CYBER SECURITY CHALLENGES IN DIGITAL SUPPLY CHAIN MANAGEMENT: A RISK ASSESSMENT APPROACH

[1]Jiten Kumar Behera, [2]Chinmay Kaushik, [3]Harsh Solanki and [4]Dr. Mohd Shuaib
[1, 2, 3]Student, Department Of Production and Industrial Engineering, Delhi Technological University, New Delhi, India
[4]Assistant Professor, Department of Mechanical, Production and Industrial and Automobile Engineering, Delhi Technological University, New Delhi, India

ABSTRACT

In today's age of digital transformation, supply chain management (SCM) has become a networked, technology-based ecosystem. Yet with this greater dependence on digital solutions, this paper identifies several cybersecurity threats. This paper delves into the cybersecurity threats in digital supply chains and introduces a risk assessment strategy to prevent future threats. It discusses several security risks such as data breaches, ransomware attacks, insider threats, and third-party vulnerabilities. Furthermore, it also talks about current cybersecurity frameworks and suggests a more improved risk management approach specific to digital supply chains. The research identifies the importance of proactive security measures and shared risk assessment approaches in order to provide assurance for the integrity, confidentiality, and availability of digital supply chains.

Keywords: *Cybersecurity, Digital Supply Chain Management, Risk Assessment, Cyber Threats, Risk Mitigation*

1. INTRODUCTION

In today's global economy, the digital evolution of supply chain management (SCM) is a critical element in maximizing operational efficiency and competitiveness. Digital Supply Chain Management (DSCM) brings together cutting-edge technologies like the Internet of Things (IoT), cloud computing, artificial intelligence (AI), and blockchain to make processes lean and enhance supply chain visibility. Yet this burgeoning use of digital technologies has brought with it the full range of cybersecurity issues which call for inclusive risk evaluation and counter-measurements.

1.1 Evolution of Digital Supply Chain Management

The transition from legacy supply chains to DSCM has been prompted by requirements for increased responsiveness, efficiency, and agility in the face of changing market requirements. Legacy supply chains tended to be linear and silo-based, which meant they were inherently inefficient and plagued by delays. Digital technologies have changed these linear paradigms into network models that allow information to be shared in real-time and stakeholders to collaborate. For example, IoT devices allow real-time monitoring of products, making it possible to manage logistics and inventory proactively (Kaspersky 2024). Cloud computing offers scalable infrastructure for data processing and storage, facilitating easy collaboration among geographically distributed teams (NIST 2014). AI algorithms process large datasets to optimize inventory management, demand forecasting, and decision-making (SCMR 2024). Blockchain technology provides transparency and immutability in transactions, building trust among supply chain partners (WSJ 2024).

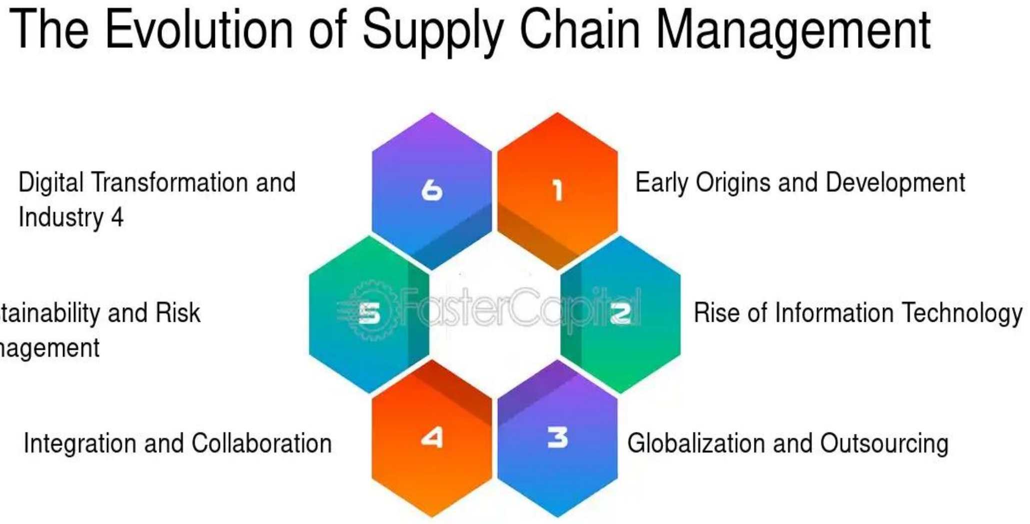

The Evolution of Supply Chain Management
1
Early Origins and Development
2
Rise of Information Technology
3
Globalization and Outsourcing
4
Integration and Collaboration
5
Sustainability and Risk Management
6
Digital Transformation and Industry 4
FasterCapital

Figure 1: Supply chain Management (Source: Faster Capital)

1.2 Cybersecurity Challenges in Digital Supply Chains

Although digitalization comes with its array of benefits, it presents supply chains to numerous cybersecurity dangers. The nature of DSCM is so intertwined that vulnerability in one will spread to every link in the entire network. The following represent the most obvious cybersecurity challenges:

- **Unauthorized Access and Data Breaches:** Confidential information, including intellectual property, customer data, and proprietary procedures, is frequently exchanged throughout the supply chain. Unauthorized access may result in data breaches, causing financial losses and reputational harm (The Sun 2024).
- **Malware and Ransomware Attacks:** Cybercriminals use malicious software to interfere with operations, encrypt vital data, and extort ransoms. These attacks can bring production lines to a standstill and cause delays in deliveries, impacting the entire supply chain (NY Post 2025).
- **Insider Threats and Human Error:** Authorized employees or contractors can consciously or unconsciously breach security protocols, causing data leaks or system vulnerabilities (NCSC 2024).
- **Third-Party and Vendor Risks:** Vendors and suppliers who do not have sufficient cybersecurity controls can be the point of entry for attackers, threatening the security of the entire supply chain (Guidepoint 2024).
- **IoT and Cloud Security Threats:** The widespread use of IoT devices and cloud computing increases the attack surface, which is difficult to protect each endpoint and data transfer channel (BSI 2024).
- **Regulatory and Compliance Challenges:** Organizations have to deal with a complex array of cybersecurity laws and standards, which may differ geographically and by industry. Non-compliance can lead to legal sanctions and loss of reputation (C-SCRM 2024).

1.3 Real-Life Events Emphasizing Cybersecurity Threats

Some notable cyber attacks have highlighted the weaknesses in online supply chains:

- **Stop & Shop Cybersecurity Incident:** In November 2024, supermarket chain Stop & Shop faced a cybersecurity incident that impacted its supply chain business, resulting in fresh produce, meat, and dairy product shortages at some locations. The attack emphasized the vulnerability of retail supply chains to cyberattacks and their ability to disrupt product availability (Bit sight 2024).
- **Morrisons Ransomware Attack:** A ransomware attack on Blue Yonder, a supply chain software provider, in late 2024 hit UK supermarket chain Morrisons, leading to fresh produce shortages. The attack interrupted Morrisons' restocking operations, highlighting the dangers of third-party software vulnerabilities (The guardian 2025).
- **Starbucks Payroll Disruption:** Starbucks experienced difficulties in its payroll and worker scheduling when its third-party software vendor, Blue Yonder, was attacked with ransomware in November 2024. Managers turned to manual methods, showing the operational disruptions caused by cyberattacks on supply partners (WSJ 2024).
- **Colonial Pipeline Ransomware Attack:** In May 2021, a ransomware attack on Colonial Pipeline resulted in a temporary shutdown of a significant fuel distribution network in the U.S., resulting in widespread fuel shortages and emphasizing the susceptibility of critical infrastructure to cyber attacks (WSJ 2025).

1.4 Significance of Risk Assessment in DSCM

With the complex cybersecurity threats, organizations need to take a proactive stance to detect, evaluate, and counter risks in their digital supply chains. An extensive risk assessment framework includes:

- **Identifying Cyber Threats:** Identifying possible threats, such as external attacks, insider threats, and third-party vulnerabilities (IoT 2024).
- **Vulnerability Analysis:** Assessing system vulnerabilities that may be targeted by cyber threats (Digital Matter 2024).
- **Impact and Likelihood Evaluation:** Determining the possible impact and likelihood of identified risks occurring (IoT 2023).
- **Risk Mitigation Plans:** Putting into effect measures to minimize the occurrence or effects of risks, i.e., implementing security controls, improving employee training, and formalizing incident response plans (Surgere 2025).

