Supply Chain Cybersecurity: Risks, Challenges, and Strategies for a Globalized World springer

Comment [lm1]: Review the abstract so that it contains the subject of the research, the methodology used and the main conclusions.

Abstract:

As the world grows more interconnected, firms increasingly rely on broad supply chains to conduct business. However, monitoring the supply chain and the risks connected with it is a process that is time-consuming and expensive for many organizations. In many instances, businesses that do not appropriately manage the risks associated with their supply chain are more likely to become victims of a cyberattack, which has the potential to cause significant disruptions in their operations. In this article, we will take a more in-depth look at supply chain risk management, the dangers that are most commonly associated with it, as well as the five actions that your company can take toward worry-free supply chain risk management.

1. Introduction:

The concept of "Supply Chain" refers to the integration of physical and technological systems across networks. This integration enables enhanced production, organization, and profitability. The key characteristics of a supply chain include autonomous actions that are not dependent on location, extensive integration, a range of automated services, and the ability to respond to customers' needs and requirements in a contextual manner(1). The phrase "intelligent supply chain systems" was introduced in conjunction with the advent of Industry systems, primarily to refer to the fourth industrial revolution and the incorporation of intelligent systems into supply chain operations(2). These systems provide support to both the industry and military sectors by facilitating production and manufacturing processes(3). They place particular emphasis on the exchange of models and information within worldwide networks, while also ensuring their secure management. Supply chains play a crucial role in businesses by facilitating the fulfillment of essential procedures and logistical needs. Within the realm of military operations, supply chains serve a purpose that extends beyond just profit-driven objectives. Instead, they possess the

potential to yield significant outcomes that are crucial to the success of missions and the preservation of human life. Contemporary society has developed a fundamental reliance on computer networks facilitated by industrial systems, which are crucial for various digital activities in daily life. Consequently, this dependence exposes society to potential cyber vulnerabilities, particularly when these systems are infiltrated by intricate cyber or physical hacking methods(4-7).

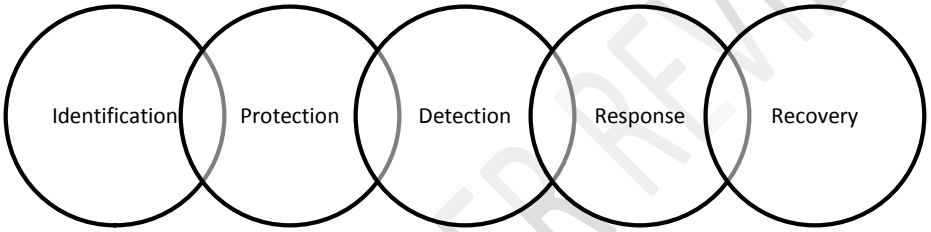

Figure 1 overview of cybersecurity

The field of research pertaining to the advancement and mitigation of cyber-attacks is a subject of international significance(8). The capacities of both country states and non-nation states are consistently expanding and improving. Simultaneously, supply networks are experiencing a growing trend towards enhanced efficiency, interconnectivity, and digitalization. The correlation between supply chains that are facilitated by digital technology and the escalating militarization of the cyber domain is a research area of considerable importance. The growing reliance on computing and communications infrastructures is causing significant transformations in the functioning and integration of supply chain processes. The potential ramifications of exploiting a weakness inside a military supply chain extend beyond economic implications, posing a significant risk to human life(9, 10). With the extensive acquisition of defense products The worldwide offensive surface for malicious actors has expanded, leading to the possibility of

amplifying the negative consequences resulting from a cyber-attack on supply chain systems(11, 12).

Comment [lm2]: review the figures in order to cite the reference source.

Figure 2how cyberattack starts

The fundamental principles of the global supply chain are increasingly reliant on the utilization of the internet and network connectivity(13, 14). The presence of this interdependence has significant implications for the security and efficacy of these systems. The significance of global supply chains is being reinforced and their vulnerability as a possible target is becoming implicated due to many factors such as shifts in the operational environment, advancements in technology, and changes in the maintenance of systems and platforms. Supply chain risk refers to the abrupt probability that influences the macro- or micro-level aspects of supply chain processes, resulting in consequences for several components of supply chain operations, including Information Technology (IT) and Operational Technology (OT)(15, 16). Risk management is a crucial process that involves the prediction and assessment of cyber hazards in order to identify and mitigate potential risk occurrences, hence reducing their impact. This approach would prove beneficial in elucidating the cyber dangers that supply chains encounter. The classification of supply chain risks encompasses two methodological categories, namely interruption and operation(17). The risk of disruption arises from natural calamities, such as seismic events or inundation, and addressing this form of risk is not a straightforward task.

Operational risk encompasses various factors, including cyber-attacks, that pertain to the ineffective execution of supply and demand operations throughout the production or delivery of finished products(18, 19).

The standardization of supply chain operations and the mitigation of mission successes can be facilitated through the creation of mission assurance, agile life-cycle engineering, and risk management methods. Furthermore, it effectively facilitates the implementation of emerging technologies such as blockchain, the Internet of Things (IoT), applications of Artificial Intelligence (AI), and Cyber-Physical Systems (CPS). These technologies enable the provision of automated and secure services to organizations, thereby enhancing the productivity and adaptability of supply chain operations(20, 21). The potential impact of mission assurance models on the response strategies of militaries and defense organizations towards Advanced Persistent Threats (APT) may be significant. The utilization of several concepts, including crown jewel analysis, business continuity methodology, ontological-based semantic models, service orchestration systems, and the enhancement of redundant and degenerate systems or processes, can contribute to the attainment of heightened mission assurance within organizational settings. The impact of the technical environment on military operations and the potential consequences of innovation within this domain can significantly influence the efficiency and efficacy of military supply chain operations. Consequently, defense businesses are facing a growing imperative to possess the capability to evaluate the potential effects of emerging technologies on their supply chains, enabling them to effectively incorporate or reduce any associated risks(22-24).

2. What Is Supply Chain Risk Management?

Supply chains refer to the intricate networks that connect a corporation with its suppliers, upon which the company depends for the production and distribution of its products or services. The management of a supply chain encompasses the oversight of the movement of goods, encompassing the various procedures involved in converting the raw materials consumed by an organization into the final products or services offered by such firm(25, 26).

