|  |  |  |
| --- | --- | --- |
| Supply Chain Management Systems | May 9  2020 | |
| Group members:  Mohammed Taha Ayaz Merchant  Zain Younas  Muaaz Uzair | | Deakin University |

Table of Contents

[Supply Chain Systems (SCM) 2](#_Toc40005397)

[General Supply chain for products 2](#_Toc40005398)

[Strategies for Supply Chain 3](#_Toc40005399)

[Flows in Supply Chain 3](#_Toc40005400)

[SHARP'S BAKERY, BIRCHIP, VICTORIA 4](#_Toc40005401)

[Services 4](#_Toc40005402)

[Management System 4](#_Toc40005403)

[Organizations Generally Pursue two types of Supply Chain Management: 5](#_Toc40005404)

[Vertical Integration 5](#_Toc40005405)

[Horizontal Integration 5](#_Toc40005406)

[Scope of Cyber Security in Supply Chain 5](#_Toc40005407)

[SCM Security risk Assessment 6](#_Toc40005408)

[Risks and threats 6](#_Toc40005409)

[Facts and Figures 7](#_Toc40005410)

[Mitigation techniques 8](#_Toc40005411)

[Why securing SCMs is essential? 10](#_Toc40005412)

[How to secure SCMs? 10](#_Toc40005413)

[Auditing 10](#_Toc40005414)

[Training and promoting cybersecurity awareness 11](#_Toc40005415)

[Use of appropriate frameworks for SCMs 11](#_Toc40005416)

[Understand the supply chain ecosystem 11](#_Toc40005417)

[Top-Down Approach 11](#_Toc40005418)

[Bottom-up approach 12](#_Toc40005419)

[Review and reflections on findings 12](#_Toc40005420)

[References 13](#_Toc40005421)

# Supply Chain Systems (SCM)

A global chain uses to release goods and co-operation from raw stuff to clients within a directed stream of knowledge, real placement, and money. (TECH TURF, n.d.)

**A picture containing device

Description automatically generated**

# General Supply chain for products

There are mainly three entities for supply chain Producer, Supplier, and customer. Moreover, the four necessary supply-chain items which are as follows.

* Physical Supplies and assistance from the supplier to client
* Money from clients to the raw material suppliers
* Data backward and forward along with the connection
* Converse Flow of goods exchanged.

# Strategies for Supply Chain

* **Stable**

This supply chain strategy is appropriate for chains that are focus on performance, Effectiveness, and Price. They use simple connectivity Technologies for real-time data. **For Example,**spices manufacturing company uses scale production and dedicated capital assets.

* **Reactive**

Runs excellent when the chain acts to fulfills needs from trade partners to illustrate, with **example**, production of sports team attire for fans when the team wins and gets to the next stage more products needed. However, the losing team request implicitly disappears.

* **Efficient Reactive**

It concentrates on performance and value management on the total delivered value of finished goods. **For Example,**in supermarket chain distribution centers and manufacturers co-operate to place the goods in stores within shorter than 24 hours. (Process view of a Supply Chain, 2016)

# Flows in Supply Chain

* **Information Flow:**

In information, the flow includes invoices, sales literature, specifications, receipts, orders and rules, and regulations

* **Primary Cash Flow:**

In primary cash flow, it includes payments of products and supplies.

* **Primary Product Flow**

In primary product flow, it includes materials, components, supplies, services, and finished products.

* **Reverse Product Flow:**

Reverse product flow includes returns for repair, replacements, recycling, and Disposal.

A screenshot of a cell phone

Description automatically generated

# ****SHARP'S BAKERY, BIRCHIP, VICTORIA****

The supply pattern of this famous bakery consists of a variety of cakes and bread. The owner of the bakery Kevin Sharp is the one end of the supply chain. They have links with different commercial food distributors that provide components such as flour, cream, and sugar. The bakeshop utilizes those ingredients and makes a diversity of food items, and the owner is the retailer who sells those items to the customers. (Process view of a Supply Chain, 2016)

## ****Services****

The supply chain design was for production, but the co-operation industry has an accumulation chain too. Industry includes all organizations except agriculture and construction. **For Example,**electricity utility acquires goods, services, and supplies. Moreover, it assigns its assistance to home-clients, commercial-clients, and different conveniences.

