Journal of Management World **2025**, 2: 233-243
DOI: 10.53935/jomw.v2024i4.907

Cybersecurity and Supply Chain Integrity: Evaluating the Economic Consequences of Vulnerabilities in U.S. Infrastructure

Mohammad Abdul Goffer[1], Syed Nazmul Hasan[2*], Niropam Das[3], Jobanpreet Kaur[4], Jahid Hassan[5], Clinton Ronjon Barikdar[6], Sachin Das[7]

[1,3,5,6,7]Department of Business Administration, International American University, Los Angeles, CA 90010, USA.
[2,4]Department of Technology & Engineering, Westcliff University, CA 92614, USA; s.hasan.104@westcliff.edu (S.N.H.).

Abstract. Supply chain cybersecurity risks are a major threat to economic security and business continuity across critical sectors in the United States, including healthcare, finance, manufacturing, and technology. This paper assesses the impact of cyber threats on the supply chain and the measures that can be taken to prevent them, such as threat intelligence, employee awareness, and vendor security. Combining qualitative and quantitative techniques, the study complements economic loss data with qualitative insights into industry issues. Findings from the research show that preventive measures taken in cybersecurity can decrease losses for businesses in high-risk industries by more than 40 percent. Using such technologies as artificial intelligence and blockchain improves threat detection and increases transparency; however, it has certain limitations. The research offers some practical suggestions, such as increasing public-private collaboration, increasing access to sophisticated technology, and enhancing the organizations' compliance with the regulations. These insights enable individuals and organizations to create robust, secure, and sustainable supply chain networks for the future.

Keywords: Cybersecurity, Supply Chain, Economic Consequences, Infrastructure.

1. INTRODUCTION

1.1. Background

The existing supply chain in today's global market is a web of manufacturers, suppliers, third-party logistics providers, and consumers connected through high-tech networks (Monjur & Akon, 2023; Susitha et al., 2024). Such a system of interdependence has revolutionized production and distribution activities through timely deliveries and reduced operating costs with enhanced output. However, digital systems' direct and gradual implementation has introduced new vulnerabilities that unscrupulous actors can exploit to disrupt operations, steal vital information or data, or cause sizable disruptions (Cheung et al., 2021). These weaknesses have made cybersecurity a critical component in supply chain protection(Ghimire et al., 2024).

Supply chain cyber risks have increased and evolved due to enhanced focus and increased frequency and sophistication of attacks in recent years against core business sectors critical to economic growth and national security (Arroyabe et al., 2024). The SolarWinds attack and the recent attack on the Colonial Pipeline are just but a sample of the impact that cyberattacks can cause(Hasan, Al Mahmud, et al., 2024). For example, the SolarWinds hack installed malware in software updates of a popular Orion IT management platform, affecting thousands of companies, including key federal agencies in the United States (Gia & Fitria, 2024). Likewise, the recent ransomware attack — Colonial Pipeline — left the East Coast fuel scarce (Dudley & Golden, 2021), a clear example of how supply chains with infrastructure are susceptible to disruptions. Such cases show the need for concrete and diverse cybersecurity strategies in supply chain networks(Biswas et al., 2024).

The use of cloud computing technology, AI, and IoT in the digital transformation of supply chains has opened the supply chain to more risks from cyber threats (Creazza et al., 2022; Rauniyar et al., 2023). These improvements in efficiency and transparency come with fresh risks. For instance, in real-time tracking and monitoring of IoT devices, the security measures implemented are usually weak and can, therefore, be exploited(Gorgun & Karamis, 2019). Likewise, cloud supply chain management systems, if not protected well, compromise the data and make it vulnerable to hacking. Globalization worsens the situation because supply chains stretch across borders, and countries may have different rules, security protocols, and levels of technology. A cyber-attack in one geographical area may reach other areas through the network and affect business globally. This also increases the risks involved with third-party suppliers that might not have adequate security protocols. For example, one vulnerable node in a supplier's network can be a gateway for the attacker to access other organizations with robust defenses(Hasan, Chy, et al., 2024).

The economic losses that organizations experience due to such breaches are not negligible. The direct threats are those that can be easily quantified in monetary terms, including ransoms paid, data recovery costs, and lost revenues due to disruptions (Pavelea & Negrea, 2024; Wang et al., 2019). Intangible losses like brand erosion, fines, and loss of customer confidence are usually sustained in the long run (Kuipers & Schonheit, 2022; Pavelea & Negrea, 2024). For example, organizations vulnerable to supply chain attacks may lose market share or receive increased scrutiny from key stakeholders. Moreover, it may lead to disruptions in essential industries, such as healthcare or energy, which can have social impacts like threatening public safety and posing national security

Article History: Received: 12 August 2024; Revised: 21 October 2024; Accepted: 29 October 2024; Published: 22 November 2024
* Correspondence: s.hasan.104@westcliff.edu

threats(Hasan, Farabi, et al., 2024).

Supply chain cybersecurity has witnessed significant developments to tackle these issues(Şenol, Çakır, et al., 2024). The government has launched contemporary measures like the Cybersecurity Maturity Model Certification (CMMC) to ensure that all defense sector contractors meet high cybersecurity standards (Bruce, 2023). Currently, industry players are implementing zero-trust architectures, threat detection systems, and blockchain technologies to protect supply chains. Still, these measures are not equally applied, especially by SMEs who cannot afford to invest in sophisticated cybersecurity systems(Hossain et al., 2024).

There is still a significant gap in the literature concerning the economic consequences of supply chain cyber security threats. Current literature mainly targets the technical aspect of the problem, while minimal attention has been paid to the economic and policy implications(Şenol et al., 2020). This research will seek to fill this gap by assessing the impact of supply chain risks and examining best practices for protecting critical infrastructure in the United States(Imran et al., 2024).

