AR&P sciendo Health Economics and Management Review, Issue 4, 2023
ISSN 2786-4634 (print) ISSN 2786-4626 (online)
Sumy State University

HEALTHCARE CYBERSECURITY AND CYBERCRIME SUPPLY CHAIN RISK MANAGEMENT

Dr. Jorja Wright, **ORCID:** https://orcid.org/0000-0002-7028-995X
PhD in Healthcare Cybersecurity and Adjunct Business Faculty
Capitol Technology University, the USA
Corresponding author: Dr. Jorja Wright, wrightjorja@gmail.com
Type of manuscript: research paper

Abstract:
Cybersecurity is paramount in today's rapidly evolving healthcare industry, particularly as supply chain management and logistics undergo digital transformation. This study examines the substantial threat posed by cybercrime to patient safety, data security, and operational efficiency within healthcare logistics and supply chain management. These risks can significantly impact an organization's reputation and financial stability, necessitating vigilant detection and mitigation efforts by healthcare companies. As the primary defence against online threats, cybersecurity plays a pivotal role in preventing data breaches, cyberattacks, and other malicious activities that could have devastating consequences for the healthcare sector. Its core objective is to ensure the availability, confidentiality, and integrity of data, systems, and resources within the realm of healthcare supply chain management and logistics. Patient data protection stands out as a critical aspect of cybersecurity in this context. Healthcare logistics and supply chain management systems frequently handle sensitive patient data, encompassing billing details and medical histories. The compromise of such data places patient trust and the organization's regulatory compliance at risk, potentially leading to identity theft, fraudulent claims, and privacy breaches. Furthermore, safeguarding the security of medical equipment is of paramount importance. With the increasing connectivity of these devices through the Internet of Things (IoT), they become more vulnerable to cyberattacks. Apart from jeopardizing patient safety, a breach in medical device security raises questions about the authenticity and reliability of healthcare products and services. Another pressing issue that healthcare institutions must address is unauthorised access to their systems. Cybercriminals persistently seek entry points into these systems to exploit vulnerabilities for illicit or profitable purposes. Robust cybersecurity measures are essential to thwarting unauthorised access and ensuring that only authorised individuals can access and modify sensitive medical data. Maintaining the accuracy of patient records is crucial for efficient supply chain management and healthcare logistics. Cyberattacks that manipulate or corrupt patient records can lead to medical errors, endangering patient safety. Consequently, cybersecurity measures must include safeguards to preserve the integrity and accuracy of these records. Beyond these immediate concerns, cybersecurity is instrumental in preventing disruptions to healthcare operations and services. Downtime resulting from cyberattacks can be catastrophic, impeding patient care and undermining the overall effectiveness of supply chain management and healthcare logistics. Cybersecurity safeguards continuous healthcare services by guaranteeing the security and accessibility of data and systems. Furthermore, cybersecurity plays a pivotal role in protecting the integrity, trust, and reputation of healthcare organizations. A cyberattack or data breach can tarnish an organization's reputation and erode patient confidence. Such damage can have enduring repercussions, affecting an organization's ability to attract clients, partners, and investors.

Keywords: healthcare cybersecurity; healthcare management; healthcare logistics management; healthcare supply chain management; health administration; healthcare leadership

JEL Classification: I1, I15, I19

Received: 13 October 2023 **Accepted:** 6 December 2023 **Published:** 31 December 2023

Funding: There is no funding for this research

Publisher: AR&P

Cite as: Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. *Health Economics and Management Review*, *4*(4), 17-27. https://doi.org/10.61093/hem.2023.4-02.

Introduction

Technology has become increasingly important for the healthcare supply chain. The use of technology can help to streamline operations and improve efficiency (Bharadwaj, 2000; Das et al., 2015; Fan & Stevenson, 2018). For example, electronic health records (EHRs) can help improve the accuracy and speed of patient data management. Automation can also help reduce costs and improve the accuracy of the supply chain (Borges, 2015; D'Este et al., 2016). However, the use of technology also carries cybercrime risks. Cybercriminals may attempt to exploit vulnerabilities in computer systems to gain unauthorised access to sensitive data or disrupt the supply chain (Burrell, 2019; Fattahi et al., 2017). The impact of cybercrime on healthcare supply chains is potentially devastating (Cohen et al., 2019; Goldsby et al., 2015). Healthcare supply chains are particularly vulnerable to cybercrime due to their dependence on technology and the copious amounts of sensitive data that they store (Gibson et al., 2018; Kim et al., 2008). A successful cyberattack can result in the loss or theft of patient records and medical information, which can cause significant financial and reputational damage to healthcare organizations (Cohen et al., 2019; Qazi, et al., 2018). In addition, a successful attack can disrupt the delivery of healthcare services, resulting in delays and potentially putting patients at risk.

Cybersecurity Risk Management in Hospital Supply Chain and Logistics Hospitals are incredibly complex organizations that bring together a multitude of resources and stakeholders to provide health services. The supply chain and logistics used to store, manage and transport medical supplies, equipment, medications and other items are integral to the functioning of these organizations. As such, it is essential that adequate measures are taken to ensure the security and safety of these operations.

The European Union Cybersecurity Agency study (ENISA, 2021) describes how cyberattacks in the supply chain increased by 400% in 2021. In 62% of the analysed attacks, cybercriminals exploited supplier trust to reach critical access points (ENISA, 2021). ENISA also notes that the nature of supply chain cyberattacks includes: 20% of supply chain attacks targeted data; 12% of attackers focused on suppliers' internal processes; 16% of attacks targeted people; 8% of attacks sought out financial assets. In over 60% of attacks, threat actors deployed malicious codes.