## ****Management System****

It is the administration of the flow of assets and assistance, which involves transportation and storehouse of crude materials work-in-process records and total assets from the time of entry to the end of consumption. An outcome that reaches an end-user describes the collective struggle of various companies. Few groups have only given regard to what was arising within their firm, some did not, though the whole deal of activity is sequentially transported goods to the ultimate client. (tatia, n.d.)

# Organizations Generally Pursue two types of Supply Chain Management:

* **Vertical Integration**
* **Horizontal Integration**

## Vertical Integration

It is an arrangement in which that company owns the supply chain of the company. Usually, each member of the supply chain produces different products or market-specific services, and these products combine to satisfy the common need. The organizations which support vertical integration may arise from an entrepreneurial foundation. **For Example**, Ford company-owned steel factories, the fleet of ships, construction plants, and showrooms, they built and distributed ford cars. (TECH TURF, n.d.)

**Benefits:**

* Its primary benefit is control.
* No dependency for components or services
* The operation can be synchronized with other company functions.

## Horizontal Integration

Expansion of a company by getting a similar business in the related trade. It is contrastive with vertical integration, wherever the organization provides different items that are associated with one outcome. The industry may do this through in-house development, purchase, or consolidation. The method could lead to a monopoly if an organization caught the vast bulk of the business for that item. For example, a company that produces shampoo may add other brands to invite to a broader client base. The real-life case of horizontal integration is Unilever, which owns 400 brands. (TECH TURF, n.d.)

**Benefits:**

* They gain economics of range and expanse.
* Concentrate on a specific market so originated more expertise.
* Knows about their business strongly.

# Scope of Cyber Security in Supply Chain

Cybersecurity in the supply chain is a subset and concentrates on the management of cybersecurity requirements for technology operations, software, and networks.

Cybersecurity activities for reducing risks include buying only from trusted vendors and educating users about threats. (Cyber security risk in SCM, n.d.)

For example: recently, Lenovo notebooks introduce a software named as Super-fish. The software encrypts the user data and gets access to every website user open. The software is built-in in the Lenovo machines, so it neither can be detected by the end-user nor by the antivirus. In such a scenario, the company and the end-user both do not know about the threat, but hackers get benefits. So cybersecurity in the supply chain plays a vital role in making sure that the end-user and the company are both secure.

SCM Security risk Assessment A picture containing light

Description automatically generated

(Source – TGB Security)

In this portion we will cover the risks and threats associated with the Supply chain management of our case study IOT and smart cities. Afterwards the mitigation techniques will be discussed in order to make the project as secure and safe as possible.

## Risks and threats

There are many risks when talking about the Supply chain and they cover a vast territory. It is often said that, the more people involved in a process, the greater the risks and their sources become. Some main types of risks are as under (source - NIST, US department of commerce):

* The people involved in any of the processes, from service providers to people working in the environment who have privileged or any other access to the equipment.
* Lack of proper security policies by the lower tier vendors.
* Software/ hardware compromised by the third party.
* Vulnerabilities in the software of the product or in the system of the vendor.
* The copy of the hardware or hardware with back door
* The third-party data storages

Risks are not only confined to the above points, but they also result in several other factors including backdoors in the hardware resulting to malware attacks, account hijacking, targeted attacks, DDoS, other undisclosed vulnerabilities, SQL attacks and many more. Some information related to it is shown in the following image.

Description: A screenshot of a cell phone

Description automatically generated

# Facts and Figures

56 percent of the organizations faced a breached that was caused by their vendors and only 35 percent of the companies have list of all the vendors with whom they share their sensitive and important information - (Ponemon institute,2018).