- **Continuous Monitoring:** Continual monitoring of the supply chain to detect new threats and vulnerabilities to make timely responses (NIST 2024).

Embracing proven cybersecurity frameworks, i.e., the NIST Cybersecurity Framework, can offer framework guidance for organizations trying to improve their cybersecurity stance (Wikipedia 2024).

2. CYBERSECURITY CHALLENGES IN DIGITAL SUPPLY CHAINS

2.1 Data Breaches and Unauthorized Access

Data breaches and unauthorized access are two of the biggest digital supply chain threats. Banking information, customer records, and intellectual property are accessed by hackers for business intelligence or profit (C R centre 2025). Cyberthieves break in to computer systems illegally by exploiting weaknesses in the form of phishing attacks, old software, and poor authentication methods. Identity and access management is a critical component of cybersecurity because a recent report found that stolen credentials are used in over 60% of supply chain attacks (S Group 2025).

Monetary loss, reputation loss, penalties imposed by the government, and even litigation can be the potential fallout from data breaches [P Group 2025].

Companies must have in place encryption policies, multifactor authentication, and monitoring on an ongoing basis to help prevent these threats [NIST 2022].

2.2 Ransomware and Malware Attacks

Ransomware and malware attacks are now becoming increasingly prevalent with supply chains proving to be the largest vulnerabilities as they are immensely interconnected [S. One 2025]. Ransomware is exploited by cybercrime syndicates in order to lock vital data using encryption and in exchange for paying money for the decryption key, which results in disruption of operations and loss of revenues. One of the most common examples is the 2021 Colonial Pipeline attack, causing fuel shortage across the United States as a result of a ransomware cyberattack on their supply chain [L. Group 2025]. Malware, including trojans and spyware, is also used for stealing sensitive data and to disrupt supply chain operations. Endpoint security software, regular software updates, and regular backup policies need to be utilized by organizations to avoid such attacks [G security 2025]. Use of AI-powered threat detection is also likely to enhance the chances of catching and preventing ransomware attacks before they take place [Bit Sight 2024].

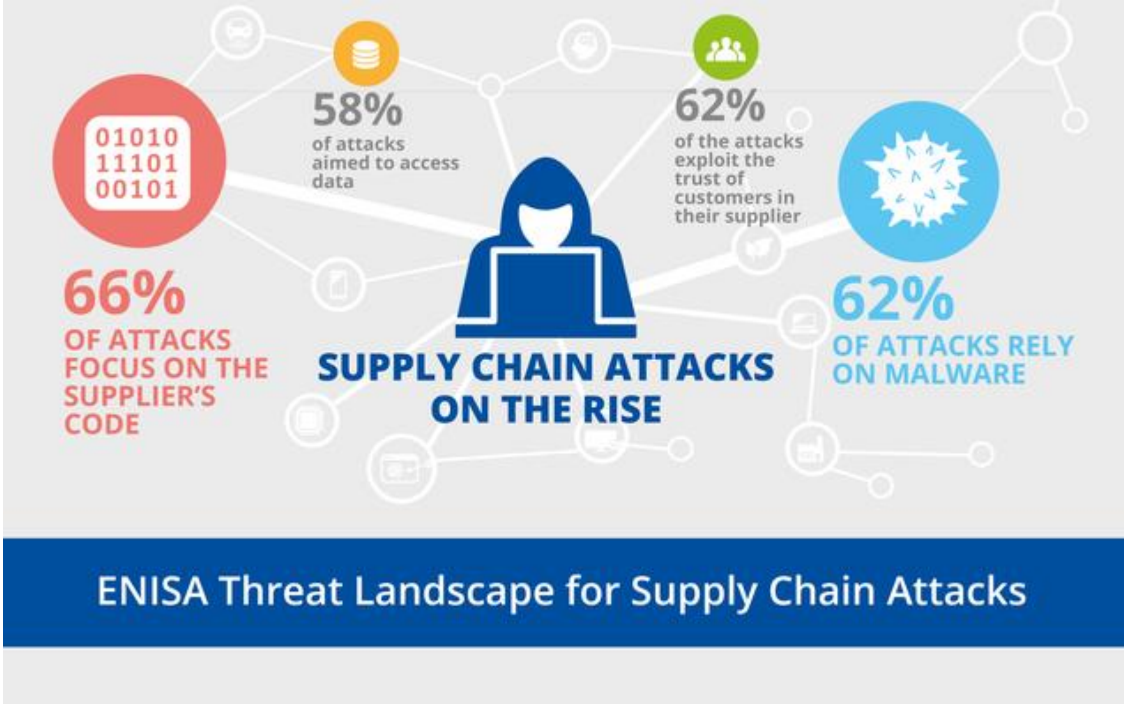


Figure 2: Supply Chain attacks on the rise (Source: ENISA 2021)

2.3 Supply Chain Integration Risks from Third-Party Digital Exposure

Modern supply chains heavily rely on a network of interconnected third-party vendors, logistics providers, cloud service platforms, and software systems for real-time data exchange and process automation. While this digital integration enhances efficiency and responsiveness, it simultaneously expands the cyber-attack surface, especially when third parties lack adequate cybersecurity frameworks [Hyperproof 2024].

A critical example is the 2013 Target breach, in which attackers gained access to the retailer's internal systems through a third-party HVAC vendor. The vendor’s weak credentials were exploited to infiltrate Target’s supply chain data, resulting in the compromise of 40 million payment records [ODNI 2024]. This incident highlights how operational dependency on external systems can expose core SCM operations to significant cyber risks.

Studies show that 60% of supply chain cyber incidents stem from vulnerable third-party systems that lack encryption, endpoint protection, or multi-factor authentication [Cybersaint 2024]. As digital SCM systems like ERP, warehouse management, and procurement portals often share access with partners, the cyber hygiene of each connected node becomes vital to end-to-end security.

To address this, organizations must adopt a zero-trust supply chain framework, enforce vendor cybersecurity compliance, and implement third-party cybersecurity SLAs (Service-Level Agreements). Tools such as vendor risk assessment platforms, continuous monitoring dashboards, and blockchain-based traceability can help secure multi-tiered vendor ecosystems and ensure supply chain integrity in the face of rising digital threats [Reuters 2024].

2.4 Supply Chain Disruption through Advanced Persistent Threats (APTs): Advanced Persistent Threats (APTs) are sophisticated, long-term cyberattacks that aim to infiltrate supply chain networks undetected, often carried out by highly skilled adversaries or state-sponsored actors (FireEye, 2025). Unlike quick-hit attacks, APTs remain hidden within a network for extended periods, collecting sensitive information, mapping infrastructure, and sometimes sabotaging critical operations. Notable incidents include the SolarWinds cyberattack, which compromised numerous U.S. government agencies and private firms through software updates (MITRE, 2024).

APTs often exploit zero-day vulnerabilities and trusted software update channels to infiltrate systems, making detection and response significantly challenging. Organizations should employ a defense-in-depth strategy, adopt threat intelligence feeds, and implement network segmentation and anomaly detection tools to identify and mitigate these advanced threats (CyberEdge, 2025).

2.5 IoT and Cloud Security Vulnerabilities

The increasing use of IoT devices and cloud computing solutions in supply chain management presents new security threats. IoT devices, which usually do not have robust security controls, can be compromised to execute cyberattacks or sabotage operations [GCHQ 2024]. In 2016, the Mirai botnet attack infected IoT devices, causing large-scale service outages across prominent websites and impacting supply chain operations worldwide [ICTS 2024]. Cloud security threats, such as misconfigurations, data leaks, and unauthorized access, also add to the complexity of supply chain cybersecurity [SCMR 2024]. To tackle these threats, businesses need to have robust authentication processes in place, network segmentation, and ongoing monitoring for IoT and cloud infrastructures [Cyberproof 2025].

