Enhancement to Cybersecurity Awareness in Supply Chain

Supervisor: Bramwell Brizendine

Team Members:	**Email**
Simon Gilbert	*gs0100@uah.edu*
Robow Adan	*ar0245@uah.edu*
Mwebie Linet	*lm0111@uah.edu*

Contents

Abstract

One of the many improvements which can be made in the cyber security in supply chains is to generally lessen the existing cyber threats. The main subject of this paper is some of the methods which have the potential to enhance the level of awareness in the ecosystem of supply chains. With the introduction of C-SCRM, it will be possible to build up a culture of keen alertness and thoroughness within organizations by providing high-quality training programs to staff members. Teams are built up through work-related teams and input sharing process which enables organizations to identify and address risks before they become serious problems. Furthermore, AI (artificial intelligence) and blockchain, which are trust technology, can be added to transparent and traceable elements. They are also not just about cyber security protection. In fact, they form a venture chain of supply network that is not only confident but also full of resilience.

1. Introduction

1.1 Problem Statement

In the world of global, complicated, and digital supply chains, highlighted by the growing dependency of these networks on digital technologies, cybersecurity has already become critical. Thus, it is vital to reinforce the security of such diverse networks. This literature review, using six informative articles, illustrates the multifaceted aspects of cybersecurity for the Supply Chain, resilience, and awareness. The articles cover diverse topics, from the cyber-security issues of small and medium enterprises (SMEs) to the part of blockchain in higher education supply chains to systematic reviews highlighting cybersecurity activities in supply chain management. In this regard, it provides an overall perception of the issues and opportunities that policymakers should keep in mind when they establish cybersecurity awareness in different industries and areas of the economic infrastructure, thus necessitating further investigation and actions in this field.

Erdogan et al. (2023) highlight that the budget constraints faced by small and medium enterprises make them risky because half of the electronic business depends on them. This sector of e-commerce that relies on SMEs is greatly affected by a need for more awareness and security practices. The researchers investigated SME cybersecurity awareness through 141 SMEs from the UK, which showed a need for more knowledge and limited risk management practices. The research thus recommends that developing customized tools and techniques to enhance cyber security for SMEs be a strategy to determine future growth in this field.

In their study, Kendzierskyj et al. (2023) examine the relationship between blockchain technology and the Cyber Security Maturity Model to affect the governance of higher education supply chains. It is argued that global supply chains, new technologies, and increased online learning demand have transformed the labor market. The hybrid model proposed in this paper adopts blockchain and CSMM (Convergence of Cloud Service Models) to resolve the data security and privacy issues in the higher education supply chains (and other sectors).

The project aims to provide a solution to an important problem of the lack of cybersecurity awareness in supply chains, which is a global issue for organizations. Regardless of the fact that the cyber-attacks are more often and more complicated than ever before, businesses especially those within SMEs are still unaware of the risks of cybersecurity throughout the supply chain which has remained the same. This inadequacy, if not addressed, may expose them to the risks of data breaches, malware infections, and supply chain disruptions. In addition, the intricate web of today's supply chains aggravates these issues as the weakness in a single entity is transmitted throughout the entire network. Therefore, the cybersecurity departments within the supply chains should be improved to deal with the risks in a more effective manner. This project aims to create the strategies, tools, and frameworks to train stakeholders, enhance threat assessment capabilities and cultivate a culture of cyber resilience all through the supply network ecosystem.

1.2 Purpose Statement

An article by Latif et al. (2021) conducted a comprehensive systematic review of cybersecurity in supply chain management. The study covers ten years, from 2010 to 2020, and is a systematic review of 41 articles collected. The assessment is categorized into four domains: network security, information security, web application security, and Internet of Things (IoT). The study calls for additional research on cybersecurity in supply chains and gives some research directions for the future.

With the aid of Masip-Bruin et al. (2021), the article delves into the particular demanding situations of cybersecurity in ICT supply chains, focusing on the need for a coordinated framework for cyber resilience. The proposed architecture objectives include safety and privacy functionalities, threat and vulnerability control, and security metrics. The paper underlines the growing dependence on ICT systems in Industry 4.0, emphasizing the critical want for cyber resilience and the challenges posed by disruptions. Additionally, it identifies the robust hyperlink

between cyber resilience and cybersecurity, highlighting the dynamic and complicated nature of contemporary threats.