Some other facts published in the RSA conference 2016 by NIST services are as under:

* 80 percent of all the breaches are linked to the supply chain.
* 45% of all the breaches were attached with the past partners.
* 72% of companies do not have full visibility in their supply chain.

# Mitigation techniques

In order to mitigate all the risks related to the supply chain of our case i.e. IOT and smart cities, we must take a proper plan to take measures. The main points in this regard are:

* Know the environment of the supply chain
* Understand the risk
* Manage the supply chain risk
* Monitor the supply chain and its control

Knowledge of the system is the first thing to remove all the threats. We should know about how important our case is and how it can affect the other people. There are several tiers which are as under:

**Nationally Critical**. If the system affects the national security and functioning of the nation

Source – Australian cyber security center

**Nationally Sensitive**. If the system affects the national security but its impact is not significant.

**Critical**. A compromise of the system would have significant but localised impact to the security of many systems. This may include some smaller critical infrastructure.

**Sensitive**. The data of the system is of national importance but it effects are local.

**Locally Important**. The system is only important to the organization.

In our case, our system is **nationally sensitive** as it affects the national security but does not has significant impact on it. A smart city has a lot of vulnerable points due to a lot of factors including hardware, vendors, software and many other things.

The **interdependency** of the safe city is yet another thing. Servers will be connected to the security services offices and other national services which can pose a threat to them as well. Several gateways are needed to install to restrict the direct access to other data servers.

The **lifespan** of the devices installed will be very long as it wills a one-time investment making it easy for the attackers to penetrate in the system.

Understanding the supply chain**.** We should be aware of the lifecycle of our products. The **Vendors** should be monitored as they can introduce a vulnerability intentionally or unintentionally.

During the **delivery and deployment** phase of the products used in the smart city, measurements should be taken to avoid any tampering, installation of malicious code in the product. We should also see for the technical issues in the devices and the **interference risk**. Vendor can always be influenced by some other party.

The cybersecurity posture of the vendor is another thing to consider. Asking for evidence of compliance and auditing the vendor to check on the policies implemented must be done. If there is a sub-contractor involved, it is to make sure that that he does comply with the policies.

Managing the supply chain.we can always avoid the risk by the re-architecture approach. For example, if there is a need of installing any software in the system, call for the person with the security clearance rather than inviting some vendor’s random guy who can pose a threat to the system. If there is a need to call someone, all the aspects of possible risks must be considered. Moreover, adding additional controls for the services can also provide significant security.

Monitoring the supply chain. The monitoring and control is the most important part in these steps. We should always keep a record and maintain a proper document for every step. We must keep a review of every critical system and check on them every now a then. With every passing day there are new ways and methods coming in the market. Keeping system up to date is a necessary step. Ensure that there is a SOC (security operation center) to keep an eye on everything and it knows about all the devices and system in the environment. Incident reporting should also be done for every attack or incident happening.

Other Things to consider. Some other things to consider are:

**Awareness.** Always promote awareness in the people working with your systems. Most of the time it is the unintentional human error leading to the loss of data or a breach**.**

**Training.** Provide training to the employees in order to keep them up to date with the technology and the loopholes in it. It can have a significant effect in decreasing the threats and risks.

# Why securing SCMs is essential?

Cybersecurity poses a significant threat to the supply chain, as any organization can be affected by the intrusion in their supply chain system. For instance, a retailer might have its consumer's data compromised by an attack on the supplier. Cyber intrusions from outsourced providers can have a significant impact on the overall financial performance and its shareholder's values (Modi, Wiles, & Mishra, 2015). However, it doesn't necessarily mean a targeted attack but can emerge from any point in the supply chain system. Firms like Target, T-Mobile, Fiat, and many others who had faced cyber-attacks due to third party providers.