1.2. Supply Chain Vulnerabilities and Cybersecurity Risks

Modern supply chains are characterized by their complexity, with multiple stakeholders operating within a single network. This complexity creates several entry points for cyberattacks:

- Software Exploits: Supply chains rely heavily on Enterprise Resource Planning (ERP) systems, which, if left unpatched, are vulnerable to exploitation.
- Network Intrusions: Inadequately secured networks connecting suppliers and vendors can serve as gateways for attackers.
- Insider Threats: Employees with malicious intent or inadequate training inadvertently expose systems to breaches.
- Third-Party Risks: Contractors and suppliers with lesser cybersecurity defenses can become pathways for these attacks.

These vulnerabilities are made worse by the increasing use of IoT devices, cloud, and AI in supply chain processes. Of course, these technologies optimize the processes, yet they expand the area of potential threats, which calls for advanced security solutions.

1.3. Economic Impacts of Supply Chain Cyberattacks

The supply chain cyber risk impacts the economy in many aspects, touching on businesses, consumers, and the economy as a whole. Direct costs include loss of revenue due to system unavailability, loss of data, and ransom costs (Pavelea & Negrea, 2024). Additional direct and indirect costs, which include reputational damage, legal suits, and loss of customers, add to the problem (Kuipers & Schonheit, 2022). For instance, the attack on the Colonial Pipeline led to fuel shortages across the East Coast and generated millions of losses for businesses and panic(Johora et al., 2024). Also, disruptions in the supply chain affect other industries and sectors within the chain, leading to ripple effects. For instance, any failure in the technology sector can cause production hold-ups across manufacturing, healthcare, and finance(Şenol, Oyan, et al., 2024). Economic consequences of such disruptions underscore the importance of having effective cybersecurity measures to protect the supply chain from interference(N. N. I. Prova, 2024).

1.4. Government and Industry Responses

Recognizing the strategic importance of secure supply chains, the U.S. government has implemented several initiatives to address cybersecurity challenges:

- Executive Orders on Cybersecurity: Measures such as new policies that require higher levels of security measures, supply chain risk analysis, and cooperative initiatives between the government and the business world (Haklai, 2023).
- Cybersecurity Maturity Model Certification (CMMC): A structure to ensure that the defense contractors comply with cybersecurity (Bruce, 2023).
- Critical Infrastructure Protection Programs: Measures directed at industries like energy, healthcare, and transport to strengthen their response to cyber risks (Parraguez-Kobek et al., 2022).

Besides governments' efforts, numerous industry players are implementing progressive cybersecurity solutions like zero-trust systems, endpoint protection, and threat intelligence in real-time. However, these initiatives remain patchy across sectors, with SMEs failing to achieve broad security strategies because of a lack of capital(Johora et al., 2021).

1.5. The Role of Advanced Technologies in Cybersecurity

Technology is playing an important role in enhancing cybersecurity in the supply chain. Among these technologies, AI is especially beneficial since it can handle big data and analyze them to determine patterns of anomalous behavior that signify threats (Kaur et al., 2023; Manoharan & Sarker, 2023). With the help of AI, organizations can implement continuous monitoring systems that can identify any form of malicious activity, thus

implying faster response to threats. Similarly, blockchain has become an effective solution in increasing the transparency and security of transactions in the supply chain. It means that the records distributed throughout the blockchain cannot be changed directly by the attackers to distort the information(Akter et al., 2024).

Another emerging area that has been mentioned is quantum computing in cybersecurity. Although it is a relatively new field, quantum cryptography can help develop encryption techniques that are almost impossible to crack, protecting valuable supply chain information from cyber threats (Singh & Kumar, 2024). Also, Internet of Things (IoT) security solutions are being deployed to mitigate the risks of connected devices. Smart devices, which are commonly employed for monitoring shipments, inventory, and logistics, are an easy target for attackers since they lack robust security measures. Better IoT security features like device authentication and secure communication protocols must be implemented to address such risks.

However, integrating advanced technologies in supply chain cybersecurity has its own set of issues. They can have high implementation costs, require specialist knowledge, and may be improperly set up. Moreover, some technologies, like AI algorithms, introduce new risks like the inclusion of biases and errors that affect the reliability of the technology. However, the benefits of utilizing advanced cybersecurity measures outweigh the drawbacks, and thus, such solutions are essential for building a stronger supply chain. Suppose organizations take the initiative to adopt these technologies. In that case, their capacity to identify, manage, and mitigate cyber threats and risks will be improved in a way that protects the authenticity of their operations(N. N. Islam Prova, 2024).

1.6. Research Gap

While the need to protect the supply chain from cybersecurity threats has been recognized, several areas are still yet to be fully understood in terms of their impact on the economy. Previous research tends to place more emphasis on the technological aspect of cybersecurity research than on the economic aspect. Additionally, while large enterprises have the resources to adopt more sophisticated cybersecurity solutions, a large population of SMEs is not adequately served. There is also a need to examine how government policies can help close these gaps.

1.7. Research Objectives

This Study aims to evaluate the economic consequences of supply chain vulnerabilities in U.S. infrastructure, with a focus on:

1. Measuring the economic losses of cyber threats on key industries.
2. Exploring the main risks in supply chain networks and their respective attack vectors.
3. Evaluating the current state of cybersecurity frameworks and approaches.
4. Exploring the impact of emerging technologies on supply chain risk management.
5. Offering practical solutions to improve the overall cybersecurity readiness of supply chain systems.

1.8. Significance of the Study

The present investigation findings are relevant for policymakers, industry professionals, and cybersecurity practitioners. Thus, this research assists in qualifying the supply chain risks and indicates that companies should involve themselves in cybersecurity solutions. An emerging technology and strategy review provides a roadmap for enhancing organizational readiness. In contrast, a subsequent case study on government policies provides a way to foster collaboration and protect vital assets.

2. MATERIALS AND METHODS

This study used quantitative and qualitative research methods to evaluate the economic effects of SSCP threats. Exploratory and descriptive research paradigms were used to develop an understanding of the issues, impacts, and solutions regarding supply chain security.

2.1. Research Design

The justification for employing a mixed-methods research design was to obtain quantitative and qualitative data. Quantitative analysis focused on assessing the impact of dollar value, organizational disruption, and security measures. This was complemented by quantitative data from questionnaires and interviews, which elicited further details about the practicalities involved and the stakeholders' perspectives. Together, these methods enabled a thorough approach to the research objectives, including estimating economic damages, identifying crucial risks, and exploring emerging technologies' possibilities in mitigating threats.

