Project #5: Supply Chain Risk Analysis

[Name of the Writer]

[Name of the Institution]

Project #5: Supply Chain Risk Analysis

**Introduction**

 A supply chain attack is a third-party attack when someone infiltrates within the boundaries of your system through an outsider or an inside partner who may have access to all the firm's systems databases that contain some confidential information, and private information. They are also termed as the Cyber attacks and Data breaches) This has provided a subtle increase in the hypothetical of the enterprise in the past, because, as the numbers of the suppliers and service providers are gaining access to the sensitive data of the films, the potential risks are at higher wages (Maria Korolov, 2019). The potential risks include

 A lack of visibility in the tracking of the sensitive components

The absence of the integration hardly fills the gap between the cyber-security and the accountability

 A control limitation in the protection of the raw data and a keen eye on the significant transactions between the manufacturers and the suppliers.

 Other minute risk factors are country of origin, shipment and delivery accuracy, internal processes and the social and environmental possibilities.

 However, the risks associated with the supply chain are increasing due to the creation of new types of attacks, awareness among the general public, and a raised in the oversight from the regulating committees. Due to which, the professional Cyber attacks are using the resources and the new methods. A significant supply attack and the breach was done by the LAX security, for the HVAC Vendor. To avoid these severe consequences, it is must to have an updated cybersecurity system to eradicate the supply chain risks among the products and the services that are being offered by the firm. (Nate Kube, 2019)

 As the chain suppliers are becoming more discreet on technology and relying on Information Technology dependent technologies, they are at a higher risk of the supply chain disruptions. These risks include through mobile communication, robotics, cloud computing, and manufacturing the efficient digitalization processes. The sources from which the attacks can mainly occur are the website builders, third-party software providers, data aggregators, and water hole attacks. A better framework applies to the standards of the International Standard Organization are good practice for security.

**Discussion**

 The risk can occur anywhere from supplying the product or service to the customer regarding managing the delivery on time and the high-quality. With time, this is getting more and more complex because of the advances in the technology and their manipulations. However, not just the only one business, but they are affecting a variety of stakeholders, which are consumers (customers), the retailers, the logistics and the producers. External risk can be driven as a primary factor on the negative influence on the business. This highlights not only the political situation but the gratifying gratitude of a political landscape. This has a major impact on the financial markets of any country that might be going through this. (Cathy Johnson, 2019)

 The raw materials purchasing and the arranging commodities are done either by banks or the financial institutions. The transparency from where the products are sourced from, under the conditions in which it was produced. This can lead the company to involvement in the direct risk which can cause a problem for any of the institutions involved.

The other risks that are involved in the supply chain are

* + - Any network or computer hardware which had a malware installed on

it, and was delivered to the customer. For Example, the delivery of the notebooks with a superfish installed on it).

* + - Malware that is inserted aftermarket into the software or hardware can be crucial to the damaging arithmetics of the cybersecurity.
		- Vulnerabilities in the software applications and the networks that are found within the chain that can be discovered by the malicious hackers. (Security Ninja, 2015)

**Due Diligence:**

It was recently reported that CIOs and hackers are trying to discover that what would be the quickest pathway to go through a firm’s classified data. The method idealized was going through a vendor, the third party involved in all of this. The due diligence comes along with a thrashing of the vendors and tries the monitoring of those, third-party systems in real life. The negligence of the due diligence can cause potential and unintended harm to the company. Hackers which stole a total of 40 million in credit and debit card from the Target Corp. during the holiday season, broke into the company's network through stealing credentials from a company’s heating and air conditioning contractor. The companies with a large interconnected, structure of networks, face a lot of things when dealing with their suppliers every day. The due diligence proves it is a must for as it is involved in the assessment vetting of the new vendors. In situations like this, the third party due diligence, which follows the cascade of the high-level process is a necessity. The complexity of the third-party networks should have an effective strategy for the evaluation of the third-party risk in the involvement through the third party relationships or any other involved. The process comprises nine steps which are

1. Understand the concerns of the Compliance
2. Define the objectives of your corporation
3. Gather the key information that is to be highly needed
4. Validation of the Information
5. Conduct a Risk Assessment
6. Screen Prospects
7. Audit of the Process
8. Create a Monitoring Plan for the whole Process
9. Review the Process Regularly (Lexi Nexis, 2019)