Moreover, with the rise of emerging technologies such as Artificial intelligence, IoT (Internet Of things), eCommerce, and smart home automation has led to increased chances for the likelihood of cyber-attacks. There can be significant damage to a firm's financial performance (Modi et al., 2015) which can be related by a practical example such as Target, who suffered a data breach in 2013 leading to a significant financial impact of $200 million (Ramakrishnan & Bose, 2017).

The IoT ecosystem is facing severe threats from cyber attackers due to several factors such as low cost and multiple pathways to attack. Some of the large scale cyber-attacks such as the Mirai botnet had exploited several vulnerabilities in the IoT system. Since the IoT system follows a decentralized platform for firms to deploy its services, it has led to increased participation for attackers to infiltrate multiple endpoints of the system consequently, making it crucial to secure the IoT supply chain.

# How to secure SCMs?

Securing supply chain systems has become increasingly essential due to their complexity in collecting data and information. The enhanced interconnectedness of supply chains makes it advantageous for hackers to intrude the system, augmenting the importance of data handling and storage. Also, there are some ways to promote the security of supply chain systems can be improved.

## Auditing

Auditing tends to be an effective and essential strategy of any firm that aims to identify security vulnerabilities. Applying auditing procedures to supply chain systems will help to define whether the preventive measures are adequate for disastrous cyber breach circumstances. The primary objective of an audit is to implement the right security steps to prevent malicious leakages in the system. Auditing is a process that can be initiated after something actions have taken place (Almadhoob & Valverde, 2014), that is categorized under being a preventive measure.

## Training and promoting cybersecurity awareness

With the rise of cyber-attacks, preventing supplying chain attacks doesn't only take into account technology, but it's a people, process, and knowledge problem(NIST, n.d.). Data breaches tend to be higher from human error than the mechanism utilized. IT systems won't be entirely secure unless the employees are trained and made aware of the frequent cybersecurity attacks and practices throughout the supply chain. Providing employees with sufficient training on how to check for suspicious emails that contain malicious links or downloading unauthorized software (EDS, 2020) is a critical factor in promoting awareness. Most of the attacks are transmitted through freeware, tricking users into installing the bogus software and infecting the supply chain system, thus leading to data compromise.

## Use of appropriate frameworks for SCMs

A research paper illustrated the importance of the objective and the functionality of specific structures (Wiesmann A. et al. eds., 2005). For instance, COBIT is a risk-management based framework categorized as an IT governance framework consisting of 4 main domains that ensure effective planning, organization, implementing, and monitoring the cyber risks. This framework aligns business objectives with the competency to achieve maximum security concerns, ensuring there is management as well as maximum security controls. COBIT provides the necessary steps on how to manage security with the customer. By using such frameworks mitigates the risk of a cyber-attack against the supply chain management system

## Understand the supply chain ecosystem

With the extremely challenging IOT environment, it is imperative to mitigate and control the supply chain concentrated risks associated with it. Due to the decentralized nature of the IoT ecosystem, the problem of securing the IoT supply chain can be followed through two approaches that are as follows.

### Top-Down Approach

The approach focuses on imposing security measures on each individual across the IoT infrastructure. Policies and regulations can be introduced that bans certain supply chain actors from making use of technology due to getting involved in malicious practices or imposing testing standards to specific suppliers based on their level of trust and reliability. Moreover, once these policies are in place, this would improve awareness across employees for the reliable procurement of suppliers and the risks involved in selecting the unethical suppliers. The primary purpose of such an approach is to increase awareness of having a centralized system to secure the IoT system and as a result, would lead to the strengthening of the supply chain management system

### Bottom-up approach

This approach focuses on the IoT ecosystem first and then spearheads towards establishing policies to control the risks. By analyzing the entire infrastructure would give the overall view of the threat landscape, source of cyber intrusions, supply chain actors involved, and many other parameters that constitute the global mapping environment. For individual home users, platforms might not be required to get a comprehensive analysis of the IoT environment. Still, large scale organizations that have many actors involved would require such tools to map. Finally, policies can be developed and enforced on firms. For instance, the Australia Department of home affairs has stated such guidelines and principles on how to secure IoT systems (ACSS, n.d.).