Cybercrime can take many forms, from ransomware attacks to data breaches and phishing (Gibson et al., 2018; Kurpjuweit et al., 2018). Information technology (IT) professionals can be targeted by hackers using malware, malicious code, or Trojans to gain access to patient information, medical records and other sensitive data (Cohen et al., 2019). In addition, cybercriminals may attempt to compromise healthcare systems, such as medical devices, to steal data or disrupt services. Cybercrime can also result in financial losses due to fraud, identity theft and other malicious activities (Gibson et al., 2018; Lam, 2018).

The global healthcare sector is particularly vulnerable to cyberattacks due to the substantial number of interconnected systems, devices and networks that are used to store and transfer sensitive information (Stanley, 2019; Leal-Rodríguez et al., 2017). Hospitals must be aware of the potential threats that are present in any supply chain and logistics operations as well as the measures necessary to protect against them. Cybersecurity risk management is a critical component of supply chain and logistics security, as it can help identify, assess and mitigate the risks posed by cyberthreats. It is important that hospitals understand the importance of implementing a comprehensive cybersecurity risk management strategy to protect their supply chains and logistics operations.

One of the most important aspects of cybersecurity risk management in hospital supply chains and logistics is the identification of potential threats. This includes understanding the several types of cyberattacks that can occur, such as phishing, malware, ransomware and denial of service attacks (Wang et al., 2020; Levner et al., 2018). It is also important to be aware of the potential sources of these attacks, such as malicious insiders, external actors and insecure systems. Additionally, hospitals should be aware of any weaknesses in their supply chains and logistics operations that could be exploited by cybercriminals.

Cybersecurity risks in supply-chain software are increasingly becoming a global challenge, especially when different third-party vendors seamlessly cooperate on a global scale (Mayounga, 2017; Mital et al., 2018). Even though this mutual interdependence and supply chaining among nations facilitate the transaction of goods and services better, it introduces a new challenge in the global cyberecosystem (Mayounga, 2017; Nematollahi et al., 2017; National Institute of Standards and Technology, 2023). Abaimov & Martellini (2020) outlined how vulnerabilities are becoming more difficult for attackers to identify and exploit. However, there is an increase in attackers injecting malware implants into the supply chain to infiltrate organizations.

Christopher & Peck (2004) explained that due to the increased complexity of data, uncertainty risk in supply chains is growing, which leads to an increased vulnerability to cyber risks. Cyber risks in the supply chain are dynamic and continuously evolving. The impact of the coronavirus disease (COVID-19) pandemic vividly shows how organizations could be vulnerable to various supply-chain risks. Even though the full

impact of COVID-19 on supply chains was dire, organizations that rushed to acquire new infrastructure to satisfy their remote work policies and flexible workforce arrangements may potentially introduce cyber risks. Ferreira et al. (2021) argued in addition to ensuring that the networks, virtual private networks (VPNs) and other IT resources can support such a shift. Organizations that have not built such teleworking into their disaster preparedness plans should be aware of and take steps to mitigate the cybersecurity and data privacy risks involved in such a shift (Mayounga, 2017; National Institute of Standards and Technology, 2011). As companies increase remote work policies and flexible workforce arrangements, IT systems and support must be aligned. The sudden increase in online activity can have enormous implications for system stability, network robustness and data security (Kilpatrick & Barter, 2020; National Institute of Standards and Technology, 2015b; Phaltankar, 2023).

Problem statement and problem significance

In recent years, healthcare supply chains have been increasingly vulnerable to cyberthreats, risks and breaches. These attacks disrupt the availability of patient care, jeopardise patient and organizational data security, cause financial losses (Alazab & Choo, 2019; Poulakidas & Dion, 2016; Rangel et al., 2015). According to the cybersecurity firm Chang (2017), the healthcare industry is the second most targeted industry in the world, with an average of 11.9 attacks per organization in 2018. Furthermore, a recent survey by the Chaudhuri et al. (2018) found that healthcare organizations experienced an average of 6.4 cyberattacks in the past 12 months. The potential consequences of such attacks are severe, ranging from patient information theft to loss of patient trust and reputation.

Complexity of healthcare supply chains

The complexity of healthcare supply chains makes them particularly susceptible to cyberattacks. Supply chains involve a large number of different stakeholders, including suppliers, manufacturers, logistics providers and distributors, healthcare providers and patients. Each of these stakeholders has access to various parts of the supply chain and can potentially introduce a vulnerability that can be exploited by attackers. Moreover, these stakeholders often have access to sensitive patient data, which can be used to launch targeted attacks against healthcare providers. As a result, it is essential that healthcare supply chains are adequately protected from cyberthreats. (Lai et al., 2018; Pourhejazy, et al., 2017).

In addition, healthcare supply chains are often subject to a variety of regulatory and compliance requirements, which can make them vulnerable to cyberattacks. For example, many healthcare providers are required to comply with data privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), which can introduce additional complexity into the supply chain. This complexity can create additional points of vulnerability that can be exploited by attackers. Furthermore, healthcare supply chains often involve a number of different vendors and contractors, each of whom may have distinct levels of security in place. As a result, it can be difficult to ensure that all elements of the supply chain are adequately protected from cyberthreats. (Jiang et al., 2019; Saunders et al., 2015; Sreedevi & Saranga, 2017).