2.6 Insider Threats and Human Error

Insider threats, either malicious or unintentional, are a severe threat to digital supply chains. Authorized employees, contractors, or business partners may inadvertently leak sensitive information or maliciously disrupt operations [Magazine 2025]. Research shows that almost 34% of data breaches are caused by insider threats, usually due to poor security awareness training or inadequate access controls [C-SCRM 2024]. Human fallibility, i.e., misconfiguration of cloud storage and mishare of credentials by accident, heightens the vulnerability of cybersecurity too [NIST 2024]. Firms can put rigorous control of access mechanisms, offer training for security awareness regularly, and carry out behavioural analytics for both the prevention of insider threat detection [Panorays 2024].

2.7 Compliance Challenges in Supply Chain Cybersecurity

Compliance in digital supply chains goes beyond internal governance—it requires aligning with evolving cybersecurity laws that span national borders and involve multiple partners. Supply chain managers must navigate a patchwork of regional regulations such as GDPR (EU), CMMC (USA), and ISO/IEC 27001, especially when handling data across various jurisdictions [NIST 2022]. Complex supply chain ecosystems that include global vendors, cloud-based platforms, and cross-border data exchange significantly increase the burden of compliance. Non-compliance may result in blocked shipments, import/export delays, fines, or even suspension of partnerships with compliant firms. The challenge lies in ensuring that every link in the supply chain adheres to data protection and cybersecurity standards. To address this, firms must adopt supply chain-wide compliance management systems, automate cybersecurity assessments, and maintain audit trails for traceability and accountability [Avetta 2025]. Proactive compliance not only ensures legal operation but also builds trust among supply chain partners.

2.8 Lack of Cybersecurity Talent and Skills Gap: One of the less discussed but highly impactful cybersecurity challenges in digital supply chains is the shortage of skilled cybersecurity professionals. With the increasing complexity of threats and the growing reliance on digital systems, many organizations struggle to hire and retain staff with the required technical skills and experience (ISC², 2025). A limited talent pool can lead to misconfigured security systems, slow incident response times, and inadequate risk assessments—leaving supply chains vulnerable. A global cybersecurity workforce study indicates a gap of over 3 million professionals worldwide, with supply chain cybersecurity expertise being among the rarest (Cybersecurity Ventures, 2024). To address this, companies can invest in continuous staff training, upskilling programs, cross-functional cybersecurity education, and leverage managed security service providers (MSSPs) to bridge talent shortages (PwC, 2025).

3. RISK ASSESSMENT FRAMEWORK

3.1 Cyber Threats Identification in Digital Supply Chains

Cyber threats to digital supply chains take numerous shapes, such as phishing, ransomware, data breaches, and insider threats. These threats leverage vulnerabilities in networked systems, third-party dependencies, and cloud-based systems [Avetta]. Organisations need to constantly evaluate probable cyber threats by using sophisticated threat intelligence, penetration testing, and security audits. Creating a risk profile assists in prioritising the most important threats and taking adequate countermeasures [Panorays 2023]. Using AI and machine learning also improves real-time threat detection features [Interos 2025].

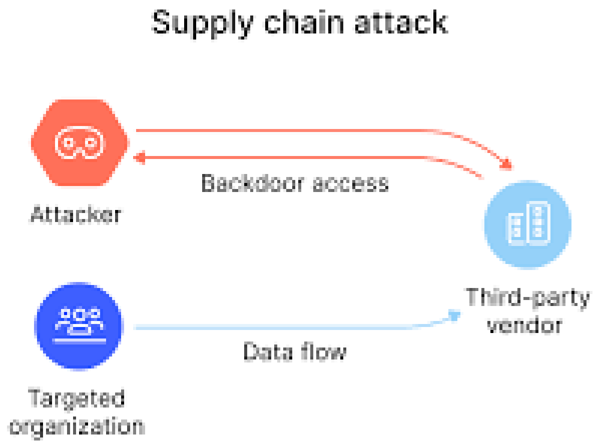


Figure 3: Supply Chain attacks on the rise (Source: Šlekytė, I. (2023)

3.2 Vulnerability Analysis and Threat Modeling

Vulnerability analysis entails the detection of software, hardware, and network system weaknesses that attackers might leverage. Threat modeling frameworks, including STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege), assist organizations in systematically examining and addressing potential attack vectors [Stride model]. Frequent vulnerability scans and patch management procedures ensure that detected risks are proactively resolved. Red team exercises also mimic actual cyberattacks to test system resilience and readiness [Stride threat modelling].

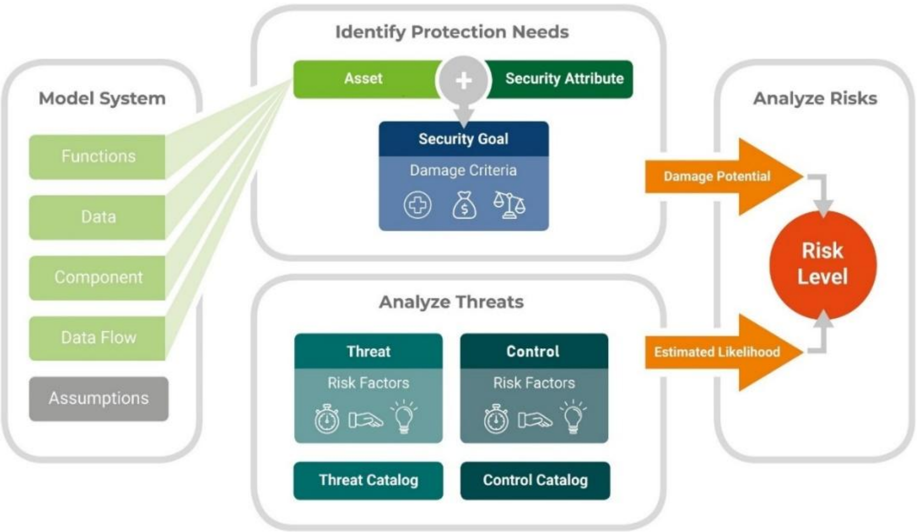


Figure 4: Supply Chain attacks on the rise (Source: YESC)

3.3 Impact and Likelihood Assessment

Estimating the likelihood and impact of recognized threats facilitates risk mitigation efforts prioritization. Organizations often apply a risk matrix to classify threats according to probability and severity [OWASP]. High-impact threats, for instance, ransomware attacks on essential infrastructure, necessitate prompt response, whereas less-priority risks can be resolved in the long term. Performing business impact assessments (BIAs) assists organizations in allocating resources optimally and protecting vital supply chain functions [Irius].

3.4 Risk Mitigation Strategies

Risk mitigation controls include technical, administrative, and procedural controls that minimize cybersecurity risk. The application of Zero Trust Architecture (ZTA), strong access controls, and encryption of sensitive information are fundamental defensive actions [MTMT]. Ongoing security training ensures the employee and third-party partner communities are aware of best practices in mitigating cyber threats. Comprehensive incident response plans and cybersecurity drills further strengthen an organization's capabilities to respond to threats [FL LLP].