Melnyk et al. (2022) mention the changing nature of supply chain management and that the latest cybersecurity offenses point to the interdependent structure of organizations' ecosystems. The authors promote cybersecurity studies using research frameworks across the supply chain. The exploratory methodology, the literature review, expert interviews, and external validation, will function as a tool to uncover the main problems and chances in this field.

Parker et al. (2023) consider the interplay between computation, network, and physical processes in chemical industries. The article presents some authors' research on cybersecurity issues in process control, operation, and supply chain management. Several machine learning based detection methods and robust control strategies are touched upon, emphasizing domain specific cybersecurity in critical infrastructures.

The study conducted by Shukla et al. (2023) proposed a framework of multi-objective measures used to identify and optimize the factors affecting cybersecurity in the Industry 4.0 supply chain. This architecture integrates breach databases and textual information computational power to identify risks, threats, and countermeasures in cyber scenarios. The model provides efficient decision-making capability using the multiple-objective optimization mechanism, which can find the trade-off relationship between cyber risk and investment. It contributes to the predictive strategies.

The overall goal of this initiative is to increase the cybersecurity awareness in the supply chain network, which further underlines the need for strong defenses against cyber threats. The project plans to put in place a complete strategy that will employ the latest technologies in a bid to create more awareness and a culture of readiness among the stakeholders. The project aspires to achieve

this by means of knowledge dissemination, training programs, and integration of C-SCRM (Cyber Supply Chain Risk Management) practices. The main objective is to enable organizations to preventatively detect, assess, and mitigate cybersecurity risks across their supply chains. Through the promotion of collaboration, information sharing and transparency, the initiative is expected to enhance the resilience of supply chains which will protect businesses from being exposed to cyber threats and ensure the secrecy and security of the operations.

2. Executive Summary

The present study uniquely discovers the areas of cybersecurity concern in complex supply networks for SMEs. The course is directed towards the strengthening of cybersecurity knowledge that can help maintain the integrity of the network against continuous cyberattacks. The project looks at the holistic approach of education, technology and community action to carry out the policy creation that is value added. The objective is to conduct a comprehensive and thorough assessment of the program's effects, with particular regard to protecting the data that has been infringed and acting before the disabilities that are caused by cybersecurity risks to the global economy. The results are summarized in the final project report, which includes the ready-to-use modules and content, and we will make presentations and technological designs available for the general public through an open-source platform. In spite of the fact that the outputs of the research are intangible, they will also result in the reorganization of the supply chain in a number of ways. It does not merely depend on known threats, rather it proactively detects, and spots the emerging new cyber threats. This plan will also target the SMEs that are part of the complex supply chains on the one hand and will be aimed at promoting collaboration and partnership among the related actors on the other hand. The organization aims to develop a solid cybersecurity policy with strict principles and standards in order to allow for a flexible platform

that can be adjusted to any kind of security flaws or changes. The study, therefore, concludes with a safe and steady virtual space that makes it possible for infrastructure operators to be a productive workforce in the existing cyberspace ecosystem.

3. Motivation

In our daily digital life, the current supply chain is facing new threats of cyber; therefore, a strategic response is a necessity for such kind of cyber problems (Kendzierskyj et al., 2023). A significant need to intensify cybersecurity awareness and education within the supply chain has arisen, and this is the reason our research project is targeted in this area. The emergence of this quality is of primary importance since it can keep valuable data away from external sources, get rid of the threats that cybercrime causes, and enforce the global economy. The stakeholders would not only focus on the cryptology battle but would also link it with the society that has more than that. Society is not just a matter of security and stability but supply chain destruction (Parker et al., 2023). Basically, the creation of effective strategies that go beyond the old scenarios should be the focus of the new schemes. These strategies should involve the knowledge of all components of the supply chain (stakeholders) and also the development of robust cybersecurity measures. With each passing day, cyber warfare becomes more sophisticated and complicated. On the contrary, when cyber attackers attempt to infiltrate the manufacturing process, the aftermath may not only bring the corporate reputation damage to the ground but also put the health and safety of customers in jeopardy. For this reason, the importance and need for the research is undoubtedly real and should be carried out now in order to be sure in the future.