Supply chain management encompasses the strategic planning and efficient execution of many activities related to the acquisition, procurement, and transformation of raw materials, along with

the effective administration of logistical operations. One of the primary rationales behind the adoption of a global supply chain management strategy by firms is to enhance their competitive edge. The presence of supply chains can bring about numerous advantages; however, it is important to acknowledge that they can also elevate an organization's exposure to risks pertaining to quality, safety, business continuity, reputation, and cybersecurity(27, 28).

Following the emergence of the COVID-19 pandemic, there has been an increased focus on supply chains in the media, as the repercussions of supply chain disruptions have impacted ordinary customers globally. The pandemic has highlighted the inherent susceptibility of conventional supply systems to such disturbances. All organizations are susceptible to both internal and external risks that arise as a result of interruptions in their supply chains. The practice of mitigating the potential risks associated with such disruptions is commonly referred to as supply chain risk management (SCRM)(29, 30).

Supply chain risk management include the systematic identification, evaluation, prioritization, and mitigation of potential threats to the supply chain and the associated risks they provide. Third-party risk management (TPRM) constitutes a crucial element within the realm of supply chain risk management. Organizations across various industries commonly engage with external entities inside their supply chain, encompassing suppliers, vendors, contractors, or service providers. The inherent characteristics of these economic connections necessarily subject these firms to significant hazards(31, 32).

According to empirical research, the average number of suppliers with whom enterprises share their data is approximately 730. Among the firms that engage in data sharing with external entities, a notable 53 percent have encountered at least one instance of data breach attributable to a third party. These breaches have resulted in an average financial burden of almost $7.5 million(33, 34).

In addition to instances of data breaches, external risks within supply chains encompass various factors, such as the impact of unpredictable or misunderstood customer demand, disruptions in the movement of products including raw materials, components, and finished goods, as well as the occurrence of natural disasters like earthquakes, hurricanes, and tornadoes, among others.In addition, internal supply chain risks encompass various factors such as disruptions in internal

operations, alterations in key management, personnel, and business processes, non-adherence to environmental regulations or labor laws, inadequate cybersecurity policies and controls to safeguard against cyberattacks and data breaches, and other related concerns(35-37).

Regardless of perspective, the involvement of a company in the supply chain, especially through the practice of outsourcing to external entities, inherently introduces risks to the firm. The supply chain exposes businesses to several possible disruptions, including legal, compliance, financial, strategic, and reputational risks, which may not be encountered in other contexts. One of the most significant hazards that the supply chain presents to businesses is the cyber risk, which entails the potential occurrence of a cybersecurity event leading to the disruption of data and business activities(38, 39).

In light of the increasing reliance on third-party entities by organizations and the concurrent rise in cybersecurity incidents, it is imperative for organizations to develop and execute a comprehensive supply chain risk management strategy. This strategy is crucial in safeguarding the organization, its clientele, and any other business affiliations from potentially catastrophic cybersecurity risks associated with the supply chain(40-42).

3. What Are the Types of Cyber Risks in Supply Chain Management?

As previously said, cyber risk is a growing concern that supply chains provide to enterprises. Regrettably, a majority of firms operating inside the supply chain are bound to encounter disruptions in the form of data, financial, or operational challenges at some juncture. The impact of these disruptions on your business will depend on the effectiveness of your supply chain risk management plan. The increasing digitization of the corporate environment necessitates the utilization of various digital technologies such as the Internet of Things (IoT) and Industrial Internet of Things (IIoT) to enhance supply chain operations within enterprises. However, the advent of these novel technologies also renders firms vulnerable to emerging cybersecurity risks, including but not limited to malware, ransomware, phishing, and hacking.Data leaks, cybersecurity breaches, and malware and ransomware assaults are prevalent hazards that firms encounter within their supply chains in contemporary times. Subsequently, a more in-depth examination will be conducted on each of these cyber dangers, elucidating the potential detrimental impact they may have on your business(43-46).

3.1. Data Breaches

Data breaches represent a significant and grave cybersecurity peril encountered by contemporary enterprises. The probability of an increase in both the number and severity of these security incidents is high in the foreseeable future. When an organization has a data leak or data breach, it typically leads to substantial financial losses and reputational harm, alongside potential regulatory and legal ramifications. The average financial impact of a data breach in the year 2021 amounted to a substantial sum of $4.2 million(47-51).

Despite the presence of appropriate regulatory and compliance standards, organizations frequently encounter significant delays in detecting data breaches after their occurrence. Research suggests that the average duration for identifying a data breach is approximately 197 days. Moreover, the aforementioned figure tends to increase when firms have a data breach due to a supply chain security issue. According to a joint analysis by IBM and the Ponemon Institute, the average duration for a corporation to identify a third-party data breach is 280 days. The probability of a data breach or leakage increases proportionally with the extent to which sensitive data is shared with other parties within the supply chain. Sensitive data refers to information that necessitates safeguarding against unauthorized access in order to protect the privacy and security of individuals or organizations. The potential manifestations of this phenomenon encompass intellectual property as well as personally identifiable information (PII). Several prevalent data breaches caused by third-party vendors include unlawful access through company email accounts, hacking of email providers, absence of encryption, and insecure websites and incorrectly stored login information(52-54).

In certain instances, it is possible for third parties to intentionally disclose confidential customer information to external entities, thereby exposing your organization to potential supply chain attacks orchestrated by cybercriminals, hacktivists, and even rogue nation-states.

3.2. Cybersecurity Breaches

The breadth of this category is deliberate, as it encompasses a range of emerging technologies that expose enterprises to heightened susceptibility to assaults within their supply chains, in manners previously unexplored. In contemporary times, the utilization of internet-connected

devices engenders potential dangers within the supply chain. The Internet of Things (IoT) typically include consumer-oriented devices, such personal fitness trackers and smart thermostats. As of 2021, the global count of active IoT devices exceeded 10 billion(55, 56).

