secure SCM practices have been approved. However, Secure SCM practices are not being followed within the organization at operational level. In these organizations, SCM risk assessment is not repeatable.

(iii) **Tier-III:** In this tier, at upper management level, the Secure SCM practices have been approved. SCM risk assessment is also repeatable. These organizations have well established agreements and standardized communication with Government and other parties like supplier and consumers.

(iv) **Tier-IV:** This is the highest level of SCM implementation in any organization. At this level, all policies, practices, rules, guidelines are well formulated and are in practice. Organization has well developed capability to counter any SCM risk in real time. This kind of organization, not only follows risk free practices within the organization but also it coordinates the secure SCM practices among other organizations, suppliers and consumers.

## 4. IMPORTANCE OF HAVING A SECURE SUPPLY CHAIN MANAGEMENT LIFE CYCLE

Supply chain risk management is not just the delivery of the products and services on time, but it is the delivery of the products and services with free of risks. A risk free and efficient product life cycle is required which minimizes the cyber security risks of the products and services. Cyber security risks may be defined as any abnormal activity like malicious behavior tainted by malicious actors, or products, services may be counterfeited or contain counterfeit circuits, components etc. which may be used for illicit purpose. Only IT security system is not sufficient to secure critical information unless whole supply chain use secure cyber security practices and standards.

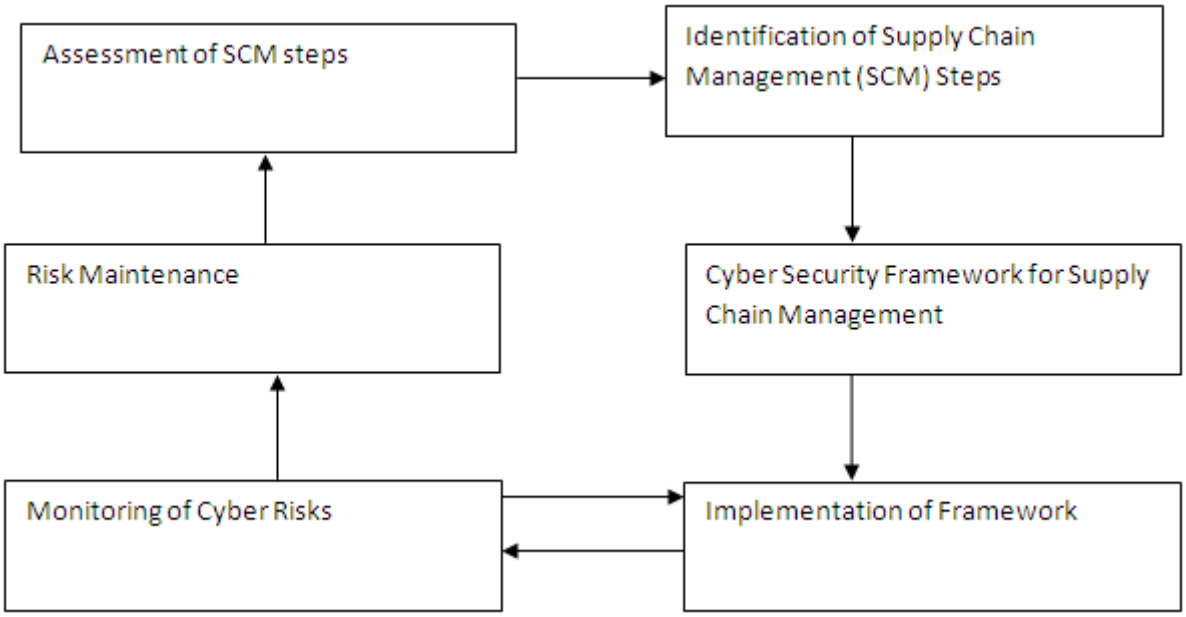


**Fig. 2: Cyber Security SCM Life Cycle**

To manage the critical information in risk free manner, the above proposed cyber security SCM life cycle may play an important role. If all steps of the Cyber Security SCM Life Cycle are followed properly then a risk free SCM cycle may be achieved.

## 5. STRATEGIES, ROAD MAP AND SOLUTIONS TO RESOLVE THE THREATS OF CYBER SECURITY IN SUPPLY CHAIN-

Global community as well as individual organizations should take the steps towards to reach an agreement on principles, standards, laws, norms of conducts, best practices, and protocols for which the trust has to be build up and continuously validated. Many organizations have already started to tackle the issue of cyber security in SCM. Following are some important steps which have been initiated by the organizations [21]-

(i) **Cyber Security Perspectives: 100 requirements formulated by Huawei Ltd**- Huawei has formulated the top 100 security-related requirements list. The formulated list focuses on technology, security related parameters etc which should be considered and should be expected from vendors. Huawei formulated the list through asking the security related questions to buyers and vendor, and Huawei continuously assesses the standards and best practice to help buyers in analyzing the cyber security capabilities of vendors while dealing with tenders.

(ii) **Huawei's approach to tackle the supply chain risks** Huawei has also developed an ISO 28000 standard supplier management system. This supplier management system is helpful in identifying and controlling the security risks during the end-to-end process from the point of incoming of the materials to delivery of the product. Huawei selects and qualifies suppliers based on their systems, process standards and products, choosing those that contribute towards the quality and security to the products and services. Huawei monitors and regularly checks the quality and efficiency of the qualified contractors and suppliers, and also checks the integrity of the materials provided by third party, production and delivery process. Huawei evaluates the performance of each point of SCM and

establishes a traceable system throughout the supply chain of the products and services.