4. Literature review

In the world of global, complicated, and digital supply chains, highlighted by the growing dependency of these networks on digital technologies, cybersecurity has already become critical. Thus, it is vital to reinforce the security of such diverse networks. This literature review, using six informative articles, illustrates the multifaceted aspects of cybersecurity for the Supply Chain, resilience, and awareness. The articles cover diverse topics, from the cyber-security issues of small and medium enterprises (SMEs) to the part of blockchain in higher education supply chains to systematic reviews highlighting cybersecurity activities in supply chain management. In this regard, it provides an overall perception of the issues and opportunities that policymakers should keep in mind when they establish cybersecurity awareness in different industries and areas of the economic infrastructure, thus necessitating further investigation and actions in this field.

Erdogan et al. (2023) highlight that the budget constraints faced by small and medium enterprises make them risky because half of the electronic business depends on them. This sector of e-commerce that relies on SMEs is greatly affected by a need for more awareness and security practices. The researchers investigated SME cybersecurity awareness through 141 SMEs from the UK, which showed a need for more knowledge and limited risk management practices. The research thus recommends that developing customized tools and techniques to enhance cyber security for SMEs be a strategy to determine future growth in this field.

In their study, Kendzierskyj et al. (2023) examine the relationship between blockchain technology and the Cyber Security Maturity Model to affect the governance of higher education supply chains. It is argued that global supply chains, new technologies, and increased online learning demand have transformed the labor market. The hybrid model proposed in this paper adopts blockchain

and CSMM (Convergence of Cloud Service Models) to resolve the data security and privacy issues in the higher education supply chains (and other sectors).

An article by Latif et al. (2021) conducted a comprehensive systematic review of cybersecurity in supply chain management. The study covers ten years, from 2010 to 2020, and is a systematic review of 41 articles collected. The assessment is categorized into four domains: network security, information security, web application security, and Internet of Things (IoT). The study calls for additional research on cybersecurity in supply chains and gives some research directions for the future.

With the aid of Masip-Bruin et al. (2021), the article delves into the particular demanding situations of cybersecurity in ICT supply chains, focusing on the need for a coordinated framework for cyber resilience. The proposed architecture objectives include safety and privacy functionalities, threat and vulnerability control, and security metrics. The paper underlines the growing dependence on ICT systems in Industry 4.0, emphasizing the critical want for cyber resilience and the challenges posed by disruptions. Additionally, it identifies the robust hyperlink between cyber resilience and cybersecurity, highlighting the dynamic and complicated nature of contemporary threats.

Melnyk et al. (2022) mention the changing nature of supply chain management and that the latest cybersecurity offenses point to the interdependent structure of organizations' ecosystems. The authors promote cybersecurity studies using research frameworks across the supply chain. The exploratory methodology, the literature review, expert interviews, and external validation, will function as a tool to uncover the main problems and chances in this field.

Parker et al. (2023) consider the interplay between computation, network, and physical processes in chemical industries. The article presents some authors' research on cybersecurity issues in

process control, operation, and supply chain management. Several machine learningbased detection methods and robust control strategies are touched upon, emphasizing domainspecific cybersecurity in critical infrastructures.

The study conducted by Shukla et al. (2023) proposed a framework of multi-objective measures used to identify and optimize the factors affecting cybersecurity in the Industry 4.0 supply chain. This architecture integrates breach databases and textual information computational power to identify risks, threats, and countermeasures in cyber scenarios. The model provides efficient decision-making capability using the multiple-objective optimization mechanism, which can find the trade-off relationship between cyber risk and investment. It contributes to the predictive strategies.

The literature on cybersecurity in supply chains, specifically in the context of Supply Chain 4.0, emphasizes the precise challenges and possibilities presented by using superior technologies. In the survey with the aid of Sobb et al. (2020), Supply Chain 4.0 is recognized as the fourth revolution in supply chain management, incorporating technologies consisting of block chain, clever contracts, synthetic intelligence, and the Internet of Things. However, this integration brings forth full-size cyber risks, a lack of semantic requirements, inadequate interoperability, and insufficient security measures.

The given articles provide for a very wide perspective on the complex area of cybersecurity, where the main obstacle is the supply chain reinforcement, especially for the Small and Medium Enterprises (SMEs). Authors focus their research on small and medium sized enterprises as part of value chains; they give examples of customized cyber risk tools, models, and strategies to enable effective cyber defense while taking into consideration the specifics of the different business settings. By emphasizing the key link between private education and industry 4.0, the talk clarifies

how two factors, information diffusion and skills training, are both essential to overcome the threats of cybercrime. This task can be achieved by the creation of policy and standardization that address the particular needs of SMEs, otherwise they can lack the resources to effectively provide cyber resiliency. In the next time, the research can be designed by the upcoming technologies and threats so that the cybersecurity ecosystem can be embedded among all the stakeholders including the supply chain.

5. Policy Development

Developing and setting up policies helps organizations to check problems before they happen and make plans to deal with them. Policies are the educational and awareness tools that increase awareness of cybersecurity in SMEs and thus reduce human error vulnerabilities (Al-Farsi et al., 2021). They also act as a basis for regular reconsideration and improvement of cybersecurity measures, keeping them up to date with fast changing attack methods.

This policy comprises of nine main practices that should be strictly observed in SMEs.

5.1 Hardware Bill Of Material (HBOM)

In the midst of a small business environment where every resource is a precious asset and where efficiency is highly considered, the use of Hardware Bill of Materials (HBOMs) can be a dynamic strategy. HBOMs function as the main reference lists, or the overall inventory of the components that are used to build or maintain hardware systems. This article revolves around the fact that HBOMs can be used in small businesses and what is their benefit and harm with the help of the cases from theory and practice.

5.1.1 The Functionality and Significance of HBOMs in Small Businesses

The fact that HBOMs can reduce the procurement processes to a single platform is one of the key benefits of this solution. For example, this small manufacturing company which has a specialty of custom electronic device production. This enables the enterprise to keep track of the HBOM for each product and subsequently facilitate the purchase of the required components in bulk that boosts the overall cost and production efficiency. In a situation where an HBOM is not part of the procurement process, this might mean a long and time-consuming manual checking of everything, from small components to large items. This may lead to delays and increased expenses because some items might be overlooked.

5.1.2 Advantages of HBOMs for Small Businesses

HBOMs enable the small businesses to streamline the inventory management, which is crucial for them given the limited space for storage. As an example, consider the computer shop that involves repairing. The shop can thereby order the required parts for routine maintenance jobs on time so as to avoid stockouts as well as overstocking simply by keeping a HBOM for such repairs in place. This is makes it possible for the shop to fulfill orders quickly which in turn offers flexibility to the shop without the need for the capital to tie up in excessive inventory.

Furthermore, HBOMs bring to the forefront the issue of quality control and product consistency. The thing about a small-scale hardware startup that needs to follow the predetermined HBOM for their products is that each of them will meet the specified standards and will perform in the same way. This consistency, in turn, creates customer trust and a strong brand reputation - two factors that are vital for continued growth and the market standing in a competitive environment.

In addition, HBOMs provide a robust support for a successful troubleshooting and maintenance. Say, for example, think of a small IT consultancy firm that handles the network infrastructure for

various clients. Through this keeping the HBOMs for each client's specific hardware configuration, the company can rapidly pinpoint and replace the failed parts, thus reducing downtime and securing complete client satisfaction. The absence of HBOMs may bring about a complex and error-full process that takes time to diagnose the hardware problems leading to long term disruptions and dissatisfaction of the customers.

5.1.3 Practical Examples of HBOMs Utilization in Small Businesses

HBOMs become very valuable resources for small businesses, enabling them to optimize utilization of their resources, improve the quality of their products, and maintain their competitiveness. Although challenges include initial investment and complexity, HBOMs can simplify the processes and fuel the enterprise development. With the strategic application and the regularity of maintenance, the small businesses can exploit the power of HBOMs for persistence in today's dynamic market.

5.2 Software Bill Of Material (SBOM)

We are living in an era that is described by the escalation of cyber threats and complex software ecosystems; therefore, small businesses are exposed to supply chain attacks which are constantly increasing in number. The SolarWinds and Log4Shell cases are the most recent of the hacking attacks that remind of how dangerous such an attack can be for organizations of any size.

Nonetheless, despite the obstacles, small businesses can curb cyber threats by implementing SBOMs as a proven approach to build up a proper cybersecurity defense. This essay is about the role of SBOMs in small businesses, where we are going to explain their pros and cons, and the practical ways of using them.

5.2.1 SBOM Tool recommendation (Surfactant)

The Surfactant serves as a Software Bill of Materials (SBOM) tool by analyzing information from different files (PE, ELF, and MSI) within a directory structure that is usually associated with a software package. As this feature doesn't involve the execution or decompilation of files, it gathers the 'surface-level' metadata. The data is recorded, and then it is utilized to generate an SBOM (Software Bill of Materials) which is an enumerated list of the components and their dependencies within software. Surfactant strategy is the most important part of the curriculum for raising awareness on cybercrime threats and is of the great value for SMEs. SME is usually not equipped with professional security teams or resources, and their responsibilities can be insufficient and incomplete in terms of digital security assessment. Surfactant is a virtual assisted task that deals with the construction of SBOM, where it would be adopted by SMEs in the software supply chain monitoring. Being supplied with such compounds they are able to quickly deal with and resolve any problem. Moreover, Surfactant enables the collaboration with vendors, ensuring that the third-party software is consistent with the cybersecurity standards of the SMEs and elevates the security of the whole platform. To understand the working of the Surfactant tool, click to the following link; https://github.com/LLNL/Surfactant

5.2.2 The Functionality and Significance of SBOMs in Small Businesses

SBOMs serve as the full catalogue that accurately indicate the components, services and dependencies involved in the software that small businesses use. This visibility brings small business owners closer to their digital infrastructure giving them knowledge of the nuances that facilitate informed decisions on the kind of security measures to be used. SBOMs are effective in determining the sources and backgrounds of software components, which in turn helps organizations identify possible vulnerabilities and respond to them promptly. Besides, with the

help of the SBOMs, small businesses can provide the necessary records to show that they comply with the ever-changing regulations and the industry standards.

5.2.3 Advantages of SBOMs for Small Businesses

Enhanced Security Posture- SBOMs bring great benefit to the SMEs, as they provide them with critical information about their software supply chain and help them to start the vulnerabilities identification and mitigation process. A SBOM is a tool that promotes transparency, and therefore, organizations can strengthen their security position and proactively thwart potential threats.

Regulatory Compliance- As a result of the growing regulations, small businesses have to deal with the compliance rules established by the government and supervision agencies. SBOMs will simplify compliance processes as they give organizations a thorough list of software components and help them stay on the right path of regulatory compliance.

Cost-Efficient Risk Management- Through fast and timely vulnerability detection and patching, SBOMs prevent small businesses from experiencing financial losses that may result from cyber incidents. The use of SBOMs to proactively address security vulnerabilities that could potentially lead to hefty damage control expenses after the breach makes such measures unnecessary.

Streamlined Software Management- SBOMs facilitate a fast software procurement and management procedure for small business entities and consequently, the stakeholders have a comprehensive view of the software dependence. This gives a chance to anyone to pick the best software, license it, and maintain it, hence saving resources.

5.2.4 Practical Examples of SBOM Utilization in Small Businesses

An SBOM implementation is an instance of how a small local clinic could bring the compliance assurance level to a higher level through its healthcare organization. For the clinic, the HIPAA law becomes one of the stricter data privacy laws, and the clinic establishes and maintains SBOM

documents, which are modified to have software constituents and dependencies. During this whole process, this method not only satisfies the regulatory requirements, but also ensures the safety of patients' confidentiality from being at risk of legal responsibilities.

On the other hand, e-commerce boutique retailer, cybersecurity readiness becomes the key focus. With the ubiquity of supply chain attack risks in mind, the retailer incorporates SBOMs into its cybersecurity framework. Through the prevention of the entrance of malicious third-party software into the retailer's system, the retailer makes its own system more robust against cyberattacks. The first being the setting up of protective measures for customers' data and that of the brand reputation which is crucial for success in the crowded e-commerce environment.