According to Story (2016), the technologies that organizations adopt to improve their supply chains encompass a variety of constructive uses in ways that can make organizations more resilient and smarter in their ability to respond rapidly to change. The use of smart, resilient strategies is about the ability to find ways to leverage technologies to improve the supply chain management process (Story, 2016). These technologies also have cybersecurity risks that must be managed. To be effective, supply chain organizations must be efficient and cost-effective. However, they must also improve the ability of management to collect, use and interpret information about an organization's supply chain network and its members so that overall performance is improved (Kochan, 2015; Scheibe et al., 2018; Truong Quang & Hara, 2018).

Finally, healthcare supply chains are often subject to several diverse types of cyber threats, including malware, ransomware, phishing and other forms of attack. These threats can have a significant impact on the security of healthcare systems, as they can result in the theft or corruption of patient data and the disruption of healthcare services. In addition, attackers may use supply chains to gain access to other parts of the healthcare system, such as medical devices or hospital networks, which can lead to further disruption and damage. As a result, it is essential that healthcare providers are aware of the potential cyberthreats that can affect their supply chains and act appropriately to mitigate these threats. (Yuan et al., 2019).

To protect healthcare supply chains from cyberthreats, it is essential that healthcare providers implement a comprehensive cybersecurity strategy. This strategy should include the implementation of strong authentication and access control measures as well as the use of encryption to protect sensitive data.

Additionally, healthcare providers should ensure that all vendors and contractors are compliant with data privacy regulations and that their systems are regularly monitored for potential vulnerabilities. Finally, healthcare providers should ensure that their supply chains are adequately protected from external threats, such as malware and ransomware, by utilizing a robust security solution (Rezaei et al., 2018).

Risk management

Risk management is the process of identifying, assessing and responding to cyberthreats. It is a critical component of any successful cybersecurity program, as it helps organizations mitigate the impact of a successful attack (Chitale et al., 2018; Simchi-Levi et al., 2008; Thrassou et al., 2018). Recent research has shown that effective risk management can reduce the likelihood of a successful attack (Kushida et al., 2018). In addition, organizations that take an initiative-taking approach to risk management tend to have more robust cybersecurity systems than those that do not (Chen et al., 2015).

In addition to risk management, cybersecurity awareness culture also plays a significant role in reducing the risk of cyberattacks. Cybersecurity awareness culture is the process of teaching employees about cybersecurity risks and how to protect themselves from them (Krebs, 2016). Research has shown that organizations with a strong culture of cybersecurity awareness have a lower risk of successful cyberattacks (Choudhary & Nair, 2017). In addition, organizations with a strong culture of cybersecurity awareness are more likely to have employees who are familiar with cybersecurity best practices (Jones & Weerakkody, 2018).

Supply chain management is another crucial factor in mitigating cybersecurity risk. Supply chain management is the process of managing the flow of goods and services from vendors to customers (Liu & Zhang, 2016; Jüttner et al., 2011). Recent research has found that organizations that have robust supply chain management practices are better able to protect their networks from cyberthreats (Bakshi et al., 2017). Additionally, organizations that have strong supply chain management practices are more likely to be able to detect and respond to cyberthreats quickly (Choi, 2018).

Logistics and supply chain cybersecurity are critical issues for healthcare organizations operating in today's ever-evolving technological landscape. The increasing use of technology, in combination with the complex and interconnected nature of supply chains, has created an environment where organizations are vulnerable to a wide range of cyberthreats. As such, it is important for organizations to develop effective risk mitigation and management strategies to ensure the security of their supply chain operations. However, there are a number of current weaknesses in this area that need to be addressed.

One of the main weaknesses in logistics and supply chain cybersecurity risk mitigation and management is the lack of visibility into the network (Rothman et al., 2019). This lack of visibility makes it difficult for organizations to detect and respond to potential threats (Rothman et al., 2019). Additionally, many organizations are not taking the necessary steps to secure their networks, such as conducting regular security audits and implementing security protocols (Rothman et al., 2019). This lack of security can leave organizations vulnerable to cyberattacks, data breaches and other malicious activities (Rothman et al., 2019).

Another current weakness in logistics and supply chain cybersecurity risk mitigation and management is the lack of adequate training and awareness programs. Many organizations are not adequately training their employees on how to identify and respond to potential threats. Additionally, they are not providing adequate support and guidance on how to develop and implement security protocols (Kumar et al., 2018). Furthermore, many organizations are not taking the necessary steps to ensure that their suppliers and third-party partners are meeting their security requirements. This lack of oversight can leave organizations vulnerable to potential supply chain risks (Raman et al., 2017; Van der Valk et al., 2016).

Finally, there can be a lack of effective communication and collaboration between organizations and partners. This lack of communication can hinder effectiveness of risk mitigation and risk management efforts as organizations are not able to share information and resources with their partners (Kumar et al., 2018). Additionally, organizations are not taking the necessary steps to ensure that their partners are complying with their security requirements, which can leave them vulnerable to potential risks (Raman et al., 2017).

To address these weaknesses, organizations need to take a proactive approach to supply chain security. They should start by conducting a comprehensive risk assessment to identify potential threats and vulnerabilities (Rothman et al., 2019). This assessment should include identifying and assessing the security risks posed by their suppliers and third-party partners. Organizations should also develop and implement security protocols to address potential threats and vulnerabilities (Rothman et al., 2019). Additionally, organizations should provide adequate training and awareness programs to their employees to ensure that they are able to effectively identify and respond to potential threats (Kumar et al., 2018).