The mixed methods approach was designed to measure several aspects of cybersecurity in supply chain contexts, as described below. It statistically quantified financial and operating impacts and applied thematic analysis to identify professional trends across different fields. These approaches enabled a reasonable level of analysis, as they incorporated numerical movements and other patterns.

2.2. Data Collection

To get broad and detailed information, the data was collected through both primary and secondary sources. These research data were collected from fifty targeted industry experts through structured questionnaires and semi-structured interviews. These people were from such fields as healthcare, finance, manufacturing, and technology, all of which are considered to be at high risk of cyber risks. Questionnaires were created to gather quantitative information on financial losses, time, and resources related to security threats. In contrast, the semi-structured interviews offered first-hand qualitative information regarding the difficulties, approaches, and organizational dynamics of operations.

Secondary data enriched the primary sources because they provided context. Official and academic documents and industry papers offered comprehensive accounts of the actual cyber attacks that took place, statistical analysis, and policy perspectives. These sources complemented the study by providing closure to some findings and revealing more effective practices from different sectors.

2.3. Analytical Framework

The analytical approach used both quantitative and qualitative methods. Qualitative data was analyzed using statistical tools such as Python and R for statistical modeling and trend analysis. This made it possible to detect the trends and connections between variables like cybersecurity spending and decreased losses. Risk management was the key area where simulation modeling was quite valuable in analyzing what-if scenarios, including the financial and operational consequences of ransomware or phishing attacks. Real-life data from previous accidents were incorporated to make these models as realistic as possible.

The open-ended questions were analyzed using thematic coding, whereby responses were grouped based on their thematic content. This was made easier by the use of NVivo software, which enables systematic organization and analysis of data. For example, during the analysis, several themes, including the complexity of incorporating higher technologies, resistance from the workforce, and compliance issues, came up and offered a background to the quantitative results.

2.4. Study Population and Sampling

The target organizations were drawn from the healthcare, finance, technology, and manufacturing industries due to their economic significance and susceptibility to supply chain cyber threats. The participants were recruited purposively to capture organizations of different sizes, ranging from small to large. This diversity offered a balanced view of the sector, including challenges peculiar to the sector and those affecting all stakeholders.

2.5. Tools and Techniques

Various techniques were employed to enhance credibility in measuring results. Quantitative analysis uses statistical software like Python and R to create regression models and trends. Tableau was utilized to build understandable and meaningful data visualizations about trends, and simulation modeling helped analyze potential ripple consequences of supply chain disturbances. In the qualitative analysis, NVivo software allowed a more structured approach in coding and categorizing the interviews to achieve the best thematic approach.

2.6. Performance Metrics

The performance of the cybersecurity measures was assessed using predetermined criteria. Economic losses averted were described as the percentage change in financial losses after the application of prevention measures. Operational resilience was measured in terms of downtime and recovery time, while threat detection systems were evaluated by the false positive and false negative rates. Such metrics offered an understanding of the correlation between investments and outcomes for organizations within cybersecurity.

2.7. Ethical Considerations

Accountability to persons was an essential component of the research process. Patient identity and data confidentiality were upheld, and all the participants' data was erased and stored by GDPR and CCPA guidelines. The participants were provided with details of the study objectives, procedures, and use of data to guarantee informed consent was taken. To ensure there was an element of accountability in the research process, the methodology, together with the findings of the study, was made clear.

2.8. Limitations

However, despite the methodological approach used in the study, some limitations cannot be ignored. Using survey and interview data increased the risk of bias as respondents' answers may not reflect the actual situation. The sample represents a good diversity, but more small organizations or less represented sectors may not be as adequately covered. Thirdly, the analysis was primarily concerned with the economic and operational effects of the decision within the short term, while the long-term consequences were ignored. These shortcomings will be addressed in future research to improve the external validity and richness of the studies.

3. RESULTS AND DISCUSSION

The findings of this research identify the significant impact of cybersecurity risks on supply chain economics and the efficiency of risk management techniques. The results of the current study are shown using data tables, charts, graphs, and a heatmap to give a clear insight into the study. In this section, these findings are elaborated further, especially in terms of their implications for industries, key players, and policies.

3.1. Economic Impact of Supply Chain Cyberattacks

Supply chain disruptions caused by cyber threats can have a significant economic impact, affecting financial performance, operational efficiency, and company reputation. These disturbances offer hazards that can spread throughout interconnected supply networks, exacerbating the damage. Table 1 depicts the expected annual economic losses in five vital sectors, allowing for a comparison of losses before and after the implementation of appropriate mitigation measures. This contrast emphasizes the need of proactive actions for reducing the economic damage caused by such dangers.

Table 1: Annual Economic Losses by Sector (in $ Billion).

Sector	Losses Without Mitigation	Losses with Mitigation	Reduction (%)
Manufacturing	25.4	15.8	37.8
Healthcare	18.6	10.4	44.1
Finance	22.3	12.5	43.9
Retail	14.2	9.1	35.9
Technology	30.1	17.4	42.2

The findings also show that sectors that handle sensitive data are projected to benefit the most from the adopted procedures, since they report the fewest losses, as indicated in Figure 1. Other industries, such as manufacturing and retail, have shown relatively smaller gains. However, these sectors continue to perform well since they rely less on real-time digital technologies than data-intensive industries.

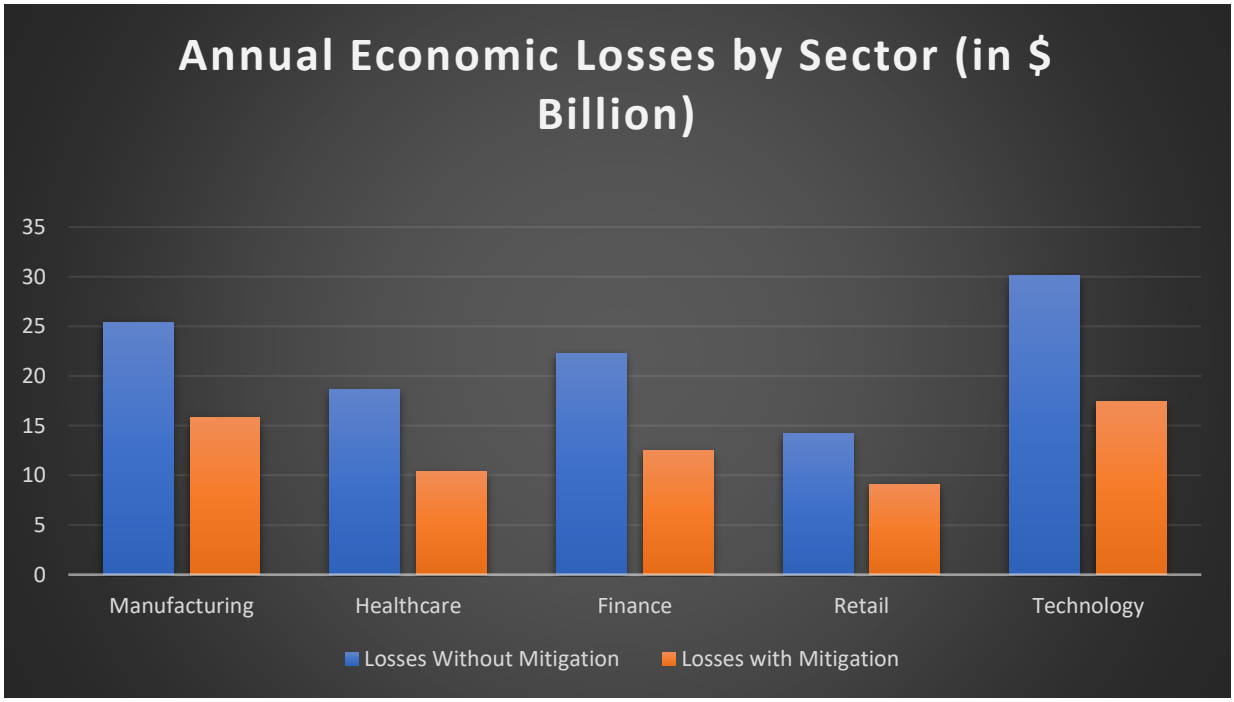


Figure 1: Annual economic losses.

3.2. Frequency and Types of Cyberattacks

The nature of attacks on supply chains also differs in that some attack methodologies are more frequent and potentially more damaging. Table 2 sorts the types of vulnerabilities and the percentage of reported incidents about the mentioned types.

Table 2: Frequency of supply chain cyberattacks by vulnerability type

Vulnerability Type	Percentage of Incidents (%)
Software Exploits	34
Network Intrusions	27
Insider Threats	18
Phishing Schemes	21

The most common form of attack detected is software exploitation, as shown in Fig. 2, emphasizing the crucial need for regular updates and patching to resolve vulnerabilities and avoid breaches. Other significant hazards include network invasions and phishing scams, highlighting the importance of strong firewalls, intrusion detection systems, and extensive user training to raise awareness and resilience to social engineering approaches.

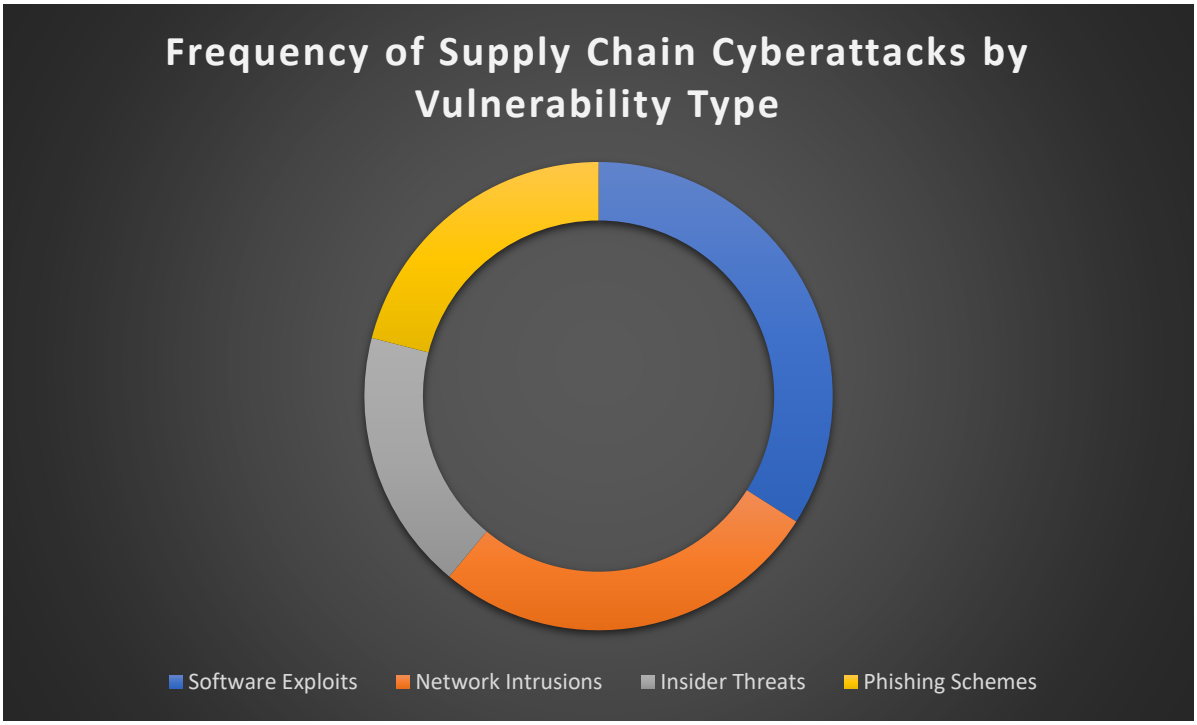


Figure 2: Frequency of supply chain cyberattacks by vulnerability type

3.3 | Operational Disruptions and Downtime

Cyberattacks can cause considerable disruptions, such as interrupting operations, incurring huge time losses, and putting businesses under financial strain. Table 3 shows a detailed breakdown of the average downtime and corresponding economic losses across important industries, illustrating the widespread impact of such accidents.

Table 3: Average Downtime and Economic Losses by Industry.

Industry	Downtime (Hours)	Economic Loss per Hour ($M)	Total Loss ($M)
Manufacturing	48	3.2	153.6
Retail	36	1.8	64.8
Healthcare	72	4.1	295.2
Technology	24	2.5	60.0

The healthcare industry has the greatest financial impact due to the vital nature of its operations and the need for ongoing functionality. Although manufacturing incurs slightly lower financial losses per hour, it suffers significant cumulative costs due to extended downtimes. Figure 3 shows a breakdown of downtime and economic losses across industries.

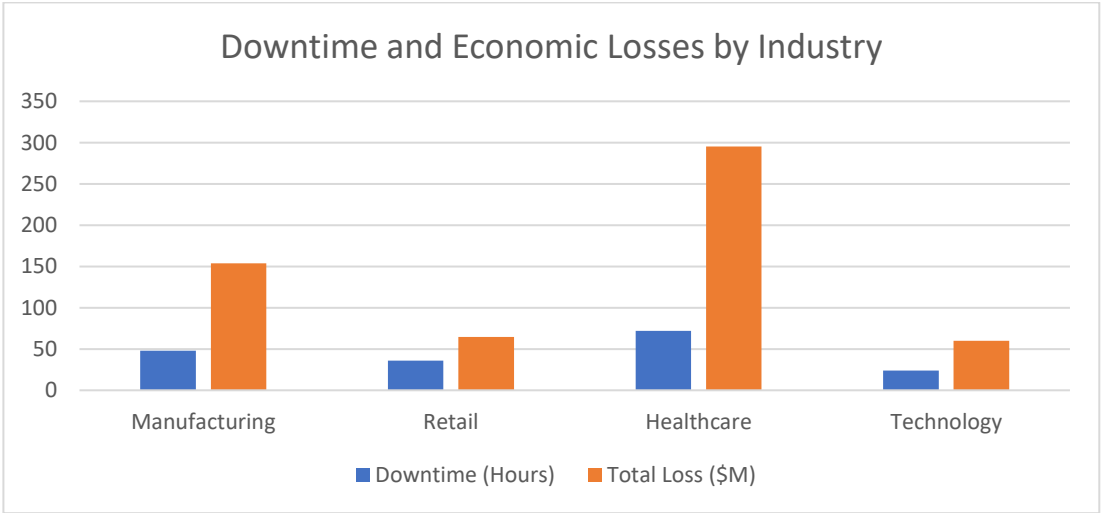


Figure 3: Downtime and Economic losses by industry

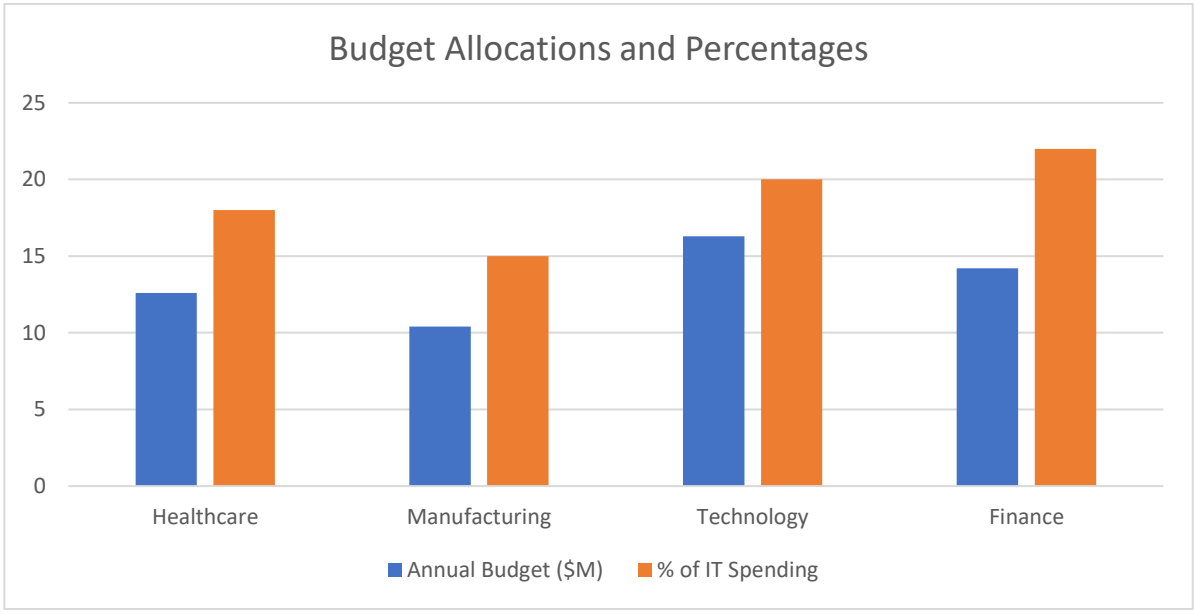
3.4. Cybersecurity Budgets and Effectiveness

Investment in cybersecurity is critical to an organization's capacity to successfully reduce risks and protect its operations. Table 4 shows the average yearly cybersecurity budget allocations in the healthcare industry, compared to other sectors, as well as their proportion to total IT spending, highlighting the growing relevance of cybersecurity across industries.

Table 4: Cybersecurity Budget Allocation by Sector.

Sector	Annual budget ($M)	% of IT spending
Healthcare	12.6	18
Manufacturing	10.4	15
Technology	16.3	20
Finance	14.2	22

Technology and finance allocate the highest proportions of their IT budgets to cybersecurity, reflecting their reliance on digital systems and sensitivity to breaches, presented in Fig. 4. Manufacturing invests comparatively less, suggesting potential vulnerabilities in less tech-focused operations.



3.5. Effectiveness of Mitigation Strategies

To evaluate the effectiveness of mitigation strategies, Table 5 provides a comprehensive summary of the performance of key approaches, drawing on both feedback from industry experts and operational data. This analysis highlights the strengths and weaknesses of each strategy, offering valuable insights into their real-world effectiveness and potential for improving overall risk management in various sectors.

Table 5: Mitigation Strategy Effectiveness.

Mitigation Strategy	Effectiveness (%)
Advanced Threat Detection	85
Employee Training	74
Vendor Risk Management	79

Figure 5 shows that, advanced threat detection emerges as the most effective strategy, highlighting the importance of real-time monitoring and AI-driven solutions. Employee training, while slightly less effective, remains a critical component, particularly for preventing phishing and insider threats.

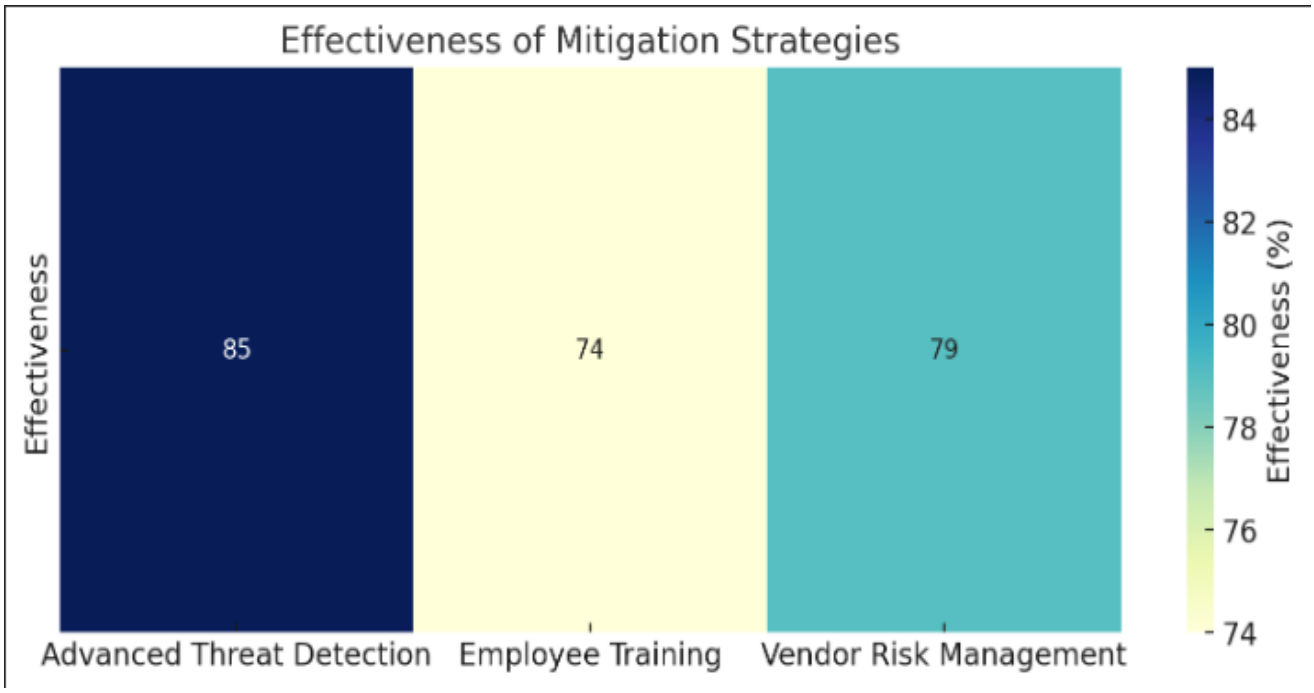


Figure 5: Effectiveness of mitigation strategies.

3.6. Discussion of Findings

These results stress the importance of cybersecurity in American industries, especially on the consequences of supply chain cyber threats. According to the data, sectors like healthcare, finance, and technologies have the most to gain from mitigation plans as they attract over 40% of economic losses from disasters. These results align with prior studies, like the National Institute of Standards and Technology (NIST), which reported that adopting strong cybersecurity investment considerably contributed to the substantial ROI in critical infrastructures (Cawthra et al., 2020). The disparity in resources discussed in the present study is consistent with the observations made by McKinsey & Company, which has noted a gap in cybersecurity spending between tech-savvy sectors and manufacturing and retail (Alissa et al., 2023). This difference emphasizes the need to have different approaches toward implementing the strategies to enhance the readiness level among sectors that have not embraced digitization.

The high rating of software exploits as the most common attack type is consistent with the data obtained in other studies, for example, the IBM Security Report, where un-updated software was identified as the cause of most breaches worldwide. This only underscores the necessity of frequent software upgrades and patching of the vulnerabilities. Furthermore, the focus of this study on operational downtime as a key cost factor is in line with Gartner's research that estimates that, for industries such as healthcare and manufacturing, one hour of unplanned downtime may cost millions of dollars and indicate the chain consequences of supply chain disruptions for sectors (Bahl, 2024).

AI and blockchain technologies were identified as promising in enhancing threat identification and increasing openness in operations. These findings are similar to previous research works by Xia et al. (2023) that highlighted the early warning system of AI and the potential of blockchain to strengthen the credibility and transparency of supply chain financial operations. However, this study also establishes some potential hindrances to using such technologies, as the cost of implementing the technologies is relatively high, and there is also the issue of integrating the existing technologies with the new ones. These barriers are often used in the literature, with the Forum (2024) pointing out that SMEs are the most affected by the lack of access to innovative cybersecurity services.

The programs established for training the employees highlighted in this study align with the research study conducted by the Ponemon Institute, which showed that human error is the leading cause of security breaches. As with this work and prior studies, it is crucial to develop a culture of cybersecurity to mitigate the risk of insiders and phishing threats. However, this study also emphasizes that training activities should be supported with technological measures to achieve overall protection.

Thus, the results are consistent with prior studies, focusing on the interaction between proactive resources, technological levers, and workforce capabilities to address supply chain risks. The study's findings support the previous evidence and expand the conversation by providing numerical values to a company's economic losses and risk reduction regarding particular sectors in the United States. These gaps include the allocation of resources and issues related to the application of technology that still need to be filled to improve the national cybersecurity posture.

4. CONCLUSION, RECOMMENDATIONS, AND FUTURE IMPLICATIONS

4.1. Conclusion

This study highlights the need for cybersecurity to protect the supply chains of major industries in the United States. It presents evidence that cyberattacks in supply chains are increasing in both the rate at which they occur and the level of complexity as they cause significant economic and operational disruptions. The study demonstrates that risk control measures such as threat identification, staff education, and vendor management help to lessen costs and improve organizational continuity.

Healthcare, finance, and technology sectors are most vulnerable to cyber risks because they involve handling valuable information and working in a real-time environment. However, industries that were less exposed to digital transformation, such as manufacturing and retail, have problems concerning the distribution of cybersecurity resources. New technologies, like artificial intelligence and blockchain, bring significant possibilities for increasing threat identification and procedural openness. However, challenges that prevent the implementation, especially among SMEs, show the need for more affordable and scalable solutions.

These results are consistent with previous studies, but they offer novel perspectives on the economic impact of cyber risks and the efficiency of protection measures. Moreover, there are still issues related to the distribution of resources, technology, and employee training to enhance national cybersecurity protection.

4.2. Recommendations

To mitigate cybersecurity risks and enhance supply chain resilience, this study proposes the following recommendations:

i. Prioritize Proactive Investments in Cybersecurity
Managers should dedicate higher proportions of their IT budgets to cybersecurity solutions, especially in industries vulnerable to cyber criminals. The use of sophisticated equipment, such as artificial intelligence in threat detection and blockchain in operational management, will help enhance threat detection and organizational clarity.

ii. Enhance Workforce Training Programs
Cybersecurity training is vital for minimizing risks from human factors, including phishing and insider threats. Managers need to conduct training sessions to enhance cybersecurity within their organizations and ensure their employees can identify potential threats.

iii. Adopt Holistic Cybersecurity Frameworks
Such solutions as zero-trust architecture and Cybersecurity Maturity Model Certification (CMMC) can help establish common security practices. Such frameworks should be adjusted to the sector's requirements and include third-party risk management to cover all the processes.

iv. Increase Accessibility of Advanced Technologies
The government and private companies should work together to reduce the entry barriers to adopting innovative solutions such as AI and blockchain. The following solutions can be used to popularize these tools and improve the situation: subsidies, PPPs, and tools that can be implemented on a large scale focusing on SMEs.

v. Foster Public-Private Collaboration
Both government agencies and companies can no longer afford to act independently, but there must be an exchange of threat information and the development of synchronized response procedures. Initiatives like industry-wide information-sharing platforms can enhance real-time threat detection and response.

vi. Strengthen Regulatory Compliance and Standards
Regulatory bodies enhance compliance standards to reflect on new threats and technologies. This entails updating IoT security standards, data protection rules, and vendor risk assessment to meet emerging cyber threats.

4.3. Future Implications

The findings of this research go beyond the direct application of the identified solutions to the problem of cybersecurity in supply chains. It offers an approach that can be used to tackle future problems systematically. The growth of digital transformation in industries will increase the attack vectors for cyber threats, hence the need for constant advancements in security solutions. Quantum computing and the next generation of AI will become the key drivers of supply chain protection in the future. However, their successful integration will only be possible if current challenges, such as high costs and scarcity of skills, are tackled.

Globalization of supply chains explains why there is a need for cooperation between nations in matters concerning cybersecurity. Future studies should focus on global structures and partnerships to achieve better compliance with security measures. Also, the changes in the regulatory environment, triggered by the GDPR and the recent Executive Orders on cybersecurity in the United States, are likely to challenge organizations.

From a societal standpoint, improving supply chain cybersecurity will help secure infrastructure, defend customer information, and promote economic resilience. Furthermore, implementing fair cybersecurity solutions

for SMEs will help eliminate such gaps and create a more robust economy.

Finally, there is a need to examine the future effects of emerging technologies and cybersecurity policies on the global supply chain. Since ethics will play an important role in the future development of technologies, more research on issues like algorithm bias and user privacy invasion will be needed to guide the direction of technology in a way that is most beneficial to society. From these challenges and opportunities, stakeholders can fashion a safe, stable, and sustainable future for global supply chains.

REFERENCES

Akter, T., Samman, A. S. A., Lily, A. H., Rahman, M. S., Prova, N. N. I., & Joy, M. I. K. (2024, 24-28 June 2024). Deep Learning Approaches for Multi Class Leather Texture Defect Classifcation. 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT),

Alissa, A., Begonha, D., Braga, D., Espírito Santo, H., Boehm, J., Candina, J., Vieira, B., & Richter, W. (2023). How to enhance the cybersecurity of operational technology environments. *McKinsey & Company*.

Arroyabe, M. F., Arranz, C. F. A., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826. https://doi.org/https://doi.org/10.1016/j.cose.2024.103826

Bahl, R. (2024). *How to guard against the cost of unplanned downtime and network outages. Forbes.* Forbes. https://www.forbes.com/councils/forbestechcouncil/2022/08/26/how-to-guard-against-the-cost-of-unplanned-downtime-and-network-outages/

Biswas, B., Mohammad, N., Prabha, M., Jewel, R. M., Rahman, R., & Ghimire, A. (2024). Advances in Smart Health Care: Applications, Paradigms, Challenges, and Real-World Case Studies. 2024 IEEE International Conference on Computing, Applications and Systems (COMPAS),

Bruce, G. J. (2023, 2023//). Cybersecurity Compliance Requirements for USA Department of Defense Contractors - Dragons at the Gate. HCI for Cybersecurity, Privacy and Trust, Cham.

Cawthra, J. L., Ekstrom, M. R., Lusty, L. N., Sexton, J. T., Sweetnam, J. E., & Townsend, A. R. (2020). Data integrity: Identifying and protecting assets against ransomware and other destructive events.

Cheung, K.-F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, 102217. https://doi.org/https://doi.org/10.1016/j.tre.2020.102217

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, *27*(1), 30-53. https://doi.org/10.1108/SCM-02-2020-0073

Dudley, R., & Golden, D. (2021). The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms. *ProPublica (24 May 2021)*.

Forum, W. E. (2024). Here's how smes can turn cybersecurity risk into opportunity. https://www.weforum.org/stories/2024/07/smes-can-turn-cybersecurity-risk-into-opportunity-heres-how/

Ghimire, A., Imran, M. A. U., Biswas, B., Tiwari, A., & Saha, S. (2024). Behavioral Intention to Adopt Artificial Intelligence in Educational Institutions: A Hybrid Modeling Approach. *Journal of Computer Science and Technology Studies*, *6*(3), 56-64.

Gia, A., & Fitria, W. (2024). SolarWinds Attack: Stages, Implications, and Mitigation Strategies in the Cyber Age. *Electronic Integrated Computer Algorithm Journal*, *2*(1), 47-52. https://doi.org/10.62123/enigma.v2i1.31

Gorgun, E., & Karamis, M. B. (2019). Ultrasonic testing to measure the stress statement of steel parts. *Journal of Mechanical Science and Technology*, *33*, 3231-3236.

Haklai, B. (2023). Cybersecurity Private-Public Partnerships: A Bridge to Advance Global Cybersecurity. *Tex. Tech L. Rev.*, *56*, 627.

Hasan, R., Al Mahmud, M. A., Farabi, S. F., Akter, J., & Johora, F. T. (2024). Unsheltered: Navigating California's homelessness crisis. *Sociology Study*, *14*, 143-156.

Hasan, R., Chy, M. A. R., Johora, F. T., Ullah, M. W., & Saju, M. A. B. (2024). Driving Growth: The Integral Role of Small Businesses in the US Economic Landscape. *American Journal of Industrial and Business Management*, *14*(6), 852-868.

Hasan, R., Farabi, S. F., Kamruzzaman, M., Bhuyan, M. K., Nilima, S. I., & Shahana, A. (2024). AI-Driven Strategies for Reducing Deforestation. *The American Journal of Engineering and Technology*, *6*(06), 6-20.

Hossain, M. A., Tiwari, A., Saha, S., Ghimire, A., Imran, M. A. U., & Khatoon, R. (2024). Applying the Technology Acceptance Model (TAM) in Information Technology System to Evaluate the Adoption of Decision Support System. *Journal of Computer and Communications*, *12*(8), 242-256.

Imran, M. A. U., Aziz, M. B., Tiwari, A., Saha, S., & Ghimire, A. (2024). Exploring the Latest Trends in AI Technologies: A Study on Current State, Application and Individual Impacts. *Journal of Computer and Communications*, *12*(8), 21-36.

Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Al Mahmud, M. A. (2024). AI-Powered Fraud Detection in Banking: Safeguarding Financial Transactions. *The American Journal of Management and Economics Innovations*, *6*(06), 8-22.

Johora, F. T., Manik, M. M. T. G., Tasnim, A. F., Nilima, S. I., & Hasan, R. (2021). Advanced-Data Analytics for Understanding Biochemical Pathway Models. *American Journal of Computing and Engineering*, *4*(2), 21-34.

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/https://doi.org/10.1016/j.inffus.2023.101804

Kuipers, S., & Schonheit, M. (2022). Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises. *Corporate Reputation Review*, *25*(3), 176-197. https://doi.org/10.1057/s41299-021-00121-9

Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *DOI: https://www. doi. org/10.56726/IRJMETS32644*, *1*.

Monjur, M. E. I., & Akon, T. (2023). Supply chain management and logistics: How important interconnection is for business success. *Open Journal of Business and Management*, *11*(5), 2505-2524.

Parraguez-Kobek, L., Stockton, P., & Houle, G. (2022). Cybersecurity and Critical Infrastructure Resilience in North America. *Forging a Continental Future*, 217.

Pavelea, A., & Negrea, P.-C. (2024). *A Comprehensive Analysis of High-Impact Cybersecurity Incidents: Case Studies and Implications* Masters thesis. Babeş–Bolyai University. doi: 10.13140/RG. 2.2. 17461.65763].

Prova, N. N. I. (2024, 28-30 Aug. 2024). Garbage Intelligence: Utilizing Vision Transformer for Smart Waste Sorting. 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI),

Prova, N. N. I. (2024, 3-5 Oct. 2024). Improved Solar Panel Efficiency through Dust Detection Using the InceptionV3 Transfer Learning Model. 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),

Rauniyar, K., Wu, X., Gupta, S., Modgil, S., & Lopes de Sousa Jabbour, A. B. (2023). Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology. *Industrial Management & Data Systems*, *123*(1), 253-277. https://doi.org/10.1108/IMDS-04-2021-0235

Şenol, H., Çakır, İ. T., Bianco, F., & Görgün, E. (2024). Improved methane production from ultrasonically-pretreated secondary sedimentation tank sludge and new model proposal: Time series (ARIMA). *Bioresource technology*, *391*, 129866.

Şenol, H., Erşan, M., & Görgün, E. (2020). Biogas production from the co-digestion of urban solid waste and cattle manure. *Avrupa Bilim ve Teknoloji Dergisi*, 396-403.

Şenol, H., Oyan, M., & Görgün, E. (2024). Increasing the biomethane yield of hazelnut by-products by low temperature thermal pretreatment. *Süleyman Demirel University Faculty of Arts and Science Journal of Science*, *19*(1), 18-28.

Singh, S., & Kumar, D. (2024). Enhancing cyber security using quantum computing and artificial intelligence: A review. *algorithms*, *4*(3).

Susitha, E., Jayarathna, A., & Herath, H. M. R. P. (2024). Supply chain competitiveness through agility and digital technology: A bibliometric analysis. *Supply Chain Analytics*, *7*, 100073. https://doi.org/https://doi.org/10.1016/j.sca.2024.100073

Wang, P., D'Cruze, H., & Wood, D. (2019). ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES. *Issues in Information Systems*, *20*(2).

Xia, J., Li, H., & He, Z. (2023). The Effect of Blockchain Technology on Supply Chain Collaboration: A Case Study of Lenovo. *Systems*, *11*(6).