Outstanding vendor supervision which is essential for a software development startup company becomes very crucial. The firm ensures the source codes are checked and third-party vendors are scrutinized for their security posture by taking advantage of SBOMs. Through the evaluation of vendor-submitted SBOMs, the company’s team receives information about potential security risks as well as the opportunity to check whether the software supply chain is secure. This particular and careful way of working increases clients and stakeholders trust, which is the basis for building a long-term success and development.

In summary, SBOMs represent the most important instruments of small enterprises that want to traverse safely the risky waters of the digital space. Although the implementation of SBOMs comes along with certain difficulties, the benefits of its adoption - improved security, regulatory compliance, cost-efficient risk management, and streamlined software maintenance - are much more than the drawbacks. Practical case studies highlight that SBOMs help small companies to strengthen their cybersecurity defenses, reduce risks, and to create trust among their customers and

partners. Small businesses face the challenge of changing cyber threats; SBOMs are the key items in their ammunition which allow them to stay strong and grow in digital world.

5.3 Determine the source of supplies of electronic devices such as laptops and computers

Taking the example of SolarWinds, it was indicated that the attack was traced back to a malicious software update that was added to the company's Orion software. This demonstrates the significance of secure software updates in the supply chain. As reported by Lazarovitz (2021) suspected nation-state hackers of SolarWinds were based in China during the same time that the Sunburst attack occurred. Based on this claim, SMEs should ensure that they purchase laptops and CPUs from trusted companies like Intel and HP rather than going for Chinese companies which may be compromised. The idea of sourcing supplies from trusted companies to avoid compromised supplies is supported by Akhtar (2020) in a discussion on latest trends in cyber-security after the case of SolarWinds. The author supported the policy by asserting that as a result of globalisation of politics, the US-China trade wars may be a threat to the respective companies in their supply chains and hence it is important to identify a reliable source of supplies. According to Coco et al. (2022), the best but painful way of addressing attacks on supply chains is naming and barring countries and companies that are associated with hacking supply chain systems. This argument is used in this policy to indicate that SMEs should identify and bar companies and countries that are engaged in supply chain attacks. Alternatively, they can get their supplies from countries such as South Korea, which produce high quality products and more secure. While Al-Farsi et al. (2021) do not agree with the idea of naming and barring supplies from a country identified as the origin of attacks, it is recommended in this policy because it would help to ensure that only the reliable sources are used. For instance, SolarWinds attack occurred as a result of software updates and

hence if the origin of the software is compromised, it would be easy for the attackers to attack the supply chains of SMEs.

5.4 Monitoring Network Connectivity

It is the conclusion of all the texts that the Solarwinds supply chain attacks, Wipro and Panasonic, etc., could have been stopped if the network connectivity and infrastructure were kept under scrutiny and any suspicious behavior or irregularities were identified early (Georgescu, 2021). Through the right network monitoring method for an SME, it can use network security tools and solutions that equipped SME with the features which are the visibility and management over their network devices, users and traffic. This could be accomplished too by the setup of a patch management process, which would ensure that all systems and application updates are installed in time. On the one hand, by means of extensive patch management that includes regular applications for all patches in the system wherever possible it is possible to reduce the attack surface and assure compliance to the timely patch management. Management on the other hand will evaluate the appropriate use of IDS and IPS to monitor the network traffic and detect known ransomware patterns and signatures. Thus, the Akhtar (2020) claims that there should be some monitoring and alerting system that indicates the unauthorized and anomalous activities like login attempts, configuration changes, and data transfer. This policy is outlined for the security analysts to perform periodical reviews and audit network records and logs in order to discover any breaches or intrusions in the net. To SolarWinds cyberattack, this is the time when a network monitoring system could have been the best solution. By that time the certificate would have been signed and the malicious code would have been detected and identified. As Lazarovitz (2021) has said, both the monitoring of the network by analyzing and detection of strange activities in the system by security analysts and they used these to mitigate the incident.

5.5 Segment Network

The use of micro-segmentation and a Zero Trust Policy engine is more effective as compared to the use of traditional network segmentation in preventing attacks on supply chain. This policy recommends the segmentation of the network into smaller and more isolated units in order to have different levels of access as well as security (Ofori et al., 2021). The practice is supported by Willett (2021) in a discussion on SolarWinds who indicated that network segmentation helps companies to limit the exposure and damage of a potential breach and at the same time reduce the attack complexity and surface of the network. This policy is aimed at dealing with the network connectivity and infrastructure in SMEs to ensure that the network is segmented into smaller units and hence when one unit is attacked the rest of the units are not attacked. In this case, SMEs should use routers, firewalls, and switches or other devices to create rules and boundaries between diverse segments of the network like functions, departments, or locations. As noted by Al-Farsi et al. (2021), micro-segmentation helps in restricting lateral movement that would contain the effect of a compromise. The combination offers dynamic access granular, controls, improved monitoring, and protection. The authors therefore indicated that micro segmentation prevents unauthorized access, isolate high- value assets, detects anomalies, and simplifies incident response.

5.6 Implement the Least Privilege Principle

The least privilege policy is a computer security concept that limits users the rights of accessing only to what is strictly required to do their jobs. The principle can restrict access rights for systems, applications, and processes to the authorized people only such as IT experts. This practice can be used to prevent attacks such as those occurred in British Airways whereby there was a data breach after a Mega cart supply chain attack. The principle denotes that in case of an attack, the actors of the threat would be limited only to the compromised operating system and hence it would not go

further to deploy their malicious code as they do not have access. Additionally, even in updating the software it should be done by a certain group of people who have received adequate training on how to effectively identify threat and mitigate it.

5.7 Secure Privileged Access Management

Once attackers have breached the defense, they search for privileged accounts because only these accounts would allow them access sensitive resources. Once the privileged account is compromised, it becomes easy to access sensitive data on supply chain (Coco et al., 2022). Some of the strategies that can be used to prevent privileged accounts include staff education, external PAM defenses, and internal PAM defenses, detecting third-party data leaks, and encrypting all internal data.

5.8 Hardening build environments against attackers

Attacks in Panasonic, SolarWinds, and Wipro occurred because the companies used poor practices like using insecure ftp protocol and public revealing passwords. However, SMEs can prevent attacks on their supply chain by hardening their build environments against the attackers whereby higher security requirements are used as in the production environments. SMEs ensure that they have quality assessments and requirements in the production but they have not implemented the same measurements in cyber-security. Reproducible builds would be used that always offers the same outputs give the same inputs so that the build outcomes are verifiable. SMEs should produce a build from source code and verify that the built outcomes came from the claimed source code. The strategies used in the company to harden build environments against the attackers should be communicated across the company to make all aware of the strategies adopted.

5.9 Identify all third-party data leaks

Companies have almost 30% chance of experiencing data breaches and over 60% of those breaches are associated to third parties (Georgescu, 2021; Blagden, 2020). So a policy that focuses on mitigating third- party breaches leading to supply chain attacks is very important. Many software applications rely on third party components and libraries that can introduce security risks if not properly managed. SBOM enables companies to assess the security posture of third-party components and evaluate the trustworthiness of their suppliers. Thus, companies make informed decisions about the suppliers to engage with and implement proper security controls to mitigate third party risks (Lazarovitz, 2021).

6.0 Educating Staff

The human resource plays a key role in the performance of any organisation particularly in ensuring that there is security of supply chain systems. Employees should be trained on HBOM and SBOM to ensure that they understand how they can use them to apply control over the materials supplied either hardware or software (Cavelty, 2014). Training should be done in phases and should as technology advances and should address how HBOM and SBOM can be used to mitigate attacks.

6.1 Integrating Cyber Supply Chain Risk Management (C-SCRM) across the organization

Implementing C-SCRM practices helps in thoroughly understanding the organization's supply chain structure. This increases visibility into the interconnected network of suppliers and vendors raising awareness among stakeholders about the potential cybersecurity risks inherent in the supply chain. It also helps in conducting comprehensive risk assessments throughout the supply chain by involving various departments and stakeholders. Through this, organizations can raise awareness about the importance of cybersecurity within the supply chain ecosystem. This heightened

visibility into the interconnected network of suppliers and vendors raises awareness among stakeholders about the potential cybersecurity risks inherent in the supply chain.