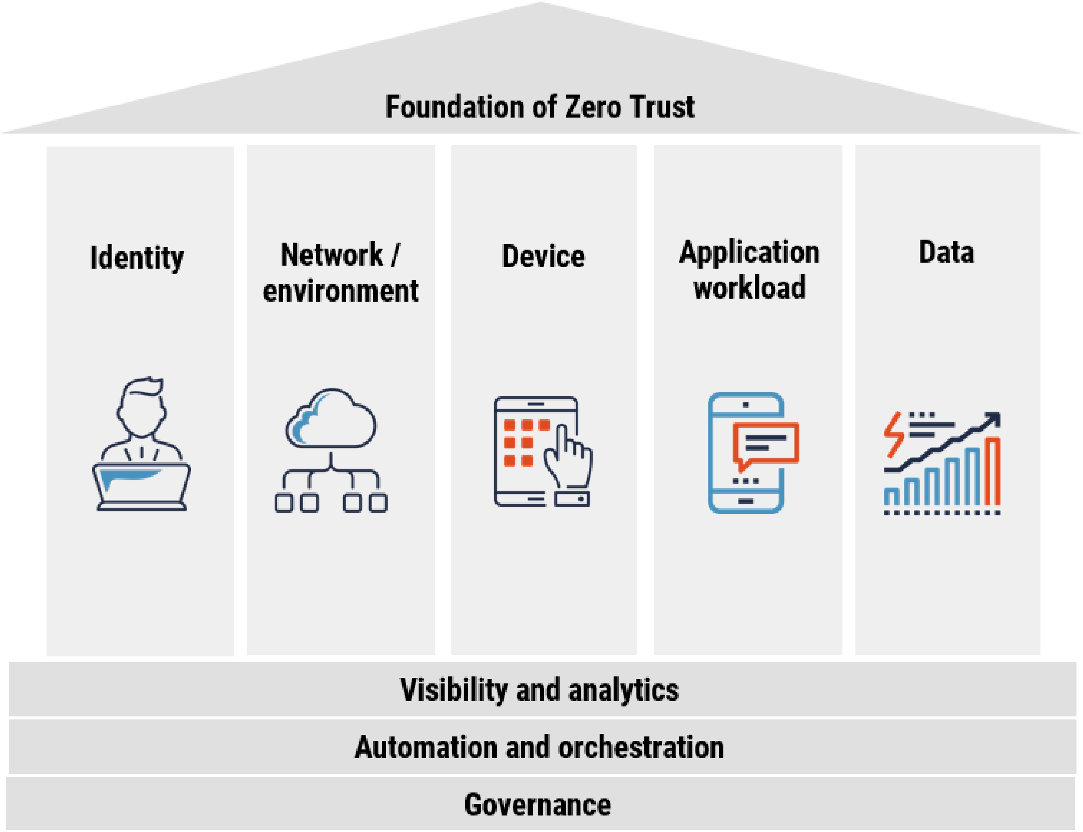


Figure 5: Foundation of Zero Trust (Source: CCCS 2022)

3.5 Continuous Monitoring and Incident Response

Ongoing monitoring is important in identifying and responding to cyber attacks in real time. Security Information and Event Management (SIEM) technologies collate and interpret security events along the supply chain [CSV 2025]. Artificial intelligence-powered anomaly detection aids in detecting strange behavior that might signal cyber threats. Automated response systems can stop threats from becoming more destructive before they are triggered, limiting the potential damage [SCMR 2024]. Mutual information sharing with industry partners and government agencies adds to the aggregate cybersecurity strength of the group [CSD].

4. CYBERSECURITY STRATEGIES FOR DIGITAL SUPPLY CHAINS

4.1 Zero Trust Architecture and Identity Management

Zero Trust Architecture (ZTA) is a security framework that revokes implicit trust in any organization, internal or external to the network. It applies strict access controls and ongoing authentication, significantly lowering the danger of unapproved access [Crowdstrike 2025]. Identity management solutions, including Multi-Factor Authentication (MFA) and Privileged Access Management (PAM), assist in the successful implementation of ZTA. By restricting access to vital supply chain information to authenticated and authorized users, ZTA reduces the attack surface [Cato networks 2025].

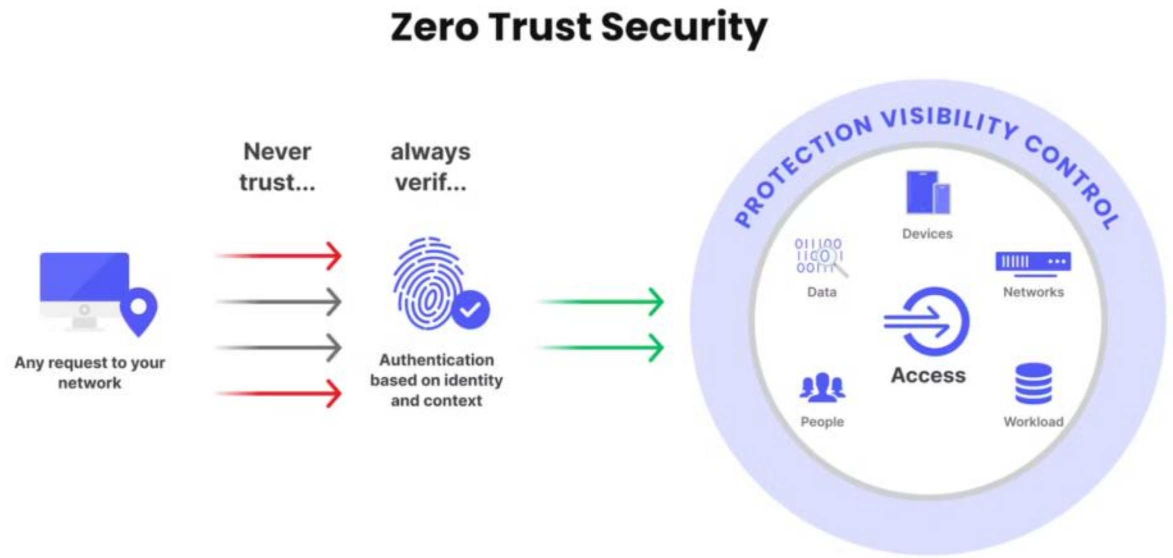

Zero Trust Security
Never trust...
always verif...
Any request to your network
Authentication based on identity and context
PROTECTION VISIBILITY CONTROL
Devices
Data
Networks
Access
People
Workload

Figure 6: Zero Trust Security (Source: Bairyey 2023)

4.2 Blockchain for Secure Transactions

Blockchain technology supports supply chain security through the use of an immutable and transparent ledger for transactions. Decentralized in nature, blockchain is tamper-resistant and fraud-proof, and its data integrity is maintained throughout the supply chain [Oracle 2025]. Smart contracts automate and execute contractual obligations, minimizing the potential for human error and fraud. Organizations can increase traceability and inhibit unauthorized modification of data by incorporating blockchain in digital supply chains [Rapid Innovation 2025].

4.3 Artificial Intelligence and Machine Learning for Threat Detection

AI and ML technologies are increasingly employed to identify cyber threats in real-time. These technologies examine patterns, detect anomalies, and forecast possible security breaches ahead of time [Digital guardian 2025]. Machine learning algorithms learn and get better with time, making adaptive threat detection and response possible. AI-driven security solutions boost supply chain resilience by detecting suspicious behavior and avoiding risks in advance [ISMS 2025].

4.4 Secure Software Development and Patch Management

Secure software development and regularly updated patches are critical for securing supply chain systems. Secure Software Development Life Cycle (SDLC) practices ensure that security is built in from the very start, beginning in the design phase. Ongoing patch management eradicates known vulnerabilities, lowering the likelihood of exploitation [NST 2025]. Automated patch deployment must be implemented by organizations to reduce downtime and avoid security breaches caused by outdated software [DDCIO 2025].

4.5 Employee Training and Awareness Programs

Human mistake is a major cybersecurity threat. Robust employee training programs enable staff to identify and counter cyber threats effectively. Phishing simulations and ongoing education on best practices improve cybersecurity awareness. Organizations must develop a security-first culture, where employees play an active role in supply chain security [Delinea 2025].

5. CASE STUDIES AND PRACTICAL APPLICATIONS

5.1 Notable Cyber Attacks on Digital Supply Chains

A number of prominent cyberattacks on digital supply chains have proved the weaknesses faced by organizations. Among the most prominent ones is the SolarWinds attack in 2020, where nation-state attackers broke into the firm's software updates and impacted thousands of companies and government institutions across the globe [Solar winds 2025]. Another significant incident was the 2021 Kaseya ransomware attack where attackers took advantage of a Kaseya's remote monitoring solution vulnerability to disseminate ransomware to several managed service providers affecting companies worldwide [Kaseya 2025]. During 2013, the data breach at Target was initiated from a third-party HVAC vendor company, which laid open the intimate information of 40 million patrons [Kaseya VSA 2025]. These cases illustrate the pervasive nature of cyber attacks in digital supply chains and the imperative need for effective security controls to preclude such occurrences.

5.2 Lessons Learnt from Historic Incidents

Learning from past cyber attacks yields useful lessons to avoid future risk. The SolarWinds incident highlighted the value of securing software supply chains by having more effective code integrity checking and multi-stage authentication controls in place [Fortinet 2025]. The Kaseya ransomware attack exposed remote access management vulnerabilities, highlighting the importance of ongoing patching, endpoint security, and zero-trust security models [UpGuard 2025]. The Target breach illustrated the dangers of third-party vendors, reiterating the importance of performing thorough security audits and imposing stringent vendor cybersecurity policies [Zscaler 2025]. A frequent learning from such incidents is the importance of threat vigilance monitoring proactively, speedy incident response practices, and ongoing employee education for improving cybersecurity resiliency [Cybersecurity 2025].