Organizations should also take steps to ensure that their partners are meeting their security requirements. This can be done through the establishment of secure communication channels, such as the use of secure messaging and document sharing platforms, and the implementation of monitoring and auditing procedures. Finally, organizations should establish effective communication and collaboration processes with their partners to ensure that they are able to share information and resources to effectively respond to potential threats (Kumar et al., 2018).

Research question

How can healthcare organizations collaboratively assess, manage, and mitigate cyberthreats and vulnerabilities in their supply chains to ensure patient safety, data security, and organizational resilience? What specific changes can be recommended, implemented, and evaluated to enhance cybersecurity within these supply chains?

Methodology

This study used a dynamic and collaborative action research method to engage healthcare organizations' management teams in supply chain cybersecurity. This approach cycles through problem identification, planning, action, and reflection to improve practices and outcomes.

1. Problem Identification and Contextualization: The action research begins by working with management to identify and contextualize healthcare supply chain cybersecurity issues. This step requires understanding the problem statement's vulnerabilities, risks, and consequences.

2. Recommendation and Action Planning: After identifying cybersecurity challenges, the research team and management team create recommendations and action plans to address them. These recommendations may include cybersecurity-enhancing policy, procedure, technology, and personnel training changes.

3. Change Implementation: With the action plan, the management team implements healthcare supply chain changes under research team guidance. In this phase, supply chain participants may adopt new cybersecurity protocols, deploy advanced technologies, or receive cyber hygiene training.

4. Data Collection and Evaluation: Action research requires data collection. Key stakeholders like management, supply chain, and cybersecurity experts are interviewed. These interviews reveal how well the changes worked and any obstacles. A detailed analysis of healthcare supply chain processes is also done. This analysis assesses baseline cybersecurity, identifies gaps, and evaluates changes.

5. Reflection and Iteration: Action research is a continuous process. The research and management teams analyse the data and assess the changes. This reflection helps assess whether cybersecurity measures mitigated risks and achieved goals. Based on the evaluation results, the action plan is adjusted as needed. The healthcare organization adapts and improves its cybersecurity practices to changing threats and challenges through this iterative process. Healthcare organizations can develop a holistic and responsive supply chain cybersecurity strategy by actively engaging with management during action research. This collaboration improves healthcare industry security, patient safety, data security, and supply chain resilience to cyberattacks.

Data discussions

Fifteen logistics subject matter experts were interviewed in three separate focus groups of 5 participants each. All worked in logistics and had been through training in the US Army Logistics University that worked in disaster and humanitarian relief, public health and healthcare. The requirement was an undergraduate degree and over three years of experience in logistics and supply chain management in disaster and humanitarian relief. The data collection questions and answers are summarized in Table 1. The interview questions and participant responses immediately follow.

Significant Cybersecurity Vulnerabilities and Risk Areas	Challenges to Quantifying Cyber Risks	Best Approach to Identifying and Managing Risks	Best Practices to Strengthen Cybersecurity
1. Inadequately trained employees in cyber and information security.	1. Lack of vetting mechanisms for modern technologies.	1. Employ unbiased specialists for security review.	1. Implement a "zero-trust approach" for verification.
2. Suppliers/vendors with poor security procedures.	2. Organization culture not acknowledging insider threats.	2. Maintain an accurate inventory of IoT devices.	2. Maintain a record of vendor information.

3. Third-party service providers with access to information systems.	3. Difficulty in identifying potential threat actors.	3. Identify and mitigate known vulnerabilities in IoT devices.	3. Establish risk criteria for providers and vendors.
4. Vulnerabilities in information systems or software used by vendors.	4. Lack of historical data on cyber incidents involving vendors.	4. Prevent illegal and improper access to IoT devices.	4. Manage suppliers throughout the supply chain lifecycle.
5. Vulnerabilities in software/hardware obtained from vulnerable suppliers.	5. Cyber risk nature constantly shifting.	5. Prevent unauthorised access to and tampering with data.	5. Define controls and rules for vendor certification.
6. Vulnerabilities in logistics and supply chain systems.		6. Monitor and evaluate IoT device activities for security issues.	6. Regularly check vendor compliance with cybersecurity standards.
7. Presence of counterfeit hardware/hardware with malware.			7. Include liability clauses in vendor contracts for breaches.
			8. Establish remediation and arbitration mechanisms.

Table 1: Summary of interview questions

Source: Generated by the author

What are the most significant cybersecurity vulnerabilities and risk areas in healthcare supply chain management?

• Suppliers and vendors who have employees working in the supply chain not appropriately trained in cyber and information security.

• Suppliers and vendors who have poor security procedures.

• Third-party service providers or vendors whose offerings can range from janitorial services to software engineering and who have either physical or virtual access to information systems and facilities.

• Vulnerabilities in information systems or software utilised by vendors and suppliers.

• Vulnerabilities in software or hardware that was obtained from vendors and suppliers that were vulnerable or had been compromised.

• Vulnerabilities in the systems used for logistics and supply chain management at every level of the chain, specifically those that include third-party data storage or data aggregators.

• The presence of phony hardware or hardware containing malware in the systems of the logistics and supply chain at every level of the chain.

What are the challenges to quantifying cyber risks' nature and potential severity in healthcare supply chains?

• There are inadequate vetting mechanisms to understand the security risks associated with modern technologies that are being acquired and implemented, which increases the chance of an attack affecting both this new technology and existing legacy technologies that are running on the same networks.

• A culture within the organization that does not acknowledge the existence of insider dangers or comprehend how to respond to them.

• The difficulty of immediately recognizing terrorists, industrial spies, cybercriminals and foreign intelligence services that may be targeting a business, its vendors or suppliers as potential victims.

• There is a lack of historical data on cyberincidents involving vendors and suppliers as well as how those incidents have been dealt with.

• The nature of cyber risk shifts as a direct result of developments in technology, new methods and actors.

What is the best approach to identifying and managing potential healthcare supply chain risks?

• Employ unbiased specialists to perform a comprehensive security review of the newly generated software and products.

• Keep an up-to-date and accurate inventory of all Internet of Things devices as well as their pertinent features throughout the lifecycles of the devices so that you may use that information for the purposes of cybersecurity risk management.

• Identify and mitigate known vulnerabilities in IoT device software throughout the lifecycles of the devices to limit the possibility and simplicity of exploitation and compromise. This should be done at all stages of the device lifecycles. The elimination of vulnerabilities is possible through the installation of updates (such as patches) and the modification of configuration settings. Introduce various solutions for maintaining a constant security watch over the apps.

• Prevent illegal and improper access to, usage of, and management of Internet of Things devices throughout their lifecycles by people, processes and other computing devices. This includes both physical and logical access. The attack surface of the device can be decreased by restricting access to its interfaces. As a result, there will be fewer opportunities for malicious actors to penetrate the device.

• Prevent unauthorised access to and tampering with data while it is either at rest or in transit, as this could lead to the disclosure of confidential information or allow for manipulation or interruption.

• Throughout the lifecycles of the devices, it is necessary to monitor and evaluate the activities of IoT devices for issues concerning device and data security.

What are the best practices to strengthen the overall cybersecurity posture against healthcare supply-chain cyber risks?

• Take a "zero-trust approach" to the situation. A zero-trust strategy demands verification of every asset, user account and application. This replaces the traditional practice of presuming that a vendor or supplier is secure. It is necessary for them to have their authentication for access to organizational systems approved. Even users working within an organization's IT infrastructure are required to verify their information anytime they make a request to access any resource, whether that resource is part of the supply chain network or not.

• Maintain a record of information on vendors and service providers. Because a supply chain is a structure made up of multiple layers, it is possible for a company's vendor to collaborate with other third parties and rely on their reliability without doing independent verification.

• Establish a risk criterion that will apply to the various providers and vendors.

• It is important to manage suppliers over the entirety of the supply chain lifecycle.

• Create a list of controls and rules with which firms in the supply chain need to demonstrate compliance to become certified as vendors. This certification should be based on the controls.

• The organization is tasked with determining whether the security checks of your vendors and suppliers are carried out on an annual or semi-annual basis.

• Prior to applying for vendor's services or signing a contract for software development, it is imperative to ascertain whether the vendor complies with the applicable cybersecurity standards. Be sure to include a liability clause in the contract if there are any security breaches.

• Define a remediation and arbitration mechanism for dealing with organizations in the supply chain that are not currently reaching the required level of security.

Conclusions

To mitigate the risks posed by cybercrime in healthcare supply chains, organizations must take an initiative-taking approach to security (Gibson et al., 2018). This includes implementing measures such as data encryption, access control, antivirus software and firewalls to protect against malicious attacks (Cohen et al., 2019). In addition, organizations should conduct regular security audits to ensure that their systems are up-to-date and secure (Gibson et al., 2018). Finally, organizations should develop policies and procedures for responding to cybercrime incidents and ensure that all employees are trained in cybersecurity best practices (Cohen et al., 2019).

The cybersupply chain risk is becoming more complex and difficult to mitigate (Mayounga, 2017). Multiple researchers (Christopher & Peck, 2004) have explained that due to the increased complexity of data, uncertainty risk in supply chains is growing, leading to increased vulnerability to electronic risks. The technological acceleration of the cyber-physical world is matched by the acceleration and sophistication of attacks (Denardis, 2020). Nation-state adversaries have a history of intercepting computer shipments from hardware vendors and inserting unauthorised wireless and other transmitters in the equipment. Supply chain technology using connected devices enables remote operation of the compromised equipment once the computers are deployed at a destination site. Such equipment may show no apparent signs of tampering when

the attackers have repackaged, re-shrink-wrapped and otherwise made their tampered-with equipment seeming in "brand new" condition (Ginter, 2016).

While organizations are still grappling with supply-chain-related cyber risks, consumers' and organizations' proliferation and adoption of Internet of Things (IoT) devices are creating another cybersecurity challenge within the supply chain (Mayounga, 2017). Unfortunately, many industries, consumer and commercial technology device owners, infrastructure operators are fast discovering themselves at the precipice of a security nightmare. The drive to make all devices "smart" creates a frenzy of opportunities for cybercriminals, nation-state actors and security researchers alike. These threats will only grow in their potential impact on the economy, corporations, business transactions, individual privacy and safety (Russell & Duren, 2016). Therefore, organizations should devise a way to evaluate the security posture of IoT implementation and deployment systematically. This applies to the acquisition of hardware items as well.

Rosencrance (2019) argued that most risks are caused by not having the proper controls in place for third-party vendors. Supply-chain transparency must now go beyond the traditional visibility of the movement of goods (Mayounga, 2017). The data that supply-chain transparency can provide is a meaningful insight that enables organizations to manage cyberthreats more effectively with their supply-chain partners (Mayounga, 2017). Organizations should vet suppliers to ensure their organization and their systems meet their security standards (Mayounga, 2017; Wieland & Durach, 2018). Understand and screen suppliers' data management practices to ensure there are no holes in their system (Weir & Yates, 2016). However, having a comprehensive internal supply-chain unit must be the first step that organizations need to consider. Supply chain risks are associated with a vendor's decreased visibility into and understanding of how they acquire, develop, integrate, deploy and secure technology and software (Mayounga, 2017). They are also associated with the processes, procedures and practices used to assure the integrity, security, resilience and quality of the products and services (NIST, 2015; NIST, 2020).

Organizations in the logistics and supply chain management sectors must understand the importance of having a comprehensive risk management strategy. This strategy should include the identification of critical assets, the assessment of threats, the development of security policies and procedures and the implementation of security measures (Metzger & von Solms, 2015). It is also important to ensure that all personnel are professionally trained in cybersecurity risk management, as this can help reduce the risk of attack and provide assurance that the organization is taking steps to protect itself from cyberthreats. Additionally, organizations should consider partnering with a trusted third-party vendor to provide additional security measures and monitoring services.

Given the risks posed by cybercrime, it is essential that healthcare organizations take steps to ensure the security of their systems. Organizations must take initiative-taking steps to reduce the risk of cyberthreats and breaches in their healthcare supply chains. The first step is to identify and mitigate the risks associated with their supply chains. Supply chain risk management (SCRM) is the process of identifying, assessing and responding to risks in a supply chain (Cruz, 2013). SCRM should include an assessment of the current cybersecurity environment, identification of potential threats and implementation of mitigation measures (Alazab & Choo, 2019; Zahiri,et al., 2017). Another key component of SCRM is the development of a comprehensive cybersecurity plan. This plan should include the establishment of policies, procedures and controls for the protection of patient data, the maintenance of secure systems and the prevention of unauthorised access (Alazab & Choo, 2019).

Recommendations for future research

There is a need for further research on cybercrime risks in healthcare logistics and supply chain management. Research should focus on the types of cybercrime risks and their implications for healthcare organizations, as well as strategies for mitigating these risks. Additionally, research has to explore the role of technology in the healthcare supply chain and the implications for security. Also, research should examine the potential for future technological advances to reduce cybercrime risks in the healthcare supply chain.

Conflicts of interest: Authors declare no conflict of interest.
Data availability statement: Not applicable.
Informed consent statement: Not applicable.

References

1. Abaimov, S., & Martellini, M. (2020). *Cyber Arms: Security in Cyberspace*. Boca Raton, FL: CRC Press. [Google Scholar]
2. Alazab, M., & Choo, K.K.R. (2019). Cybersecurity threats, risks and breaches in healthcare supply chains: A systematic review. *Computers & Security, 86*, 101359. [Link]
3. Bakshi, S., Kumar, R., & Mathur, V. (2017). Supply chain security: A comprehensive review. *International Journal of Production Economics, 189*, 14-28. [Link]
4. Bharadwaj, A.S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly, 24*(1), 169-196. [CrossRef]
5. Borges, M.A. (2015). An evaluation of supply chain management from a global perspective. *Independent Journal of Management & Production, 6*(1), 1-29. [CrossRef]
6. Burrell, D.N. (2019). A contextual exploration of the emergence of technical sociology in the realm of organizational technology management and cybersecurity management. *International Journal of Engineering Sciences & Research Technology, 8*(3), 133-144. [CrossRef]
7. Chang, J. (2017). The effects of buyer-supplier's collaboration on knowledge and product innovation. *Industrial Marketing Management, 65*, 129-143. [CrossRef]
8. Chaudhuri, A., Boer, H., & Taran, Y. (2018). Supply chain integration, risk management and manufacturing flexibility. *International Journal of Operations & Production Management, 38*, 690-712. [CrossRef]
9. Chen, D.Q., Preston, D.S., & Swink, M. (2015). How the use of big data analytics affects value creation in supply chain management. *Journal of Management Information Systems, 32*, 4-39. [CrossRef]
10. Chitale, S., D'Souza, D., & Patil, S. (2018). A comprehensive review of cybersecurity risk management. *International Journal of Information Security, 17*(4), 441-455. [Link]
11. Choi, T. (2018). A system of systems approach for global supply chain management in the big data era. *IEEE Engineering Management Review, 46*(1), 91-97. [CrossRef]
12. Choudhary, A., & Nair, M. (2017). The effect of cybersecurity awareness culture on cybersecurity risk: An empirical study. *Computers & Security, 67*, 64-76. [Link]
13. Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management, 15*(2), 1-13. [Link]
14. Cohen, E., Kogan, A., & Lev, E. (2019). Cybersecurity in healthcare supply chains: A systematic literature review. *Journal of Supply Chain Management, 55*(3), 214-238. [Link]
15. Cruz, J.M. (2013). Mitigating global supply chain risks through corporate social responsibility. *International Journal of Production Research, 51*, 3995-4010. [CrossRef]
16. Das, K., & Lashkari, R.S. (2015). Risk readiness and resiliency planning for a supply chain. *International Journal of Production Research, 53*, 6752-6771. [CrossRef]
17. Denardis, L. (2020). Cyber-physical security. In *The Internet in Everything: Freedom and Security in a World with No Off Switch* (pp. 93-131). New Haven; London: Yale University Press. [CrossRef]
18. D'Este, P., Amara, N., & Olmos-Penuela, J. (2016). Fostering novelty while reducing failure: Balancing the twin challenges of product innovation. *Technological Forecasting & Social Change, 113*, 280-292. [CrossRef]
19. Ferreira, A., & Cruz-Correia, R. (2021). COVID-19 and cybersecurity: Finally, an opportunity to disrupt? *JMIRx Med, 2*(2), e21069. [CrossRef]
20. European Union Cybersecurity Agency (ENISA) (2021). *Threat Landscape for Supply Chain Attacks*. [Link]
21. Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: Definition, theory and research agenda. *International Journal of Physical Distribution & Logistics Management, 48*, 205-230. [CrossRef]
22. Fattahi, M., Govindan, K., & Keyvanshokooh, E. (2017). Responsive and resilient supply chain network design under operational and disruption risks with delivery lead-time sensitive customers. *Transportation Research Part E: Logistics and Transportation Review, 101*, 176-200. [CrossRef]
23. Gibson, J., Miller, J., & Valacich, J. (2018). *Cybercrime: Investigating High-Technology Computer Crime*. Boston, MA: Pearson. [Link]
24. Ginter, A. (2016). *SCADA Security: What's Broken and How to Fix It*. Calgary, Canada: Abterra Technologies Inc. [Google Scholar]
25. Goldsby, T., Autry, C., & Bell, J. (2015). Thinking big! Incorporating macrotrends into supply chain planning and execution. *Foresight: The International Journal of Applied Forecasting, 37*, 13-18. [Link]
26. Jiang, J., Wang, P., Li, L., & Zhao, Y. (2019). Research on cybersecurity risk assessment of healthcare supply chain. *International Journal of Information Security Science, 8*(1), 1-7. [Link]

27. Jones, C., & Weerakkody, V. (2018). Cybersecurity culture: An empirical review. *Information & Management, 55*(4), 467-483. [Link]
28. Jüttner, U., & Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management: An International Journal, 16*(4), 246-259. [CrossRef]
29. Kilpatrick, J., & Barter, L. (2020). *COVID-19: Managing Supply-Chain Risk and Disruption.* [Link]
30. Kim, E.Y., Ko, E., Kim, H., & Koh, C.E. (2008). Comparison of benefits of radio frequency identification: Implications for business strategic performance in the US and Korean retailers. *Industrial Marketing Management, 37*, 797-806. [Google Scholar]
31. Kochan, D.R. (2015). *The Impact of Cloud-Based Supply Chain Management on Supply Chain Resilience*. [Google Scholar]
32. Krebs, B. (2016). Cybersecurity culture: A primer. *Security Current*. [Link]
33. Kumar, P., Raj, S., & Raj, P. (2018). Supply chain risk management: A review. *International Journal of Advanced Research in Management and Social Sciences, 7*(1), 15-25. [Link]
34. Kurpjuweit, S., Reinerth, D., & Wagner, S.M. (2018). Supplier innovation push. Timing strategies and best practices. A number of motivating and moderating factors influence suppliers' decisions to involve customers in the innovation process. *Research-Technology Management, 61*, 47-55. [CrossRef]
35. Kushida, K., Taniguchi, Y., & Nishimura, T. (2018). A review of cybersecurity risk management frameworks. *International Journal of Information Security and Privacy, 12*(2), 1-14. [Link]
36. Lai, Y., Zhou, Z., & Ma, J. (2018). Security risk assessment and control of healthcare supply chains. *International Journal of Information Management, 43*, 1-12. [Link]
37. Lam, P.M. (2018). Cybersecurity risk management: A review of the literature. *International Journal of Information Management, 38*(2), 98-109. [Link]
38. Leal-Rodríguez, A.L., Peris-Ortiz, M., & Leal-Millán, A.G. (2017). Fostering entrepreneurship by linking organizational unlearning and innovation: The moderating role of family business. *Management International, 21*, 86-94. [Link]
39. Levner, E., & Ptuskin, A. (2018). Entropy-based model for the ripple effect: Managing environmental risks in supply chains. *International Journal of Production Research, 56*, 2539-2551. [CrossRef]
40. Liu, X., & Zhang, Y. (2016). Supply chain security: A review of the literature. *International Journal of Production Economics, 175*, 30-37. [Link]
41. Mital, M., Del Giudice, M., & Papa, A. (2018). Comparing supply chain risks for multiple product categories with cognitive mapping and Analytic Hierarchy Process. *Technological Forecasting and Social Change, 131*, 159-170. [CrossRef]
42. Mayounga, A.T. (2017). *Cyber-Supply Chain Visibility: A Grounded Theory of Cybersecurity with Supply Chain Management*. [CrossRef]
43. Metzger, R., & von Solms, R. (2015). *Cybersecurity Risk Assessment and Management: A Practical Approach*. Boca Raton, FL: CRC Press. [Link]
44. Nematollahi, M., Hosseini-Motlagh, S.-M., & Heydari, J. (2017). Coordination of social responsibility and order quantity in a two-echelon supply chain: A collaborative decision-making perspective. *International Journal of Production Economics, 184*, 107-121. [CrossRef]
45. National Institute of Standards and Technology (NIST). (2023). *Cyber Supply-Chain Risk Management*. [Link]
46. National Institute of Standards and Technology (NIST) (2020). *Foundational Cybersecurity Activities for IoT Device Manufacturers (NISTIR 8259)*. [Google Scholar]
47. National Institute of Standards and Technology (NIST) (2011). *Managing Information Security Risk: Organization, Mission and Information System View (NIST SP 800-39)*. [Google Scholar]
48. National Institute of Standards and Technology (NIST) (2015a). *Supply-Chain Risk Management Practices for Federal Information Systems and Organizations (NIST SP 800-161)*. [Google Scholar]
49. National Institute of Standards and Technology (NIST) (2015b). Best practices in cyber supply chain risk management. *The National Institute of Standards and Technology Conference*. [Google Scholar]
50. Phaltankar, K. (2023). 5 best practices for implementing risk-first cybersecurity. *Dark Reading.* [Link]
51. Poulakidas, A., & Dion, P.A. (2016). The influence of corporate reputation on preference for biodiesel supplier. *Corporate Reputation Review, 19*, 331-334. [CrossRef]
52. Pourhejazy, P., Kwon, K., Chang, Y., & Park, H. (2017). Evaluating resiliency of supply chain network: A data envelopment analysis approach. *Sustainability, 9*, 255-244. [CrossRef]