(iii) **NIST Framework** is a tool that analyzes the possible risks and prepares an appropriate path towards a risk free environment for any organization. NIST Framework is a tool which analyzes the risks of a particular organization neutrally. It analyzes and applies the standards which are applicable in risk evaluation for that organization. In general, it lays out a method of risk analysis framed by standards and best practices, so any organization can use it. Using the present standards and best practices of the organization, it analyzes the risks. It also provides guidance to organization and to help it to determine and implement the best path forward by mapping the risk elements to whatever standards are applicable to the requirement for that sector or industry.

(iv) **Open Trusted Technology Provider Standard (O-TTPS)**- O-TTPS has been recognized by ISO (International Standards Organization) and International Electro technical Commission (IEC) as ISO/IEC 20243:2015 recently. This tool address the risks related to supply chain security, third-party providers, vendors and product integrity for any organization. O-TTPS provides a set of predictive requirements and appropriate recommendations to follow the best practices throughout the product lifecycle.

(v) **Initiatives taken by other Countries to tackle the supply chain risks-**

(a) **Chinese Counter-terrorism Law (CTL),** which took effect on January 1, 2016, outlines rules for internet and telecom enterprise to cooperate and support to government authorities in investigation of terrorist activities in China. Chinese Counter-terrorism Law also requires Internet Service Providers (ISPs) to implement the content monitoring system, and adopt the security measures as recommended by Government to prevent the dissemination of information which contains extremist, terrorist and anti-national content.

(b) **Centre for the protection of national infrastructure (CPNI), UK Government**- CPNI issues advisories to organizations to implement a risk mitigation plan that include the following: Comprehensive mapping of all tiers of the upstream (supply of components from small vendors to main vendor) and downstream (main vendor to consumer through distribution channel) supply chain to the level of individual contracts which plays the role of risk-scorer in to the organization's existing security risk assessment, assurance of suppliers, due diligence, accreditation, appropriate and proportionate measures to mitigate the risk, audit arrangements of the system and compliance of the security measures in the SCM system.

## 6. CONCLUSION

It is seen that current practices to deal with cyber security risks in supply chain are not adequate. Any faulty component in the network may be a serious cause of damage in terms of business loss, security breach, disclosing of secret information etc. These kinds of cyber security risks may be minimized if proper inspection of the network components, monitoring of supply chain steps, assessment of possible cyber security risks, process monitoring, product evaluation, integrity check of third party products, history check of network component suppliers etc is done properly. To address these issues, there is need of standard cyber security practice frameworks, cyber security guidelines in supply chain management to mitigate the cyber security risks in the supply chain of the network components. In this paper, the need of cyber security practice frameworks, Strategies, Road Map and possible solutions to resolve the threats of Cyber security in supply chain are discussed and analyzed. Each enterprise or business unit should practice the appropriate supply chain frameworks and guidelines like NIST framework, O-TTPS, ISO 2800 (Supply chain security Management). In addition of this, audit of Cyber SCM may be conducted at appropriate levels like branch level, regional level, and Country level etc. Questionnaire may be prepared by the expert committee for their employees to know the security requirement at their functional level. Training and workshop may be conducted for employees to understand the available Frameworks, standards, best practices to reduce the risk in Cyber Security SCM.

## 7. REFERENCES


1. https://www.nist.gov/sites/default/files/documents/2016/09/16/huawei_rfi_supply_chain.pdf
2. http://www.prnewswire.com/news-releases/huawei-introduces-cyber-security-top-100-requirements-for-selecting-suppliers-300174398.html
3. http://resources.infosecinstitute.com/hardware-attacks-backdoors-and-electronic-component-qualification/
4. http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity
5. http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-310548.htm#.WBxYsi197IU
6. http://www.cambridgewireless.co.uk/Presentation/SecDefSIG_29.09.15_DaveFrancis_Huawei.pdf
7. Cyber-security risks in the supply chain, CERT-UK report 2015. ( https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf)
8. James J. Cebula Lisa R. Young (2010), A Taxonomy of Operational Cyber Security Risks, report of Carnegie Mellon University. (http://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf)
9. David Inserra and Steven P. Bucci (2014), "Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace" Backgrounder (http://thf_media.s3.amazonaws.com/2014/pdf/BG2880.pdf)
10. http://www.govtech.com/security/5-Steps-to-Cyber-Security.html
11. http://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security.aspx
12. https://staysafeonline.org/re-cyber/cyber-risk-assessment-management/
13. CANSO Cyber Security and Risk Assessment Guide, June 2014 (https://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf)

14. https://www.bitsighttech.com/blog/supply-chain-risk-management
15. http://www.supplychainquarterly.com/topics/Technology/20150622-is-your-supply-chain-safe-from-cyberattacks/
16. https://en.wikipedia.org/wiki/Supply_chain_cyber_security
17. http://www.supplychainbrain.com/content/blogs/think-tank/blog/article/why-cybersecurity-is-a-supply-chain-problem/
18. https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252
19. http://utc.org/wp-content/uploads/2016/03/SupplyChain2015.pdf
20. http://www.huawei.com/en/news/2015/11/Huawei%20Introduces%20Cyber%20Security%20Top%20100%20Requirements%20for%20Selecting%20Suppliers
21. Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology(2017) (https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf)