Cyber Security Threats in Supply Chain and its Solutions

– **Nishtha Agarwal**
Research Scholar, IIFT, nishtha_phdmf19@iift.edu

There is no denying of the fact that ICT has been helping organizations in improving their business processes. One such business process is that of supply chain management. Use of ICT in supply chains has been influential in increasing efficiencies, agility, flexibility, transparency and hence profits. However, this transparency is accompanied by several negative consequences- one of it being cyber security. Organisations usually have perimeter defense mindset but the most dangerous attacks come from within the system. This article discusses some of the cyber security threats that may originate from within the supply chain and then goes on to classify them on the risk impact vs. probability matrix. Lastly some solutions, based on the global best practices, have been given to counter-attack these threats.

Introduction

As we near to the end of the second decade of the 21st century, we find more and more organizations realizing the importance of digitization of their supply chains making them more connected, smart and efficient. Traditionally, these supply chains were a series of discrete, siloed steps taken through marketing, product development, manufacturing, distribution and then finally into the hands of the customer. Digitization has brought these walls down making it a complete integrated ecosystem that is end to end transparent (PwC, 2019). This has been done by establishing electronic linkages amongst purchasing activities and order management, customer and supplier relation management, inventory monitoring and forecasting, manufacturing control and management etc. However, with increased transparency come great risks. These linkages, established by means of ICT, can be compromised to jeopardize the entire supply chains. For example an unauthorized intrusion in the information layer of an oil supply chain could cause a black out of the ordering system and the consequent temporary stoppage of delivery of oil. Consequences could be serious if this unauthorized access manipulates or replicates the production of food or pharmaceutical supplies (Urciuoli, Männistö, Hintsa, & Khan, 2013). The problem becomes even graver with most managers denying cyber security as an issue in itself (livemint, 2019). This article hence tries to become a wake-up call for such managers by delving into the various kinds of cyber-crime risk that may impact a supply chain with latter half of the article classifying these risks and providing solutions thereafter by analyzing the global best practices. The article has been written post extensive review of journal articles, news about global supply chains and informal conversations with experts.

Cyber Threats Lurking in the Supply Chain

A vast majority of supply chains approach cyber security from a perimeter defense mindset wherein the focus is on hackers and other bad actors that shouldn't be able to access the systems (MIT Management Sloan School, 2019).

However, organisations often fail to consider attack vectors originating intentionally or unintentionally- with outside individuals, contractors, firms or groups that are authorized to access those systems. The severity of this aspect can be gauged from the fact that these are parties belonging to the supply chain and once these have slid in then all those perimeter defenses are next to useless. Madnick, the founding director of Cyber security (Interdisciplinary Consortium for Improving Critical Infrastructure) at MIT Sloan pointed that these attacks come in the following forms:

1. Software service Providers and outside contractors-An instance that brought the entire operations to halt was when a smaller company, that made crucial software for a global firm, was affected by a ransom ware which hijacked its servers and used it as a beachhead to get into the clients network. The results were devastating for firms across the globe whose shipments were delayed. This kind of exploitation of smaller and typically less secure companies who have access to credentials of larger corporations is becoming increasingly common which supply chain managers should be aware of.

2. Mergers and acquisitions- another potential point of complication in the supply chain of a company is when they acquire a smaller organization. It has been found in a survey that almost 40% of organizations discover a cyber-security problem during the post-acquisition integration of the acquired company. The most famous one being when Verizon discovered a prior data breach at Yahoo! after the execution of acquisition deal (Forbes, 2019). Checking any prior data breach in the to-be acquired company is important as it not only changes the valuation but also prevents any further attack on the combined entity.

3. Physical Components- In 2014, Lenovo a major laptop maker sold laptops with pre-loaded software called Visual Discovery in order to deliver pop up advertisements and blocked browsers from warning users when they tried to access malicious websites. A vulnerability called Man-in-the-Middle (MITM) was identified in this software which couldn't be caught by antivirus because it was default software (Infosec). This point to the supply chain managers that it is important to take each and every component of the supply chain into considerations. Besides this, any authorized personnel may bring an infected physical device which may be harmful for the system

4. Network Services- Since the data in the network chooses the fastest path; chances are that the data could be routed to a hub where malicious actors could get their hands on it. If the data is routed through such routes then chances are that these actors might compromise the data.

5. With Internet of Things (IoT) devices emerging as an important functionality to improve the supply chain efficiencies, any device connected to the internet can pose a cyber-security risk. But, by incorporating cyber security into the design from the beginning, one can end up with more secure and higher quality products.

Supply Chain Cyber Security Risk Classification

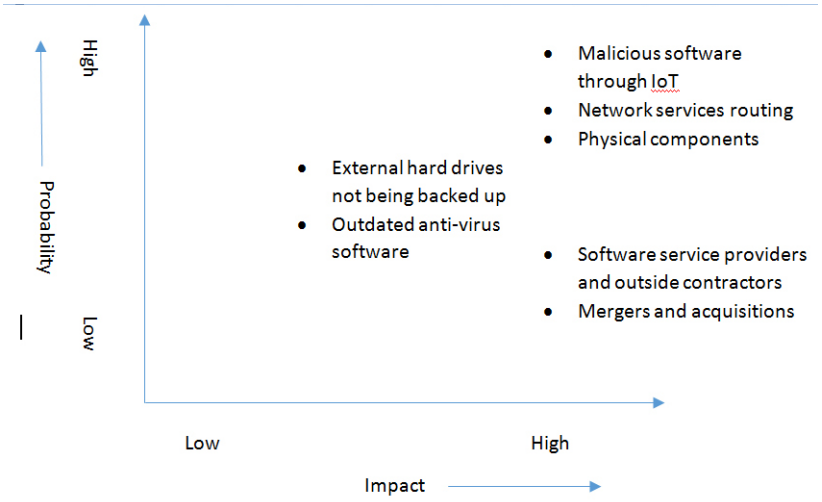
With increasing attack surface, it is important for supply chain managers to assess these risks and act on them accordingly. For assessing the risk, a popular impact- probability matrix can be developed for the various kinds of cyber security risks that an organization faces. This matrix classifies the risks into four quadrants namely low impact-low probability risks, low impact-high probability risks, high impact-low probability risks and high impact-high probability risks. The matrix is given as follows with classification of above mentioned risks into the matrix.

Global Best Practices In Managing A Cyber-Secured Supply Chain

As may be seen from the above figure, the cyber security risks in a supply chain have been classified into four categories based on their probability of occurrence and their impact. It can be clearly noted that the cyber security risks poses medium-high negative impact to an organization. These risks cannot be managed only by IT tools but by coordinated management of supply chain management, quality and production assurance standards, manufacturing process standards (Pal & Alam, 2017) etc. Following are some of the global best practices:

1. National Institute of Standards and Technology (NIST) frameworks- NIST framework is a tool comprising of Identify, Protect, Detect, Respond and Recover which helps in analyzing the possible risks and prepares and appropriate path towards a risk free environment in a neutral manner. 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

2. Open Trusted Technology Provider Standard- O-TTPS



has been recognized by ISO (International Standards Organization) and International Electro Technical Commission (IEC). 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.

3. Center for the protection of national infrastructure (CPNI), UK government- CPNI issues advisories to organizations, public or private, to implement a risk mitigation plan. The major steps of the plan includes:

    a. 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

    b. Assurance of suppliers

    c. Due diligence

    d. Accreditation

    e. Appropriate and proportionate measures to mitigate the risk

    f. Audit arrangements of the system

    g. Compliance of the security measures in the SCM system

4. Huawei's approach to tackle supply chain risks- Huawei has also developed an ISO 28000 standard supplier management system. This supplier management system identifies and controls the security risks during the end-to-end process from the point of incoming of the materials to delivery of the product. Huawei, then, 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.

Conclusion

It is not denying the fact that in a fully digitized supply chain, any faulty component may cause a serious damage in terms of loss of business, loss of goodwill, disclosing secret information etc. The severity of the situation increases multifold because of denial of these issues by supply chain managers. Such managers, when faced with a breach, tackle it in an ad-hoc manner which makes it difficult for the organizations to recover. The correct manner is the one in which there is continuous process improvement of all policies, practices, rules guidelines that are in place. To this end, it is first important to analyze the cyber security risks and classify in the risk impact vs probability matrix. It is important here to note that risks having high probability and impact should have proper risk mitigation measures in place. On the other hand, the risks having low impact high probability and low impact and low probability should be tackled during the daily operations. These risks include weak passwords, regular checking of firewalls, security patches etc. The high impact-low probability risks are the ones which require organizations to build resilience against them through proper control mechanisms, infrastructure and culture.

References

- American Shipper. (2019, September). *'Cyber Deniers' are a threat to cyber security*. Retrieved from American Shipper: https://www.freightwaves.com/news/cyber-deniers-are-a-threat-to-supply-chain-security
- Forbes. (2019, November). *Data Privacy And Cybersecurity Issues In Mergers And Acquisitions*. Retrieved from Forbes: https://www.forbes.com/sites/allbusiness/2018/11/11/data-privacy-cybersecurity-mergers-and-acquisitions/#7852e60772ba
- Infosec. (n.d.). *Cyber Security Risk in Supply Chain Management: Part 1*. Retrieved from Infosec: https://resources.infosecinstitute.com/cyber-security-in-supply-chain-management-part-1/#gref
- livemint. (2019, September). *Only 24% of Indian IT managers see supply chain as a top security risk: Report*. Retrieved from livemint: https://www.livemint.com/technology/tech-news/only-24-of-indian-it-managers-see-supply-chain-as-a-top-security-risk-report-1568101261948.html
- MIT Management Sloan School. (2019, February). *These are the cyberthreats lurking in your supply chain*. Retrieved from Ideas Made to Matter:Cyber security: https://mitsloan.mit.edu/ideas-made-to-matter/these-are-cyberthreats-lurking-your-supply-chain
- Pal, O., & Alam, B. (2017). Cyber Security Risks and Challenges in Supply Chain. *International Journal of Advanced Research in Computer Science* , 662-666.
- PwC. (2019). *How digitisation makes the supply chains more efficient, agile and customer-focused.* Munich: PwC.
- Urciuoli, L., Männistö, T., Hintsa, J., & Khan, T. (2013). Supply Chain Cyber Security – Potential Threats. *Information & Security: An International Journal* , 51-68.

Nishtha Agarwal is Research Scholar at Indian Institute of Foreign Trade (IIFT), New Delhi, Area of Research: Operations and Supply Chain Management.

nishtha_phdmf19@iift.edu