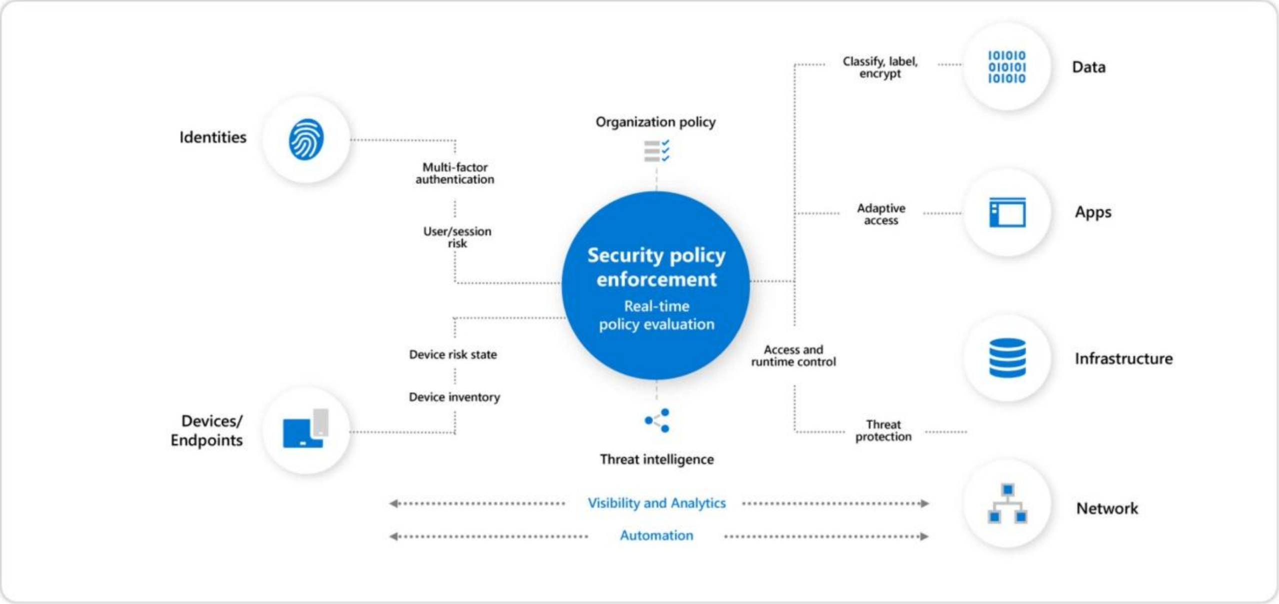


Figure 7: Security policy enforcement (Source: 848 group 2021)

5.3 Best Practice Adoption in Industry

Business entities in different industries have utilized best practices to enhance digital supply chain cybersecurity. Firms such as Microsoft and Google use Secure Software Development Life Cycle (SDLC) best practices, integrating security from the initial phases of development [Solar winds 2025]. Implementing blockchain technology in logistics, as utilized by Walmart's supply chain, increases product movement traceability and security [SEC 2025]. Various organizations have also adopted AI-powered security analytics to identify and react to cyber threats in real-time [US fines 2024]. Additionally, Zero Trust Architecture (ZTA) is becoming more commonly applied in industries to reduce insider attacks and unauthorized access [Reuters 2025]. Frameworks such as the NIST Cybersecurity Framework and ISO 27001 ensure compliance regulatory guidelines for providing companies with well-defined rules of how their cybersecurity initiatives need to comply with industry norms [Kaseya VSA 2025]. Through combining these best practices, organizations are able to fortify their supply chain security and prevent the adverse impacts of cyber threats.

6. FUTURE RESEARCH DIRECTIONS

6.1 Development of Cybersecurity Technologies

The fast development of cybersecurity technologies brings many possibilities for strengthening digital supply chain security. Quantum cryptography is one area with much promise in that it enables ultra-safe communication channels using quantum mechanics to resist eavesdropping and cyber espionage. Future studies need to emphasize real-world applications of quantum key distribution (QKD) to protect data exchanges in supply chain networks. Furthermore, AI-based anomaly detection systems are increasingly becoming essential to detect cybersecurity threats in real time. Machine learning algorithms can process huge volumes of network traffic to identify deviations from standard patterns, thus detecting potential cyberattacks before they can do any damage.

Blockchain technology also promises to play an important role in maintaining the integrity of supply chain transactions. Future studies can delve into how blockchain scalability and compatibility across various supply chain partners can be improved. Smart contracts that can automatically enforce security policies and track compliance within supply chains can further enhance cybersecurity protocols. Introducing cybersecurity automation into threat intelligence platforms can also enable organizations to counter cyber threats in real-time, minimizing human intervention and enhancing response efficiency.

As cyber threats evolve, predictive analytics for cyber risk assessment will become a core field of research. Through big data and AI, organizations are able to pre-empt vulnerabilities and predict forthcoming threats before they arise. Predictive models to measure supply chain risk factors need to be refined in research so that cybersecurity can become more resilient to unknown threats.

6.2 Policy and Governance for Secure Supply Chains

A key element of digital supply chain security is the creation of strong policy frameworks and governance mechanisms. Future studies must assess the efficacy of current cybersecurity legislation, including the NIST Cybersecurity Framework and the GDPR of the European Union, in addressing supply chain vulnerabilities. The globalized nature of supply chains calls for harmonized cybersecurity standards across jurisdictions. Research must investigate novel methods of international cooperation and legal harmonization to provide unified cybersecurity governance.

Blockchain audit trails are a nascent research field that can strengthen compliance enforcement. As immutable and transparent transaction records, blockchain technology can keep supply chain operations within regulatory compliance. AI-powered regulatory surveillance can also automate compliance procedures by automatically identifying policy breaches and security vulnerabilities.

Cyber insurance is another sector that needs more work. With supply chain cyber threats ongoing, it is critical to create robust cyber insurance models that factor in digital supply chain intricacies. Risk quantification methods that enable insurance companies to measure and price cybersecurity policies for supply chain risks accurately should be explored in future studies.

Additionally, with increasing dependence on third-party vendors, vendor risk assessment models are essential to study. AI-driven automated risk evaluation tools can assist organizations in constantly evaluating the cybersecurity stances of their vendors, minimizing third-party vulnerabilities and adherence to cybersecurity policies.

6.3 Emerging Threats and Adaptive Security Measures

The cybersecurity environment is ever-changing, with new threats coming from nation-state actors, cybercrime groups, and insider threats. The most significant concern in digital supply chain security is the increase in supply chain attacks that use trusted software vendors to breach networks. Research must aim at creating supply chain threat intelligence platforms that track vendor software updates and identify potential compromises before they hit end-users.

Dynamic adaptive security architectures that adapt to changing threats will be essential to future cybersecurity resilience. AI-driven defense systems that automatically identify and neutralize attacks in real time are a new field of research. Such systems employ self-learning algorithms to learn about threat behavior and evolve countermeasures accordingly, reducing human intervention in threat response.

Another area of increasing concern is the security of Internet of Things (IoT) devices in supply chains. The proliferation of IoT sensors for logistics, inventory tracking, and transportation monitoring brings new vulnerabilities. Research needs to be conducted on creating lightweight security protocols specifically for resource-limited IoT devices, providing strong authentication and encryption schemes without compromising system performance.

Edge computing is also emerging as an essential part of digital supply chains, facilitating real-time processing of data near the source. Edge devices are, however, vulnerable to cyber attacks because they are distributed in nature. Future studies must explore new ways of securing edge computing infrastructures, such as decentralized authentication protocols and real-time anomaly detection at the network edge.

Moreover, studies related to the effectiveness of cyber deception methods in protecting supply chains are also picking pace. Through deploying decoy platforms and honeypots in cybersupply chains, organizations may deceive attackers as well as create intelligence on attackers' methods. This security policy can assist companies in formulating more effective defense strategies against attacks.

FRAME OF WORK

Cybersecurity Factors Ranking and Enabler Efficiency Enhancement Framework (E3F)

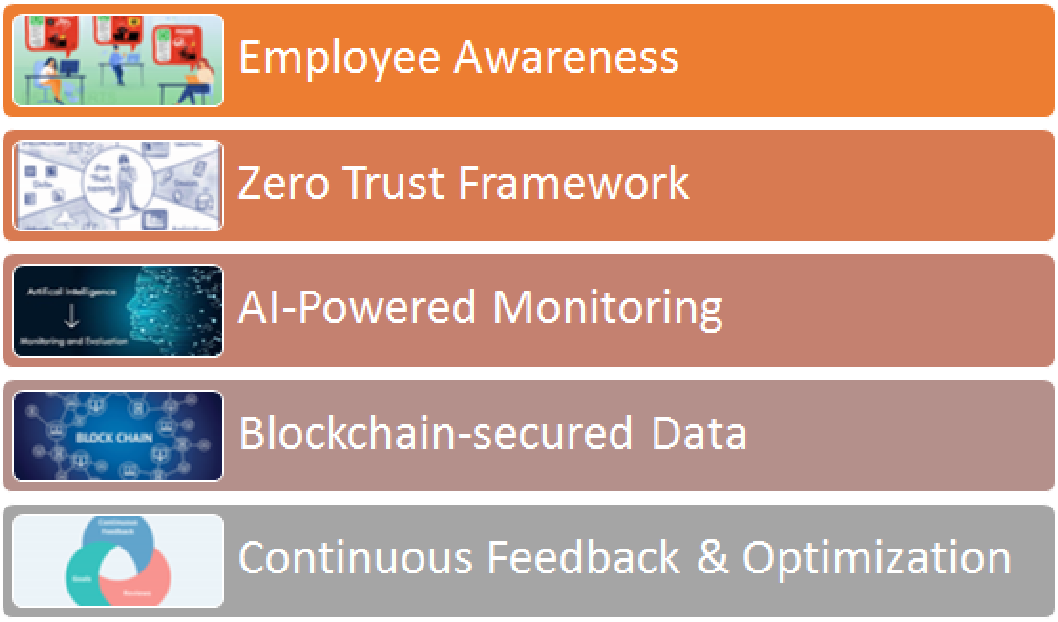
In the case of Digital Supply Chain Management (DSCM), cybersecurity threats need to be understood and addressed through a dual strategy: determining the important risk factors (barriers) and enhancing core capabilities (enablers). This research ranks eight fundamental cybersecurity factors and suggests a model of structured approach to enhance the efficiency of enablers to increase resilience and operational continuity.

Ranked Cybersecurity Factors with Classification and Description
The following table provides the ranking of the eight recognized cybersecurity factors by their criticality and influence. Each factor is listed as either a barrier, denoting a cybersecurity issue, or an enabler, denoting a strategic countermeasure or capability.

Ranked Cybersecurity Factors with Classification and Description
The following table ranks the eight identified cybersecurity factors based on their criticality and impact. Each factor is categorized either as a barrier, representing a cybersecurity challenge, or an enabler, representing a strategic countermeasure or capability.

Table 1: Ranked Cybersecurity Factors with Classification and Description

Rank	Factor	Type	Description
1.	Third-Party Vendor Risks	Barrier	External partners often lack adequate cybersecurity, leading to major breaches.
2.	Ransomware & Malware Attacks	Barrier	Disrupt operations and cause financial loss by locking systems or stealing data.
3.	Unauthorized Access & Data Breaches	Barrier	Stolen credentials and weak access controls lead to data theft.
4.	Zero Trust Architecture (ZTA)	Enabler	Eliminates implicit trust, enforces strict identity verification across the network.
5.	AI/ML for Threat Detection	Enabler	Detects and prevents cyber threats in real-time using behavioral analytics.
6.	Insider Threats & Human Error	Barrier	Often accidental or malicious activities by insiders compromise security.
7.	Blockchain Technology	Enabler	Provides immutable, transparent records ensuring secure data exchange.
8.	Employee Training & Awareness	Enabler	Reduces risk from phishing and human error through regular education.



Cybersecurity Enabler Efficiency Enhancement Model (E3M)
The Enabler Efficiency Enhancement Model (E3M) is a strategic model aimed at enhancing cybersecurity in digital supply chains through maximizing the deployment of the fundamental enablers. As digital supply chains encounter more advanced and multi-aspect cyber threats, a proactive, multilayered, and integrated strategy is imperative. E3M framework revolves around four main enablers—employee awareness and training, Zero Trust Architecture (ZTA), AI/ML for threat detection in real time, and blockchain technology—and each of these caters to targeted vulnerabilities of the supply chain network. The fifth one, integration and feedback, acts as the glue holding the layers together by providing learning and improvement in perpetuity across levels.

The initial layer of the model is awareness and organizational culture because human error continues to be the primary reason for cybersecurity incidents. In this layer, employee awareness and training are absolutely essential. Frequent awareness programs, phishing campaigns, and interactive sessions are advocated for educating employees about best practices, making them vigilant, and establishing a culture of shared responsibility concerning cybersecurity. When staff are taught to detect threats early and respond in a responsible manner, the probability of internal compromise or unintentional disclosures is greatly minimized.

The second defense focuses on security architecture, namely through the implementation of the Zero Trust Architecture (ZTA). In contrast to conventional models that are perimeter-defensive in nature, ZTA presumes that no actor—internal or external—can be absolutely trusted. In contrast, access to data and systems is controlled through strict identity verification, ongoing authentication, and least privilege. Micro-segmentation of networks will ensure that in the event one node is attacked, the compromise is isolated. This model has the effect of severely restricting lateral movement by hackers and assists with enforcing granular control over what can be accessed by whom, and under what circumstances.

The third element of the framework utilizes Artificial Intelligence (AI) and Machine Learning (ML) to strengthen real-time threat detection and incident response. AI-powered systems scrutinize vast amounts of data to identify anomalous behavior patterns that may indicate a breach or active attack. ML algorithms learn from historical incidents over time, enhancing their accuracy and responsiveness. These technologies can be combined with Security Information and Event Management (SIEM) solutions to offer centralized, automated, and adaptive security monitoring throughout the supply chain environment.

Secondly, the model includes blockchain technology to provide data integrity, transparency, and trust throughout the supply chain. Blockchain's decentralized and tamper-resistant ledger makes it a perfect fit for logging transactions, authenticating supplier identities, and tracking the origin of goods and data. The application of smart contracts also increases automation and compliance by enforcing pre-established rules and permissions. This level of the model introduces resilience by stopping unauthorized data changes and allowing end-to-end traceability in intricate supply chain processes.

Lastly, the model is brought together by a dynamic integration and feedback mechanism. A centralized Cyber Risk Dashboard combines information from all enabler systems—ZTA enforcement logs, AI/ML alerts, employee behavior analytics, and blockchain audit trails—to give real-time visibility. An integrated view aids decision-makers in analyzing system performance, detecting gaps, and taking corrective action on a timely basis. Feedback loops are built into the system to improve access policies, training programs, and algorithm performance continuously by drawing on incident data and changing threat landscapes.

In all, the Enabler Efficiency Enhancement Model (E3M) offers a holistic, multi-faceted model for maximizing cybersecurity within digital supply chains. It allows for not just prevention and detection but also resilience and adaptability, keeping organizations ahead of new and upcoming cyber threats while enhancing operational efficiency and stakeholder confidence.

CONCLUSION

Cybersecurity of digital supply chains is a rising issue that requires proactive and multi-layered defense. Organizations need to implement thorough risk assessment frameworks, adopt best practices, and remain in front of changing threats to maintain the resilience of supply chain networks. The adoption of advanced cybersecurity technologies, regulatory guidelines, and adaptive security practices will be crucial in countering cyber risks.

Future studies need to further investigate new solutions to improve supply chain security in a more digitalized world. Quantum cryptography, AI-based cybersecurity, blockchain technology, and adaptive security models will be key drivers of the future of supply chain cybersecurity. Harmonized policy environments and cross-border collaboration will also be essential in countering cyber threats on a global level.