# Review and reflections on findings

The primary objective of this report was to create awareness of how necessary is it to apply cybersecurity measures related to supply chain management systems. The report explored the different aspects of SCMs that include the environment, process flows, risk assessments, and the recommendations required in securing this system. However, the report also highlights the importance of using an appropriate framework for aligning business objectives with cybersecurity.

The report findings implicate the use of such structures where firms can enjoy the full benefits of mitigating cyber-attacks on SCMS. This study also promotes awareness of cybersecurity, as stated by (NIST n.d.) says that supply chain attacks not only contribute to the utilization of technology but it's people, processes, and knowledge problems. The present literature has also emphasized the use of freeware, which is a source for transmitting malware into systems and networks.

# References

* Ramakrishnan, S., & Bose, N. (2017). Target in $18.5 million multi-state settlement over data breach. Last modified January 10, 2019. <https://www.reuters.com/article/us-target-cyber-settlement/target-in-18-5-million-multi-statesettlement-over-data-breach-idUSKBN18J2GH>
* DIST (Department of Industry, Science and Tourism) (1998), Stats Electronic Commerce in Australia, Commonwealth of Australia, Canberra.
* Best Practices in Cyber Supply Chain Risk Management Conference Materials Cyber Supply Chain Best Practices. (n.d.). [online] Available at: <https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf>.
* Evans Distribution Systems. (2020). Cybersecurity in Logistics: How to Protect Your Supply Chain from Cyber-Attacks. [online] Available at: https://www.evansdist.com/cybersecurity-in-logistics/ [Accessed 8 May 2020].
* Simon, J & Omar, A n.d., ‘Cybersecurity investments in the supply chain: Coordination and a strategic attacker’, EUROPEAN JOURNAL OF OPERATIONAL RESEARCH, vol. 282, no. 1, pp. 161–171, viewed 8 May 2020, <http://search.ebscohost.com/login.aspx?direct=true&db=edswsc&AN=000509816100011&authtype=sso&custid=deakin&site=eds-live&scope=site>
* Wiesmann A. et al. eds. (2005) A Guide to Building Secure Web Applications and Web Services, 2.0 Black Hat Edition,FreeSoftwareFoundation.[Online]Available:https://www.owasp.org/index.php/Category:OWASP\_Guide\_Project (Accessed: 9th May 2020)
* Securing the Internet of Things for Consumers. (n.d.). [online] Available at: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf [Accessed 9 May 2020].
* Yang, K, Forte, D & Tehranipoor, M n.d., ‘ReSC: An RFID-Enabled Solution for Defending IoT Supply Chain’, ACM TRANSACTIONS ON DESIGN AUTOMATION OF ELECTRONIC SYSTEMS, vol. 23, no. 3, viewed 9 May 2020, <http://search.ebscohost.com/login.aspx?direct=true&db=edswsc&AN=000433485200003&authtype=sso&custid=deakin&site=eds-live&scope=site>
* *TECH TURF*. (n.d.). Retrieved from https://tech-turf.com/introduction-supply-chain-its-management/(2016). *Process view of a Supply Chain.* Hassan Basodan.
* *Cyber security risk in SCM*. (n.d.). Retrieved from https://resources.infosecinstitute.com/cyber-security-in-supply-chain-management-part-1/#gref
* tatia. (n.d.). *TermPaper*. Retrieved from <https://www.termpaperwarehouse.com/essay-on/What-Is-The-Right-Supply-Chain/335749>
* <https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf>
* <https://medium.com/@KodiakRating/the-cyber-security-of-supply-chains-whos-the-real-risk-man-or-machine-ecdcc365d49d>
* <https://www.cyber.gov.au/publications/cyber-supply-chain-risk-management>
* <https://www.cyber.gov.au/publications/cyber-supply-chain-risk-management-practitioner-guide>