The term "IIoT" primarily pertains to the utilization of equipment for powering organizations on a significantly greater scale. The purpose of the Industrial Internet of Things (IIoT) is to enhance industrial processes by integrating various devices that are interconnected and capable of communication through the Internet. These devices range from sensors and scales to engines and elevators. These technologies facilitate the enhancement of organizational efficiencies, encompassing reduced time to market, improved asset monitoring across the supply chain, cost reductions, and the establishment of safer workplaces, among other benefits. Moreover, these technologies pose several cybersecurity vulnerabilities to the entities that employ them.Cybercriminals are aware of the suboptimal state of security in the realms of IoT and IIoT, rendering them more susceptible to cyberattacks. Based on statistical data on IoT-based attacks in 2019, it was observed that the average duration between the activation of an IoT device and the occurrence of an attack was approximately five minutes(57-59).

In the context of Industrial Internet of Things (IIoT) devices utilized in industrial systems, the ramifications of a cybersecurity breach can have far-reaching and severe implications. These include but are not limited to the following: disruption of production processes, financial repercussions, unauthorized access and theft of sensitive data, substantial harm to equipment, acts of industrial espionage, and potential physical injury to individuals. With the increasing proliferation of devices and sensors, there is a corresponding rise in the creation of additional communication channels, data storage facilities, ports, and endpoints. The expanded attack surface provides additional risks in the absence of protection for such endpoints(60-62).

3.3. Malware and Ransomware Attacks

The prevalence of malware and ransomware attacks is regrettably increasing. The primary objective of these attacks is to illicitly acquire information, manipulate internal data, or obliterate confidential information. Malware refers to a category of invasive software that has the capability to penetrate computer systems with the intention of causing harm, such as damaging

or destroying the systems, or extracting data from them. The prevalent forms of malware attacks encompass viruses, worms, Trojans, and ransomware(63, 64). The SolarWinds malware attack of 2020 stands out as a highly notable incident within the realm of previous malware assaults(65). In the first stages of the year, the systems of SolarWinds, a corporation headquartered in Texas, were compromised by cybercriminals who inserted malevolent code into the organization's software system known as Orion. This particular program was extensively employed by approximately 33,000 clients for the purpose of overseeing their information technology assets(66, 67).

In March 2020, SolarWinds distributed software upgrades to its clientele through the Orion platform, inadvertently containing the malevolent code that had been implanted by the hackers. Subsequently, the virus established a covert access point within the information technology infrastructure of SolarWinds' clientele, thereby enabling the malevolent actors to deploy more malware for the purpose of clandestine surveillance on those entities and corporations.Ransomware is a prevalent form of malicious software assault. This particular type of malicious software employs encryption techniques to secure the files of its targets, so enabling the perpetrator to demand financial compensation in return for a decryption key. In the majority of instances, the financial transaction including a decryption key for data recovery is conducted through the utilization of cryptocurrencies such as bitcoin, with the intention of concealing the identity of the perpetrators(68, 69).The year 2021 witnessed a ransomware attack targeting Colonial Pipeline, resulting in the temporary cessation of the company's activities for a number of days. Consequently, this incident precipitated a scarcity of gasoline throughout the southern region of the United States. The hackers initially obtained unauthorized access to Colonial's computer networks through a virtual private network (VPN) account, which was intended for distant employee access to the network. However, the virtual private network (VPN) did not implement multi-factor authentication as a requirement for access. Consequently, the attackers were able to infiltrate Colonial's network by utilizing a hacked username and password. It is highly probable that this login information was obtained through a data breach that revealed an employee's credentials(70, 71).

Ultimately, Colonial remunerated the cybercriminals a sum of $4.4 million as a quid pro quo for the provision of a decryption key to facilitate the retrieval of their compromised data.

Nevertheless, due to the sluggish performance of the decryption key, the organization was compelled to depend on its internal backup systems in order to reinstate the provision of services. Subsequently, Colonial Pipeline managed to recommence its activities; nonetheless, it incurred significant detrimental effects to its business, including various financial and reputational ramifications(72).

4. Supply Chain Risk Management Strategies to Help

In order to safeguard both your corporation and its clientele from the aforementioned cyber dangers, it is advisable for your company to adopt some best practices in supply chain risk management. Outlined below are several strategies that can be employed to enhance one's cybersecurity measures in order to mitigate the aforementioned cyber threats:

- The implementation of compliance rules for all third-party vendors, encompassing manufacturers, suppliers, and distributors, is vital.
- The establishment of precise user roles and the implementation of security measures to limit system access and determine the extent of clearance or privilege granted to individuals. The aforementioned concept is commonly referred to as the principle of least privilege.
- The process of establishing and recording data stewardship protocols, together with delineating data ownership and associated rights and permissions.
- Ensuring the provision of comprehensive security awareness training to all workers.
- Collaborating with vendors across the supply chain network to establish a cohesive disaster recovery strategy aimed at ensuring uninterrupted business operations.
- Implementing backup rules is crucial in order to ensure the protection and security of data backups.
- It is imperative to consistently update software solutions, such as antivirus, anti-spyware, and firewalls, in order to maintain optimal security measures. It is advisable to additionally explore more sophisticated cybersecurity strategies, such as DNS filtering and network access control.

- The use of a software solution, such as the Reciprocity ROAR platform, enables users to attain comprehensive visibility into the risks associated with their supply chain. This facilitates the prompt identification of potentially hazardous conduct or anomalous activities.

5. What Are the 5 Steps of Supply Chain Risk Management?

Having gained a more comprehensive comprehension of prevalent cyber hazards within the supply chain, it is now imperative to examine the measures that can be undertaken to effectively execute a supply chain risk management strategy that aligns with the specific needs of one's firm(73).

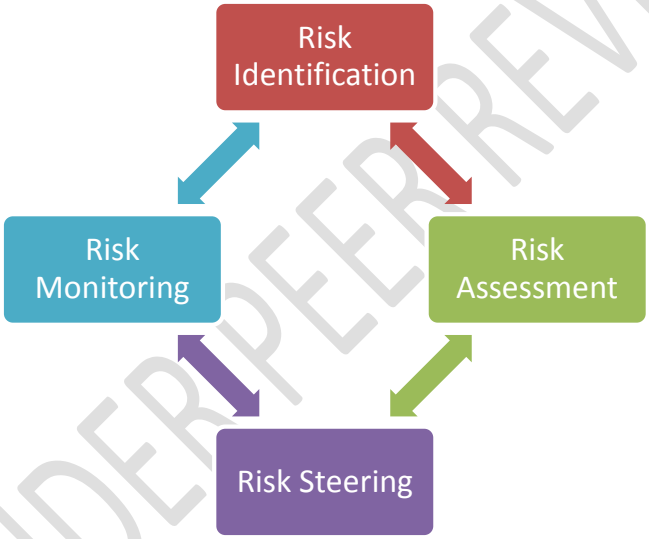

Figure 3overview

Comment [lm3]: review the figures in order to cite the reference source.