As cyber threats evolve, organizations need to stay alert and keep investing in cybersecurity innovation. Through collaboration among industry, academia, and policymakers, the digital supply chain ecosystem can be protected from evolving cyber threats, maintaining its integrity, confidentiality, and operational continuity.

REFERENCES

Kaspersky, "Story of the Year: global IT outages and supply chain attacks," Securelist, Dec. 2024. [Online]. Available: https://securelist.com/ksb-story-of-the-year-2024/114883/. [Accessed: 04-Mar-2025].

National Institute of Standards and Technology, "Cybersecurity Framework," NIST, 2014. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed: 04-Mar-2025].

Supply Chain Management Review, "Analyzing the supply chain risks behind the top data breaches in 2024," SCMR, Oct. 2024. [Online]. Available: https://www.scmr.com/article/analyzing-the-supply-chain-risks-behind-the-top-data-breaches-in-2024. [Accessed: 04-Mar-2025].

The Wall Street Journal, "Stop & Shop Races to Restock Shelves After 'Cybersecurity Issue'," WSJ, Nov. 2024. [Online]. Available: https://www.wsj.com/articles/stop-shop-races-to-restock-shelves-after-cybersecurity-issue-ba45accb. [Accessed: 04-Mar-2025].

FasterCapital. (n.d.). *The evolution of supply chain management*. FasterCapital. https://fastercapital.com/topics/the-evolution-of-supply-chain-management.html

The Sun, "Major supermarket hit by shortages as shoppers spot popular items missing from shelves," The Sun, Nov. 2024. [Online]. Available: https://www.thesun.co.uk/money/31934374/morrisons-stock-issues-software-hackers-blue-yonder/. [Accessed: 04-Mar-2025].

New York Post, "Starbucks bosses using pen and paper to pay employees after ransomware attack," NY Post, Nov. 2024. [Online]. Available: https://nypost.com/2024/11/26/business/starbucks-using-pen-and-paper-to-pay-workers-after-ransomware-attack/. [Accessed: 04-Mar-2025].

National Cyber Security Centre, "Supply Chain Attack Examples," NCSC, 2024. [Online]. Available: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples. [Accessed: 04-Mar-2025].

GuidePoint Security, "What is Cyber Supply Chain Risk Management?," GuidePoint, 2024. [Online]. Available: https://www.guidepointsecurity.com/education-center/what-is-cyber-supply-chain-risk-management/. [Accessed: 04-Mar-2025].

BSI Group, "Cybersecurity in the Spotlight: Safeguarding the Digital Supply Chain," BSI, 2024. [Online]. Available: https://www.bsigroup.com/en-US/insights-and-media/insights/blogs/cybersecurity-in-the-spotlight-safeguarding-the-digital-supply-chain/. [Accessed: 04-Mar-2025].

Prevalent, "Cyber Supply Chain Risk Management (C-SCRM) Best Practices," Prevalent, 2024. [Online]. Available: https://www.prevalent.net/blog/cyber-supply-chain-risk-management-cscrm/. [Accessed: 04-Mar-2025].

BitSight, "7 Cybersecurity Frameworks to Reduce Cyber Risk in 2024," BitSight, 2024. [Online]. Available: https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk. [Accessed: 04-Mar-2025].

The Guardian, "Rejoice! The charade of having to change our passwords every few months is coming to an end," The Guardian, Oct. 2024. [Online]. Available: https://www.theguardian.com/commentisfree/2024/oct/28/password-change-requirement-ending. [Accessed: 04-Mar-2025].

The Wall Street Journal, "New Technology is Taking Package Tracking Past Scanning," WSJ, Dec. 2024. [Online]. Available: https://www.wsj.com/articles/new-technology-package-tracking-2024. [Accessed: 04-Mar-2025].

The Wall Street Journal, "Companies Prepare to Fight Quantum Hackers," WSJ, Sep. 2024. [Online]. Available: https://www.wsj.com/articles/companies-fight-quantum-hackers-2024. [Accessed: 04-Mar-2025].

IoT For All, "5 Key Developments in IoT for Transportation and Logistics," IoT For All, 2024. [Online]. Available: https://www.iotforall.com/articles/iot-developments-logistics. [Accessed: 04-Mar-2025].

Digital Matter, "How IoT has Enhanced Supply Chain Visibility," Digital Matter, 2024. [Online]. Available: https://www.digitalmatter.com/blog/iot-supply-chain-visibility. [Accessed: 04-Mar-2025].

Technology Innovators, "Internet of Things (IoT) in Logistics: Real-time Tracking and Asset Management," Technology Innovators, 2023. [Online]. Available: https://www.technologyinnovators.com/iot-logistics-real-time-tracking. [Accessed: 04-Mar-2025].

Surgere, "How GPS Powers IoT with Real-Time Tracking," Surgere, 2024. [Online]. Available: https://www.surgere.com/gps-iot-tracking. [Accessed: 04-Mar-2025].

National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST, Feb. 2024. [Online]. Available: https://www.nist.gov/news-events/news/2024/02/nist-cybersecurity-framework-20. [Accessed: 04-Mar-2025].

Wikipedia, "NIST Cybersecurity Framework," Wikipedia, 2024. [Online]. Available: https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework. [Accessed: 04-Mar-2025].

C. R. Center, "Top 5 Cybersecurity Concerns for Enterprises in 2025," CyberProof, Feb. 2025. [Online]. Available: https://www.cyberproof.com/blog/top-5-cybersecurity-concerns-for-enterprises-in-2025/

S. Group, "Top Cybersecurity Challenges & Solutions for 2025," TechnologyAdvice, Feb. 2025. [Online]. Available: https://technologyadvice.com/blog/information-technology/cybersecurity-challenges/

P. Group, "Cybersecurity Risks Explained: Detect, Manage, and Mitigate Threats," Protecht, Feb. 2025. [Online]. Available: https://www.protechtgroup.com/en-us/blog/understanding-cybersecurity-risks-comprehensive-guide

N. I. of Standards and Technology, "Cybersecurity Supply Chain Risk Management," NIST, 2022. [Online]. Available: https://csrc.nist.gov/csrc/media/Projects/cyber-supply-chain-risk-management/documents/C-SCRM_Fact_Sheet.pdf

S. One, "12 Cyber Security Issues and How to Mitigate Them," SentinelOne, Jan. 2025. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-issues/

L. Group, "Top Cybersecurity Threats Facing 3PL Companies and How to Mitigate Them," Lean Group, Feb. 2025. [Online]. Available: https://www.leangroup.com/blog/top-cybersecurity-threats-facing-3pl-companies-and-how-to-mitigate-them

G. Security, "What is Cyber Supply Chain Risk Management?," GuidePoint Security, Feb. 2025. [Online]. Available: https://www.guidepointsecurity.com/education-center/what-is-cyber-supply-chain-risk-management/

B. Insight, "7 Cybersecurity Frameworks to Reduce Cyber Risk in 2024," BitSight, 2024. [Online]. Available: https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

European Union Agency for Cybersecurity (ENISA). (2021, July 29). *Understanding the increase in supply chain security attacks*. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

C. Magazine, "How Kroll and DORA Tackle Supply Chain Cybersecurity Risks," Cyber Magazine, Jan. 2025. [Online]. Available: https://cybermagazine.com/articles/kroll-cybercriminals-target-supply-chain-it

E. Blog, "Key Considerations for Successful Cybersecurity Supply Chain Risk Management (C-SCRM)," Eclypsium, 2024. [Online]. Available: https://eclypsium.com/blog/key-considerations-for-successful-cybersecurity-supply-chain-risk-management-c-scrm/

C. S. R. Management, "Best Practices in Cyber Supply Chain Risk Management," NIST, 2024. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

P. Blog, "Understanding IoT Cybersecurity in Supply Chains," Panorays, Dec. 2024. [Online]. Available: https://panorays.com/blog/iot-cybersecurity-in-supply-chains/

H. Resource, "Cybersecurity Risk Management | Frameworks & Best Practices," Hyperproof, 2024. [Online]. Available: https://hyperproof.io/resource/cybersecurity-risk-management-process/