**Practices for Managing the Global Chain Supply Management in the Cybersecurity and their benefits:**

 For the outbreaks in the cybersecurity of the network in the supply chain, also, the network attacks. This will substantially save your company, and the structured documentation can increase the companies supply chain from the inside out. For the possibility of obtaining and ensuring a higher number of value, following are the best practices for managing the Supply Chain Risk in the Biloh

 ***Assess your Readiness:***

Before the start of every plan, it is essential for us to have a great system for their proper and objective. For the best way to visualize your standing with your Cybersecurity risks on the supply chain, hire a 3rd party which should assess the vulnerability and penetration. Because nothing is stopping these digital experts. They will hack into your systems and penetrate the firewall, looking for the loopholes of your digital security. Hence, this will beneficially evaluate the security of your company from another perspective.

 ***Evaluation of the Risks before Mitigation:***

After the passing of the vulnerabilities, a list may focus on some other multiple systems. This doesn’t mean that you have to perform a replacement of your whole infrastructure. Instead, you need to sit back and make sure to act upon the amendments that are needed for the recommended size of the organization. Be careful in handing out the information like credit cards, financial information, or personal data of the customers which in turn increases the grip for each issue and prioritize that in the case of any damage, fixes will be provided.

 ***Designing your operations to act coherently with the Security Policies:***

 After closing up the holes, and making sure that all the house is clearly in order. After getting in the first order, your house can have the most penetrable structure which can be potential viral and harmful for your security barriers and company digital systems. For this, schedule a frequent training session, and create regular reminders for these.

 ***Extend Security Guidelines to your Vendors:***

Sharing data with your suppliers can help them easily pass the security barriers which can be down for your operations. Through this, they will have open access to your internal systems. In case, vendors are not in the place; hackers can essentially substitute their name, attack your company and stole your company's confidential data.

 ***Test and Repeat:***

The security and precautionary measures are not just a one time play, but instead, it needs to be focused in repetitions. As the cybercriminals are motivated and creative, they can easily penetrate the defense system anytime. A renewal through repeating these practices will help in this gradually. (Ed Gort, 2019)

**Conclusions**

 The supply chain attack is the data breach into the personal, confidential and files which can be used by the Cyber hackers and the Cybercriminals for their potential use. This can be caused by some risk factors which involve the installation of either a built-in or aftermarket malware into the software or the hardware of a system which potentially damages the working and easily let hackers hack into the data. Due diligence which checks up on the vendor, as well as the certain aspects of the company's system for their cybersecurity, can apprehend the potential threat to the system. Certain practices are involved, which can substantially decrease the spontaneous infiltration of the cyberhackers into the system. These include assess your readiness, evaluation of the risks before mitigation, Designing your operations to act coherently with the security policies, extend security guidelines to your vendors, and test and repeat.

**References**

Korolov, M. (2019). What is a supply chain attack? Why you should be wary of third-party providers. CSO Online. Retrieved 21 January 2019, from <https://www.csoonline.com/article/3191947/data-breach/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html>

Cyber Security Risks in Industrial Supply Chains | SecurityWeek.Com. (2019). Securityweek.com. Retrieved 21 January 2019, from <https://www.securityweek.com/cyber-security-risks-industrial-supply-chains>

Different Types of Risk in Your Supply Chain, and How to Avoid Them | The European Business Review. (2017). Europeanbusinessreview.com. Retrieved 21 January 2019, from <http://www.europeanbusinessreview.com/types-risk-supply-chain-avoid/>

Cyber Security Risk in Supply Chain Management: Part 1. (2015). InfoSec Resources. Retrieved 21 January 2019, from <https://resources.infosecinstitute.com/cyber-security-in-supply-chain-management-part-1/#gref>

9 Steps to Effective Supplier Due Diligence - Risk Management Guide. (2019). Lexisnexis.com. Retrieved 21 January 2019, from <https://www.lexisnexis.com/en-us/products/lexis-diligence/ctr/9-steps-to-effective-third-party-due-diligence.page>

Review, C. (2019). 5 Cybersecurity Best Practices for your Supply Chain Ecosystem. CIOReview. Retrieved 21 January 2019, from <https://supply-chain.cioreview.com/cxoinsight/5-cybersecurity-best-practices-for-your-supply-chain-ecosystem-nid-14195-cid-78.html>