- **Step 1: Start with a Plan**

Like any risk management program, the initial phase involves ensuring the presence of suitable personnel to achieve success. It will be imperative to form a team of employees who possess the necessary skills and expertise to effectively identify, analyze, prioritize, and mitigate risks within the supply chain. Once the team has been assembled, commence the collaborative planning phase. The task at hand involves the delineation of distinct roles and duties for the members of

your team. Additionally, it requires the creation or incorporation of an established vendor risk management policy. Furthermore, it necessitates the determination of the approach to be used in drafting a comprehensive description of the procedures and processes to be employed for each stage within the plan for managing risks within the supply chain. Developing a comprehensive risk management plan is an effective approach to adequately equip both the team and the broader company in anticipation of the unavoidable risks that may arise across the supply chain. In the realm of cyber risk management, it is imperative to devote specific attention to the risks that have an impact on the cybersecurity of an organization, as well as the potential harm that these risks may inflict upon the organization's supply chain(74, 75).

In addition, it is imperative to develop appropriate metrics for assessing risk. The choice between employing qualitative measurements, such as a high/medium/low scale, or quantitative metrics, such as statistical analysis, is at your discretion. In conclusion, it is advisable to select a methodology that aligns most effectively with the specific requirements of your organization. Prior to commencing the subsequent phase, it is advisable to allocate a certain amount of time to consult pertinent frameworks that may offer guidance throughout the process. Fortunately, there exists a variety of risk management frameworks and approaches that can be utilized in the development or strengthening of a supply chain risk management program(76, 77).

To initiate the risk management process inside your business, it is advisable to refer to established frameworks such as the National Institute of Standards and Technology (NIST) and the International business for Standardization (ISO). These frameworks serve as illustrative models that can guide your firm in embarking on its own risk management endeavor(78, 79).

- **Step 2: Identify, Assess, and Prioritize Risks**

Prior to implementing risk mitigation strategies, it is essential to first ascertain the presence of the risk through identification processes. During the risk identification phase, it is recommended that the team actively engages in table-top activities to not only uncover known hazards but also to consider any potential concerns that may have been overlooked. One essential step in the process involves compiling a comprehensive inventory of the potential hazards inside your supply chain, so facilitating subsequent analysis and evaluation.It is advisable to seize this opportunity to conduct a thorough examination of the service level agreements (SLAs) pertaining

to each third-party association in order to ensure satisfactory performance by vendors and ascertain the compliance obligations applicable to your business. It is imperative for your organization to possess comprehensive knowledge regarding the regulations and standards that necessitate compliance, not only for your own operations but also for your third-party entities, ensuring continuous adherence(80, 81).

Subsequently, initiate the procedure of doing risk analysis. Commence the process by undertaking a comprehensive evaluation of supply chain risks, which can be accomplished internally or by engaging the services of an autonomous cybersecurity organization or expert. Conducting a risk assessment enables the evaluation of the identified hazards within the supply chain, facilitating the classification of contractors based on their associated risks and access levels.In essence, a comprehensive cybersecurity risk assessment should furnish an extensive examination of all cybersecurity threats, encompassing those that may arise from the supply chain network.Please assign a risk level to each identified risk and categorize the supply chain hazards based on their respective types. Next, it is important to prioritize these dangers based on their individual risk ratings. In general, it is advisable to address hazards at the highest level of severity initially, and afterwards proceed in descending order of risk priority(82, 83).

- **Step 3: Mitigate Risks**

After identifying the risks that require immediate attention, it is necessary to determine the appropriate approach for managing each of them. The decision on the acceptance, rejection, transfer, or mitigation of each risk must be made. In the context of supply chain risk management, it may be prudent to consider the option of sourcing from an alternative vendor with a lower level of inherent risk.It is imperative to regularly engage in risk management questionnaires with third-party entities in order to assess the adequacy of risk mitigation measures for existing risks and identify any emerging concerns. Whether an individual opts to utilize a pre-existing risk management framework template or develops their own, the construction of onboarding questionnaires and routine inquiries should be strategically devised to facilitate a thorough examination of the security measures that third parties are implementing inside their operational processes(84).

Depending on the responses provided in the questionnaires, third parties exhibiting significantly elevated levels of risk may necessitate an audit. In certain instances, it may be imperative to undertake on-site visits as deemed required(85).

- **Step 4: Repeat**

Upon the completion of the aforementioned steps, it will be necessary to initiate the aforementioned process anew. Supply chain risk management constitutes a continuous procedure applicable to all third-party entities inside the supply chain. This process necessitates frequent repetition and should be implemented over the whole lifecycle of the third-party relationship(86).

- **Step 5: Practice Continuous Monitoring**

Continuous monitoring is an imperative activity due to the dynamic nature of business partners, who frequently modify their operational procedures. The responsibility of consistently monitoring changes in one's own business, supply chain network, and regulatory and industry standards is a challenging yet necessary endeavor.In numerous instances, the reliance solely on due diligence becomes insufficient in the realm of cybersecurity. Continuous monitoring has the potential to mitigate the occurrence of cyberattacks and data breaches, thereby safeguarding not only the organization itself but also the third parties involved in its supply chain(87, 88).

At a certain juncture, numerous firms must acknowledge their inability to independently manage the complete process of supply chain risk management. Unless an organization is a huge firm, the process of risk management can be financially burdensome and time-intensive, rendering it unfeasible for smaller companies to undertake internally.Businesses seeking solutions can utilize software to aid in their endeavors. The utilization of governance, risk management, and compliance (GRC) software can facilitate the enhancement of one's risk management program, specifically in relation to cyber risk. By utilizing straightforward and automated methods for supply chain risk management, organizations can enhance their supply chain network and alleviate the workload imposed on internal personnel(89, 90).

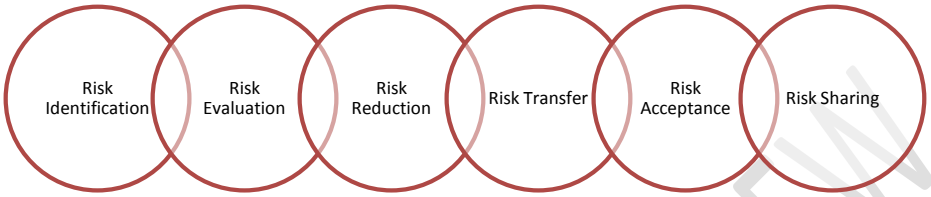

Figure 4 risk managment

Comment [lm4]: review the figures in order to cite the reference source.

6. Risk Management Models

Organizations can enhance their supply chain processes by implementing established supply chain management models. The Six Sigma DMAIC model encompasses a series of sequential steps, commencing with the definition of improvement targets for a given process. Subsequently, the model incorporates the measurement, analysis, improvement, and ultimately, the control of that process. A study conducted in 2006 examined the feasibility of implementing the Six Sigma methodology in the defense supply chain of the United Kingdom. The findings indicated that although the methodology could be applied, certain factors such as stock holding policies and activity levels posed limitations that hindered its implementation(91).

The Cyber Kill Chain is a framework utilized to delineate the many phases involved in a cyber-based assault. The Cyber Kill Chain encompasses several distinct steps, namely reconnaissance, weaponization, delivery, exploitation, installation, command and control, and operations on objectives. Reassessments of the model in the context of Cyber-Physical Systems have proposed modifications to existing knowledge on attacks, particularly in the domains of control systems and physical systems, where the resulting outcomes have palpable ramifications. The Supply-Chain Operations Reference model (SCOR) presents itself as a viable substitute for the Cyber

Kill Chain. SCOR is a comprehensive framework that spans several industries and aims to assess and enhance the overall performance and management of supply chains inside enterprises. The SCOR framework delineates the following distinct elements and their interconnectedness: processes, benchmarking measures, management practices, and software product mappings. The primary objective of the SCOR (Supply Chain Operations Reference) model is to facilitate the exchange, evaluation, and advancement of novel or enhanced techniques within the realm of supply chain management(92).

6.1. Assessment of Existing Risk Management Models

Risk analysis and management models are valuable tools for evaluating the possible risks associated with the integration of new technologies into military supply chains. A multitude of frameworks are at one's disposal, encompassing CSCRM, risk matrices, Crown Jewel Analysis, and the Supply Chain Resilience Framework. Although these models contribute to the evaluation of risk, they fail to offer a comprehensive and equitable assessment of all the tangible and intangible factors that must be taken into account when contemplating the integration of new technology into military supply chains(93).

Numerous endeavors have been made to establish semantic models for risk assessment methods and paradigms, yielding certain levels of accomplishment. The continual study and development in this area is driven by the complexity, intricacy, and contextual demands associated with individual business, government domains, and regulatory requirements. The incorporation of cyber elements into these processes introduces further intricacy, necessitating new requirements for mapping and modeling(94).

The current management models pertaining to cyber security and supply chain management primarily concentrate on either cyber security or supply chains 4.0 in isolation, without adequately addressing their junction. The models discussed exhibited a certain degree of cross-compatibility; nevertheless, none of them explicitly addressed the military context of supply chains. Although certain aspects of these models may provide insights into the potential effects of new technology on military supply chains, it is important to note that they do not offer a

comprehensive answer. Consequently, there exists a research vacuum that has to be addressed(95).

6.2. Summary of Threats and Assessment Models

The applicability of adoption assessments is typically hindered by their specificity to a particular technology, hence limiting their wider use. This section provides a comprehensive overview of many currents and upcoming technologies, highlighting their profound implications for military supply networks. The subsequent assessment involved evaluating the methodologies employed to ascertain their suitability, with the aim of identifying any shared patterns in impact modeling across different technologies(96).

There exist numerous autonomous research domains that aim to explicitly conceptualize and delineate each of these domains, with the concurrent development of different models. The future research challenge in this domain involves the integration of these novel models, both among themselves and with other preexisting models in interconnected domains of discourse(97).

It is important to highlight that the current state of wireless communications, Cloud computing, the Internet of Things (IoT), the Industrial Internet of Things (IIoT), Industry 4.0, track and trace processes, cyber-physical systems, blockchain technologies, and Artificial Intelligence (AI) collectively play a significant role in the exploitability of supply chain 4.0. Therefore, it is imperative to address all these factors in order to enhance supply chain security. A prevailing pattern observed across the methodologies discussed in this part is the limited transferability of the frameworks to diverse and emerging technologies, as well as the notable absence of emphasis on military applications(98-104).

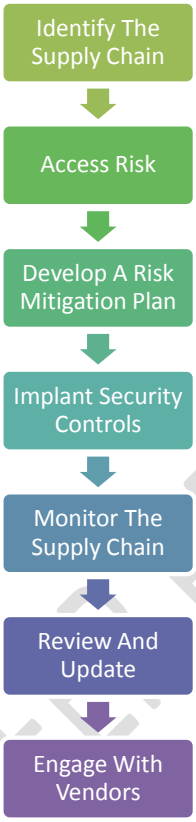

Figure 5 Risk Managment

Comment [lm5]: review the figures in order to cite the reference source.

Conclusions:

In an era of rising global interconnectedness, companies are increasingly dependent on expansive supply chains to facilitate their operations. Nevertheless, the process of monitoring the supply chain and its associated risks is a laborious and costly endeavor for several firms. In numerous cases, enterprises that fail to effectively mitigate the risks connected with their supply chain are at a higher probability of falling prey to a cyberattack, hence leading to substantial interruptions in their operational activities. This article aims to provide a comprehensive analysis of supply chain risk management, focusing on the typically associated hazards and proposing five recommended measures that organizations can undertake to address these concerns.The concept of supply chain risk management, which involves the identification, assessment, and mitigation

of potential risks within a supply chain, has gained significant attention in recent years. Organizations are increasingly recognizing the importance of effectively managing risks that may disrupt the flow of goods.

The future trajectory of Social Customer Relationship Management (SCRM) is expected to involve a heightened emphasis on the management of third-party risks, a more extensive utilization of Artificial Intelligence (AI) and Machine Learning (ML), an increasing adoption of blockchain technology, amplified regulatory oversight, and the emergence of novel technologies and solutions.Organizations that demonstrate proactive measures in adjusting to these developments will be more effectively positioned to mitigate the risks associated with their supply chain and uphold the comprehensive security of their operations. In summary, firms who use these methods are more likely to enhance their business growth and maintain a competitive advantage over their rivals.

References:

Comment [lm6]: Many of the references that appear as bibliographical references do not appear in the text of the article. Review and keep only those mentioned.

1. Barreto L, Amaral A, Pereira T (2017) Industry 4.0 implications in logistics: an overview. Procedia Manuf. https://doi.org/10.1016/j.promfg.2017.09.045.
2. Barros AC, Senna P, Marchiori I, Kalaitzi D, Balech S (2020) Scenario-driven supply chain charaterization using a multi-dimensional approach. Fornasiero Ed et al (eds) Next generation supply chains: a roadmap for research and innovation. Springer.
3. Beamon B (2008) Sustainability and the future of supply chain management. Oper Supply Chain Manag Int J. https://doi.org/10.31387/oscm010003.
4. Boström M et al. (2015) Sustainable and responsible supply chain governance: challenges and opportunities. J Clean Prod. https://doi.org/10.1016/j.jclepro.2014.11.050.
5. Al-Mudimigh, A. S., Zairi, M., & Ahmed, A. M. M. (2004). Extending the concept of supply chain: The effective management of value chains. Int J Prod Econ, 87(3), 309–320.
6. Anderson G (2016) The economic impact of technology infrastructure for smart manufacturing. NIST Econ Anal Briefs 4. https://doi.org/10.6028/NIST.EAB.4.

7. Ani, U. D., Watson, J. D. M., Nurse, J. R. C., Cook, A., & Maple, C. (2019). A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic Modelling landscape. PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT - 2019, 1–16. Retrieved from http://arxiv.org/abs/1904.01551. Accessed 1 Oct 2019.

8. Anthi, E., Williams, L., & Burnap, P. (2018). Pulse: an adaptive intrusion detection for the internet of things. Living Internet Things 35 (4 pp.). doi: https://doi.org/10.1049/cp.2018.0035.

9. Ashton K (2011) In the real world, things matter more than ideas. RFID J 22(7) Retrieved from http://www.rfidjournal.com/articles/pdf?4986. Accessed 1 Oct 2019.

10. ASI, A. for strategic initiatives. (2016). National Technology initiative, Agency for Strategic Initiatives. Retrieved May 10, 2017, from Government of Russia website: https://asi.ru/eng/nti/. Accessed 1 Oct 2019.

11. Charmaz K (2006) Constructing grounded theory : a practical guide through qualitative analysis. Sage Publications, London.

12. De Roure, D., Page, K. R., Radanliev, P., & Van Kleek, M. (2019a). Complex coupling in cyber-physical systems and the threats of fake data. Living in the Internet of Things (IoT 2019), 2019 Page, 11 (6 pp.). doi: https://doi.org/10.1049/cp.2019.0136.

13. Easterby-Smith M, Thorpe R, Lowe A (2002) Management research : an introduction. Sage Publications, London.

14. Eriksson P, Kovalainen A (2008) Qualitative methods in business research. Sage, London.

15. Evans, P. C., & Annunziata, M. (2012). Industrial Internet: Pushing the Boundaries of Minds and Machines. Retrieved from https://www.ge.com/docs/chapters/Industrial_Internet.pdf.

16. Goulding C (2002) Grounded theory : a practical guide for management, business and market researchers. Sage Publications, London.

17. Gummesson E (2000) Qualitative methods in management research. Sage Publications, London.

18. John, P. (2017). High Value Manufacturing Catapult. Retrieved from https://ec.europa.eu/growth/tools-databases/regional-innovation-monitor/sites/default/files/report/High value manufacturing Catapult_1.Pdf.

19. Kaplan, R. S., & Norton, D. P. (1996). Using the balanced scorecard as a strategic management system. Harvard business review Boston.

20. Lee, B., Cooper, R., Hands, D., & Coulton, P. (2019b). Value creation for IoT: Challenges and opportunities within the design and development process. Living in the Internet of Things (IoT 2019). IET, Living in the Internet of Things 2019, London, United Kingdom, 1–8. Retrieved from doi: https://doi.org/10.1049/cp.2019.0127.

21. Madaan A, Nurse J, de Roure D, O'Hara K, Hall W, Creese S (2018) A storm in an IoT Cup: The Emergence of Cyber-Physical Social Machines. SSRN Electron J. https://doi.org/10.2139/ssrn.3250383.

22. Mentzer JT, DeWitt W, Keebler JS, Min S, Nix NW, Smith CD, Zacharia ZG (2001) Defining supply chain management. In: Journal of Business logistics (Vol. 22). Wiley Online Library.

23. METIJ (2015) RRI, robot revolution initiative - summary of Japan's robot strategy - It's vision, strategy and action plan. Ministry of Economy, Trade and Industry of Japan, Japan. Retrieved from http://www.meti.go.jp/english/press/2015/pdf/0123_01c.pdf.

24. MIUR (2014) Italian Technology Cluster: Intelligent Factories. Ministry of Education Universities and Research Retrieved May 9, 2017, from Cluster Tecnologico Nazionale Fabbrica Intelligente | Imprese, università, organismi di ricerca, associazioni e enti territoriali: insieme per la crescita del Manifatturiero, Italy. website: http://www.fabbricaintelligente.it/en.

25. Ouyang, J., Lin, S., Jiang, S., Hou, Z., Wang, Y., Wang, Y., … Hou, Zhenyu; Wang, Yong; Wang, Y. (2014). SDF: software-defined flash for web-scale internet storage systems. Proceedings of the 19th international conference on architectural support for programming languages and operating systems - ASPLOS '14, 42(1), 471–484. doi: https://doi.org/10.1145/2541940.2541959.

26. Radanliev P, De Roure D, Nicolescu R, Huth M (2019a) A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0. In: University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre. https://doi.org/10.13140/RG.2.2.26854.47686.

27. Radanliev P, Nicolescu R, De Roure D, Huth M (2019b) Harnessing economic value from the internet of things, London.

28. Radanliev P, Roure D, De Nurse J, Nicolescu R (2019c) Cyber risk impact assessment–discussion on assessing the risk from the IoT to the digital economy. University of Oxford Combined Working Papers and Project Reports Prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre.

29. Radanliev P (2014) A conceptual framework for supply chain systems architecture and integration design based on practice and theory in the North Wales slate mining industry. British Library, Cardiff. https://doi.org/ISNI:0000 0004 5352 6866.

30. Radanliev P (2015a) Architectures for green-field supply chain integration. J Supply Chain Oper Manage 13(2). https://doi.org/10.20944/preprints201904.0144.v1.

31. Radanliev P (2016) Supply chain systems architecture and engineering design: green-field supply chain integration. Oper Supply Chain Manage 9(1). https://doi.org/10.20944/preprints201904.0122.v1.

32. Radanliev, Petar, De Roure, D., Cannady, S., Mantilla Montalvo, R., Nicolescu, R., & Huth, M. (2018a). Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. Living in the Internet of Things: Cybersecurity of the IoT - 2018, (CP740), 3 (9 pp.). doi: https://doi.org/10.1049/cp.2018.0003.

33. Radanliev, Petar, Roure, D. C. De, R.C. Nurse, J., Montalvo, R. M., Cannady, S., Santos, O., Maple, C. (2020). Future developments in standardisation of cyber risk in the internet of things (IoT). SN Appl Sci, (2: 169), 1–16. doi: https://doi.org/10.1007/s42452-019-1931-0.

34. Tan, Y., Goddard, S., & Pérez, L. C. (2008). A prototype architecture for cyber-physical systems. ACM SIGBED Review - Special Issue on the RTSS Forum on Deeply Embedded Real-Time Computing, 5(1). Retrieved from http://delivery.acm.org/10.1145/1370000/1366309/p26-tan.pdf?ip=129.67.116.155&id=1366309&acc=ACTIVE SERVICE&key=BF07A2EE685417C5.F2FAECDC86A918EB.4D4702B0C3E38B35.4D4702B0C3E38B35&CFID=922793771&CFTOKEN=47199625&__acm__=1492383641_ca27b2c456d59140.

35. Taylor P, Allpress S, Carr M, Lupu E, Norton J, Smith L, Blackstock J, Boyes H, Hudson-Smith A, Brass I, Chizari H, Cooper R, Coulton P, Craggs B, Davies N, De Roure D, Elsden M, Huth M, Lindley J, Maple C, Mittelstadt B, Nicolescu R, Nurse J, Procter R, Radanliev P, Rashid A, Sgandurra D, Skatova A, Taddeo M, Tanczer L, Vieira-Steiner R et al

(2018) Internet of things realising the potential of a trusted smart world. Royal Academy of Engineering, London.

36. Advanced Manufacturing Partnership. NIST Advanced Manufacturing Office2013.

37. Industrie 4.0 smart manufacturing for the future2014 2014//.

38. Industria Conectada 4.0: La transformación digital de la industria española Dossier de prensa; Ministry of Economy Industry and Competitiveness Accessibility2015 2015//.

39. NRS, New Robot Strategy - Vision Strategy and Action Plan; Ministry of Economy Trade and Industry of Japan2015 2015//.

40. Partnering for Cyber Resilience Towards the Quantification of Cyber Threats2015 2015//.

41. G20 New Industrial Revolution Action Plan2016 2016//.

42. The Industrial Internet of Things, Volume B01: Business Strategy and Innovation Framework; Industrial Internet Consortium2016 2016//.

43. New Industrial France: Building France's industrial future - updated text from the 2013 version2016 2016//.

44. The Industrial Internet of Things Volume G5: Connectivity Framework; Industrial Internet Consortium2017 2017//.

45. Plattform Industrie 4.0 - Testbeds2017 2017//.

46. Industrial Value Chain Reference Architecture; Industrial Value Chain Initiative2017 2017//.

47. Made in China 2025; the state council People Republic of China2017 2017//.

48. Made Different: Factory of the Future 4.02017 2017//.

49. Petras - cyber risk assessment for coupled systems (CRACS)2018 2018//.

50. Petras - Impact Assessment Model for the IoT (IAM). Retrieved February 20, 20202018 2018//.

51. Common vulnerability scoring system SIG. Retrieved December 26, 20172019 2019//.

52. FAIR risk analytics platform management. Retrieved December 26, 20172020 2020//.

53. Agyepong E, Cherdantseva Y, Reinecke P, Burnap P. Challenges and performance metrics for security operations center analysts: a systematic review. J Cyber Secur Technol. 2019;4.

54. Ahmed SH, Kim G, Kim D. Cyber physical system: architecture, applications and research challenges. IFIP Wireless Days (WD). 2013;2013.

55. Akinrolabu O, Nurse JRC, Martin A, New S. Cyber risk assessment in cloud provider environments: current models and future needs. Comput Secur. 2019;87.

56. Allen, Hamilton. Cyber Power Index: Findings and Methodology2014 2014//.

57. Almeida L, Santos F, Oliveira L. Structuring Communications for Mobile Cyber-Physical Systems2016 2016//.

58. Anderson R, Moore T. The economics of information security. Sci AAAS. 2006;314.

59. Anthi E, Williams L, Slowinska M, Theodorakopoulos G, Burnap P. A supervised intrusion detection system for smart home IoT devices. IEEE Internet Things J. 2019;6.

60. Anthonysamy P, Rashid A, Chitchyan R. Privacy Requirements: Present & Future. 2017 IEEE/ACM 39th international conference on software engineering: software engineering in society track (ICSE-SEIS)2017.

61. Axon L, Alahmadi B, Nurse JRC, Goldsmith M, Creese S. Sonification in Security Operations Centres: What do Security Practitioners Think?2018 2018//.

62. Balaji B, Faruque MA, Dutt N, Gupta R, Agarwal Y. Models, abstractions, and architectures2015 2015//.

63. Bauer W, Hämmerle M, Schlund S, Vocke C. Transforming to a Hyper-connected Society and Economy – Towards an "Industry 4.0.". Procedia Manufacturing. 2015;3.