In summary it can be noted that the policy has three practices; determining the source of supplies of electronic devices such as laptops and computers, network connectivity monitoring, and network segmentation. These practices are designed to ensure that any anomaly is detected before it occurs and hence it does not affect the operations of SMEs.

6. Conclusion

In conclusion, the given articles provide for a very wide perspective on the complex area of cybersecurity, where the main obstacle is the supply chain reinforcement, especially for the Small and Medium Enterprises (SMEs). Authors focus their research on small and medium sized enterprises as part of value chains; they give examples of customized cyber risk tools, models, and strategies to enable effective cyber defense while taking into consideration the specifics of the different business settings. By emphasizing the key link between private education and industry 4.0, the talk clarifies how two factors, information diffusion and skills training, are both essential to overcome the threats of cybercrime. This task can be achieved by the creation of policy and standardization that address the particular needs of SMEs, otherwise they can lack the resources to effectively provide cyber resiliency. In the next time, the research can be designed by the upcoming technologies and threats so that the cybersecurity ecosystem can be embedded among all the stakeholders including the supply chain.

7. References

Akhtar, N. (2020). Latest trends in the cyber-security after the solar wind hacking attack. *Latest Trends in the Cyber-security after the Solar Wind Hacking Attack, 1*(2), 14-24.

Al-Farsi, S., Rathore, M.M. & Bakiras, S. (2021). Security of blockchain-based supply chain management systems: Challenges and opportunities. *Applied Sciences, 11*(12), 5585

Blagden, D. (2020). Deterring cyber coercion: The exaggerated problem of attribution. *Survival, 62*(1), 131–48

Cavelty, M.D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science & Engineering Ethíc, 20*(3), 701-712.

Coco, A., Dias, T. & Van Benthem, T. (2022). Illegal: The SolarWinds hack under international law. *European Journal of International Law, 33*(4), 1275– 1286

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. B. (2023). Cybersecurity Awareness and Capacities of SMEs. https://sintef.brage.unit.no/sintefxmlui/handle/11250/3056514

Georgescu, T.M. (2021). A study on how the pandemic changed the cyber-security landscape. *Informatică Economică, 25*(1), 42–60.

Kendzierskyj, S., Jahankhani, H., Jamal, A., Hussien, O., & Yang, L. (2023). The Role of Blockchain with a Cybersecurity Maturity Model in the Governance of Higher Education Supply Chains. In AI, Blockchain and Self-Sovereign Identity in Higher Education (pp.

135). Cham: Springer Nature Switzerland. https://link.springer.com/chapter/10.1007/978-3-031-33627-0_1

Latif, M. N. A., Aziz, N. A. A., Hussin, N. S. N., & Aziz, Z. A. (2021). Cyber security in supply chain management: A systematic review. LogForum, 17(1), 49-57. https://www.sciencedirect.com/science/article/pii/S1366554520308590

Lazarovitz, L. (2021). Deconstructing the SolarWinds breach. *Computer Fraud & Security, 6*(1), 17–19.

Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., & Kalogiannis, G. (2021). Cybersecurity in ICT supply chains: key challenges and a relevant architecture. Sensors, 21(18), 6057. https://www.mdpi.com/1424-8220/21/18/6057

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. International Journal of Production Research, 60(1), 162-183. https://www.tandfonline.com/doi/abs/10.1080/00207543.2021.1984606

Ofori, A., et al. (2021) Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access, 99*, 1-11 .

Parker, S., Wu, Z., & Christofides, P. D. (2023). Cybersecurity in process control, operations, and supply chain. Computers & Chemical Engineering, 108169. https://www.sciencedirect.com/science/article/abs/pii/S0098135423000388

Shukla, M., Sarmah, S. P., & Tiwari, M. K. (2023). A multi-objective framework for identifying and optimizing factors affecting cybersecurity in the Industry 4.0 supply chain. International Journal of Production Research, 61(15), 5266-5281. https://www.tandfonline.com/doi/abs/10.1080/00207543.2022.2100840

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions, and future directions. Electronics, 9(11), 1864. https://www.mdpi.com/2079-9292/9/11/1864

Willett, M. (2021). Lessons of the SolarWinds hack. *Survival*, *63*(2), 7-26