N. C. and S. Center, "Protecting Critical Supply Chains," Office of the Director of National Intelligence, Sep. 2024. [Online]. Available: https://www.dni.gov/files/NCSC/documents/supplychain/20240926_Securing-Your-Supply-Chain-Ecosystem.pdf

C. Saint, "Applying the NIST Supply Chain Risk Management Framework," CyberSaint, 2024. [Online]. Available: https://www.cybersaint.io/blog/nist-supply-chain-risk-management-framework

C. Point, "Cyberattacks on US utilities surged 70% this year, says Check Point," Reuters, Sep. 2024. [Online]. Available: https://www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says-check-point-2024-09-11/

R. Horne, "Britain now worse at dealing with cyberattackers, GCHQ says," The Times, Dec. 2024. [Online]. Available: https://www.thetimes.co.uk/article/britain-now-worse-at-dealing-with-cyberattackers-gchq-says-h7v57rh0d

R. News, "The 'ICTS' rules: Technology supply chain regulation has arrived," Reuters, Oct. 2024. [Online]. Available: https://www.reuters.com/legal/legalindustry/icts-rules-technology-supply-chain-regulation-has-arrived-2024-10-30/

S. C. M. Review, "Analyzing the supply chain risks behind the top data breaches in 2024," SCMR, Oct. 2024. [Online]. Available: https://www.scmr.com/article/analyzing-the-supply-chain-risks-behind-the-top-data-breaches-in-2024

C. Proof, "Top 5 Cybersecurity Concerns for Enterprises in 2025," CyberProof, Feb. 2025. [Online]. Available: https://www.cyberproof.com/blog/top-5-cybersecurity-concerns-for-enterprises-in-2025/

N. I. of Standards and Technology, "Cybersecurity Supply Chain Risk Management," NIST, 2022. [Online]. Available: https://csrc.nist.gov/csrc/media/Projects/cyber-supply-chain-risk-management/documents/C-SCRM_Fact_Sheet.pdf

Avetta. "Top 5 Supply Chain Cyber Risks." Avetta, https://www.avetta.com/blog/top-5-supply-chain-cyber-risks.

Panorays. "Digital Supply Chain Risk Trends in 2023: A Look Back." Panorays, https://panorays.com/blog/digital-supply-chain-in-2023/.

Interos.ai. "How Supply Chain Cyber Threats Cost The Global Economy." Cyber Magazine, https://cybermagazine.com/articles/interos-supply-chain-risks-2025.

Šlekytė, I. (2023, March 6). *Supply chain attack: What is it and how does it work?* NordVPN. https://nordvpn.com/blog/supply-chain-attack/

"STRIDE Model." Wikipedia, https://en.wikipedia.org/wiki/STRIDE_model.

Software Secured. "STRIDE Threat Modeling: What You Need to Know." Software Secured, https://www.softwaresecured.com/post/stride-threat-modelling.

YSEC. (n.d.). *Threat analysis and risk assessment*. YSEC. https://ysecurity.io/knowledge-base/threat-analysis-and-risk-assessment

OWASP Foundation. "Threat Modeling Process." OWASP, https://owasp.org/www-community/Threat_Modeling_Process.

Irius Risk. "Threat Modeling Methodology: STRIDE." IriusRisk, https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride.

Microsoft. "Microsoft Threat Modeling Tool." Microsoft Learn, https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

Foley & Lardner LLP. "Combatting Supply Chain Cyber Threats: Safeguarding Data and Operations." Foley & Lardner LLP, https://www.foley.com/insights/publications/2024/04/supply-chain-cyber-threats-safeguarding-data/.

Canadian Centre for Cyber Security. (2022, November). *Zero Trust security model (ITSAP.10.008)*. https://www.cyber.gc.ca/en/guidance/zero-trust-security-model-itsap10008

Cybersecurity Ventures. "Software Supply Chain Attacks To Cost The World $60 Billion By 2025." Cybersecurity Ventures, https://cybersecurityventures.com/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025/.

SCMR. "Analyzing the Supply Chain Risks Behind the Top Data Breaches in 2024." Supply Chain Management Review, https://www.scmr.com/article/analyzing-the-supply-chain-risks-behind-the-top-data-breaches-in-2024.

Cybersecurity Dive. "The Art of Threat Modeling: 3 Frameworks to Know." Cybersecurity Dive, https://www.cybersecuritydive.com/news/cyber-threat-modeling-framworks-STRIDE-LINDDUN-decision-trees/713587/.

CrowdStrike. "What is Zero Trust Security? Principles of the Zero Trust Model." Accessed March 4, 2025.

crowdstrike.com

Cato Networks. "Zero Trust Security: Principles and Framework Explained." Accessed March 4, 2025.

catonetworks.com

Bairyev, M. (2023, February 28). *What is Zero Trust Architecture and how does it work?* Mad Devs. https://maddevs.io/blog/what-is-zero-trust-network-architecture/

Oracle. "Blockchain for Supply Chain: Uses and Benefits." Accessed March 4, 2025.

oracle.com

Rapid Innovation. "Smart Contracts in Supply Chain: Benefits, Use Cases, and Examples." Accessed March 4, 2025.

rapidinnovation.io

Digital Guardian. "Understanding the Zero Trust Security Model to Safeguard Digital Infrastructure." Accessed March 4, 2025.

digitalguardian.com

ISMS.online. "Multi-Factor Authentication and Zero Trust." Accessed March 4, 2025.

isms.online

NIST. "Zero Trust Architecture." Accessed March 4, 2025.

nvlpubs.nist.gov

Department of Defense Chief Information Officer. "Department of Defense Zero Trust Reference Architecture." Accessed March 4, 2025.

dodcio.defense.gov

Delinea. "The Zero Trust Model and PAM (Privileged Access Management)." Accessed March 4, 2025.

delinea.com

Government Accountability Office, "SolarWinds Cyberattack Demands Significant Federal and Private Sector Response," [Online]. Available: https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic. [Accessed: Mar. 4, 2025].

Kaseya, "Kaseya Responds Swiftly to Sophisticated Cyberattack," [Online]. Available: https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/. [Accessed: Mar. 4, 2025].

"Kaseya VSA ransomware attack," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack. [Accessed: Mar. 4, 2025].

Fortinet, "SolarWinds Supply Chain Attack," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack. [Accessed: Mar. 4, 2025].

UpGuard, "How Did Kaseya Get Hacked?," [Online]. Available: https://www.upguard.com/blog/how-did-kaseya-get-hacked. [Accessed: Mar. 4, 2025].

Zscaler, "What is the SolarWinds Cyberattack?," [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-the-solarwinds-cyberattack. [Accessed: Mar. 4, 2025].

Cybersecurity & Infrastructure Security Agency, "Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers," [Online]. Available: https://www.cisa.gov/news-events/news/kaseya-ransomware-attack-guidance-affected-msps-and-their-customers. [Accessed: Mar. 4, 2025].

848 Group. (2021, June 17). *Zero Trust: Why you should never trust and always verify*. 848 Group. https://848.co/insights/zero-trust-why-you-should-never-trust-and-always-verify

"SolarWinds hack explained: Everything you need to know," TechTarget, [Online]. Available: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. [Accessed: Mar. 4, 2025].

"SEC fines four companies for downplaying SolarWinds hack," Axios, Oct. 22, 2024. [Online]. Available: https://www.axios.com/2024/10/22/sec-solarwinds-disclosure-fines. [Accessed: Mar. 4, 2025].

"U.S. Fines Tech Companies Over Disclosures Related to SolarWinds Hack," Wall Street Journal, Oct. 22, 2024. [Online]. Available: https://www.wsj.com/articles/u-s-fines-tech-companies-over-disclosures-related-to-solarwinds-hack-e08fedc8. [Accessed: Mar. 4, 2025].

"Wave of cyber-related SEC enforcement activity may signal increased scrutiny," Reuters, Dec. 9, 2024. [Online]. Available: https://www.reuters.com/legal/legalindustry/wave-cyber-related-sec-enforcement-activity-may-signal-increased-scrutiny-2024-12-09/. [Accessed: Mar. 4, 2025].

"Kaseya VSA ransomware attack," Wikipedia, [Online]. Available:
https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack. [Accessed: Mar. 4, 2025].