64. Benveniste A. Loosely Time-Triggered Architectures for Cyber-Physical Systems. 2010 Design. Dresden: Exhibition; 2010 2010//.

65. Benveniste A, Bouillard A, Caspi P. A unifying view of loosely time-triggered architectures. Proceedings of the tenth ACM international conference on embedded software - EMSOFT '102010.

66. Bhave A, Krogh BH, Garlan D, Schmerl B. View consistency in architectures for cyber-physical systems. 2011 IEEE/ACM second international conference on cyber-physical systems2011.

67. Biener C, Eling M, Wirfs JH. Insurability of cyber risk 12014 2014//.

68. Blatter J, Haverland M. Designing case studies2012 2012//.

69. Bloem da Silveira Junior LA, Vasconcellos E, Vasconcellos Guedes L, Guedes LFA, Costa RM. Technology roadmapping: A methodological proposition to refine Delphi results. Technol Forecast Soc Chang. 2018;126.

70. Böhm F, Menges F, Pernul G. Graph-based visual analytics for cyber threat intelligence. Cybersecurity. 2018;1.

71. Bouws T, Kramer F, Heemskerk P, Os M, Horst T, Helmer S. Smart Industry: Dutch Industry Fit for the Future2015 2015//.

72. Boyes H, Hallaq B, Cunningham J, Watson T. The industrial internet of things (IIoT): an analysis framework. Comput Ind. 2018;101.

73. Brass I, Pothong K, Tanczer L, Carr M. Standards, Governance and Policy. Cybersecurity of the Internet of Things (IoT): PETRAS Stream Report2019 2019//.

74. Brass I, Tanczer L, Carr M, Elsden M, Blackstock J. Standardising a moving target: the development and evolution of IoT security standards. Living Internet Things. 2018;24.

75. Brettel M, Fischer FG, Bendig D, Weber AR, Wolff B. Enablers for self-optimizing production Systems in the Context of Industrie 4.0. Procedia CIRP. 2016;41.

76. Breza M, Tomic I, McCann J. Failures from the environment, a report on the first FAILSAFE workshop. ACM SIGCOMM Comput Commun Rev. 2018;48.

77. Bryceson KP, Slaughter G. Alignment of performance metrics in a multi-enterprise agribusiness: achieving integrated autonomy? Int J Product Perform Manag. 2010;59.

78. Carruthers K. Internet of things and beyond: cyber-physical systems - IEEE internet of things. IEEE Internet of Things2016 2016//.

79. Córdova F, Durán C, Sepúlveda J, Fernández A, Rojas M. A proposal of logistic services innovation strategy for a mining company. J Technol Manag Innov. 2012;7.

80. Craggs B, Rashid A. Smart cyber-physical systems: beyond usable security to security ergonomics by design. 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)2017.

81. David M. Science in society. New York: Palgrave Macmillan; 2005 2005//.

82. DiMase D, Collier ZA, Heffner K, Linkov I. Systems engineering framework for cyber physical security and resilience. Environ Syst Decisions. 2015;35.

83. Dombrowski U, Wagner T. Mental strain as field of action in the 4th industrial revolution. Procedia CIRP. 2014;17.

84. Eggenschwiler J, Agrafiotis I, Nurse JR. Insider threat response and recovery strategies in financial services firms. Comput Fraud Secur. 2016;2016.
85. Eisenhardt KM. Building theories from case study research. Acad Manag Rev. 1989;14.
86. Faller C, Feldmüller D. Industry 4.0 learning factory for regional SMEs. Procedia CIRP. 2015;32.
87. Ghirardello K, Maple C, Ng D, Kearney P. Cyber security of smart homes: development of a reference architecture for attack surface analysis. Living Internet Things. 2018;45.
88. Giordano A, Spezzano G, Vinci A. A smart platform for large-scale cyber-physical systems2016 2016//.
89. Gordon LA, Loeb MP. The economics of information security investment. ACM Trans Inf Syst Secur. 2002;5.
90. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): A vision, architectural elements, and future directions. Futur Gener Comput Syst. 2013;29.
91. Hahn A, Ashok A, Sridhar S, Govindarasu M. Cyber-physical security Testbeds: architecture, application, and evaluation for smart grid. IEEE Trans Smart Grid. 2013;4.
92. Hermann M, Pentek T, Otto B. Design principles for Industrie 4.0 scenarios. 2016 49th Hawaii international conference on system sciences (HICSS)2016.
93. Hussain F. Internet of everything. Internet of Things: Building Blocks and Business Models: SpringerBriefs in Electrical and Computer Engineering2017.
94. Jayaram J, Tan KC. Supply chain integration with third-party logistics providers. Int J Prod Econ. 2010;125.
95. Jazdi N. Cyber physical systems in the context of industry 4.0. 2014 IEEE international conference on automation, quality and testing, robotics2014.
96. Jensen JC, Chang DH, Lee EA. A model-based design methodology for cyber-physical systems2011 2011//.
97. Okutan A, Yang SJ. ASSERT: attack synthesis and separation with entropy redistribution towards predictive cyber defense. Cybersecurity. 2019;2.
98. Kambatla K, Kollias G, Kumar V, Grama A. Trends in big data analytics. J Parallel Distrib Comput. 2014;74.
99. Kang W, Kapitanova K, Son SH. RDDS: A real-time data distribution Service for Cyber-Physical Systems. IEEE Trans Ind Inform. 2012;8.

100. Kleek M, Binns R, Zhao J, Slack A, Lee S, Ottewell D, et al. X-ray refine2018 2018//.
101. Maple C, Bradbury M, Le AT, Ghirardello K. A connected and autonomous vehicle reference architecture for attack surface analysis. Appl Sci. 2019;9.
102. Müller JM, Buliga O, Voigt KI. Fortune favors the prepared: how SMEs approach business model innovations in industry 4.02018 2018//.
103. Nicolescu R, Huth M, Radanliev P, Roure D. Mapping the values of IoT. J Inf Technol. 2018;33.
104. Nurse JR, Radanliev P, Creese S, Roure D. Realities of risk: 'if you can't understand it, you can't properly assess it!': The reality of assessing security risks in internet of things systems. Living Internet Things. 2018;2018.