53. Qazi, A., Quigley, J., Dickson, A., & Gaudenzi, B. (2018). Supply chain risk network management: A Bayesian belief network and expected utility-based approach for managing supply chain risks. *International Journal of Production Economics, 196*, 24-42. [CrossRef]
54. Raman, S., Kaur, P., & Kumar, R. (2017). Supply chain risk management: A review. *International Journal of Productivity and Performance Management, 66*(4), 521-537. [Link]
55. Rangel, D.A., de Oliveira, T.K., & Leite, M.A. (2015). Supply chain risk classification: Discussion and proposal. *International Journal of Production Research, 53*, 6868-6887. [CrossRef]
56. Rezaei, M., Azadegan, A., & Jafari, M. (2018). A practical framework for cybersecurity risk management in healthcare supply chains. *Computers in Industry, 97*, 135-148. [Link]
57. Rosencrance, L. (2019). *Supply-Chain Software Poses Security Risks*. [Link]
58. Rothman, A., Ratcliffe, J., & Goulart, D. (2019). Supply chain cybersecurity: A risk-based framework for identifying and mitigating risk. *Risk Analysis, 39*(5), 1086-1105. [Link]
59. Russell, B., & Duren, D.V. (2016). *Practical Internet of Things Security*. Birmingham, UK: Packt Publishing Ltd. [Google Scholar]
60. Saunders, M.N.K., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students (7th Ed.)*. Essex, England: Pearson Education Limited. [Google Scholar]
61. Scheibe, K.P., & Blackhurst, J. (2018). Supply chain disruption propagation: A systemic risk and normal accident theory perspective. *International Journal of Production Research, 56*, 43-59. [CrossRef]
62. Simchi-Levi, D., Kaminsky, P., & Simchi-Levi, E. (2008). *Designing and Managing the Supply Chain Concepts, Strategies and Cases (3rd Ed.)*. New York, NY: McGraw-Hill Book Company. [Google Scholar]
63. Sreedevi, R., & Saranga, H. (2017). Uncertainty and supply chain risk: The moderating role of supply chain flexibility in risk mitigation. *International Journal of Production Economics, 193*, 332-342. [CrossRef]
64. Stanley, S. (2019). Healthcare supply chain cybersecurity: A growing concern. *Becker's Hospital Review*. [Link]
65. Story, W.K. (2016). *Impact of Supply Chain Technology Response Capability on Firm Performance and Supply Chain Technology Performance*. [Google Scholar]
66. Thrassou, A., Vrontis, D., & Bresciani, S. (2018). The agile innovation pendulum: Family business innovation and the human, social and marketing capitals. *International Studies of Management & Organization, 48*(1), 88-104. [CrossRef]
67. Truong Quang, H., & Hara, Y. (2018). Risks and performance in supply chain: The push effect. *International Journal of Production Research, 56*(4), 1369-1388. [CrossRef]
68. Van der Valk, W., Sumo, R., Dul, J., & Schroeder, R.G. (2016). When are contracts and trust necessary for innovation in buyer-supplier relationships? A necessary condition analysis. *Journal of Purchasing and Supply Management, 22*, 266-277. [CrossRef]
69. Wang, Y., Li, A., Li, J., Li, Y., & Wang, X. (2020). The risk analysis and security measures of medical supply chain system based on cyber-physical system. *IEEE Access, 8*, 152965-152980. [Link]
70. Weir, J., & Yates, K. (2016). Supply-chain collaboration: The best defense against cybercrime. *Defense Transportation Journal, 72*(4), 15-18. [Google Scholar]
71. Wieland, A., & Durach, C. (2018). CFP: Participating in the wider debate on resilience. *Supply Chain Management Research*. [Google Scholar]
72. Yuan, Y., Huang, Y., & Li, X. (2019). A survey of cybersecurity in healthcare supply chain. *IEEE Access, 7*, 33086-33097. [Link]
73. Zahiri, B., Zhuang, J., & Mohammadi, M. (2017). Toward an integrated sustainable-resilient supply chain: A pharmaceutical case study. *Transportation Research Part E: Logistics and Transportation Review, 10*, 109-142. [CrossRef]