Group 1

Supply Chain Management (IS228 - B)

Implementation of Cybersecurity

in Protecting SCM from Cyberattacks

Group Members:

- Alessandra Valentina (75386)
- Kenny Budiarso Lawson (81065)
- Sabrina Nurul Azmi (77730)

Overview

- Background
- PRISMA Flow Process
- Problem Objectives
- Critical Factor Issues
- Research Questions

- Conclusion
- Recommendation (App Prototype)
- Future Work
- SLR Article

Background

Recently, The supply chain has increasingly dependent on IT and communication in managing operations. This is certainly a challenge because the process involves many parties starting from the production stage, shipping and distribution of goods to consumers. This process is vulnerable to cyber attacks such as data theft, and even virus attacks. In 2020, there was an attack on the software at SolarWinds where the sensitive data of users using the software was compromised, affecting operations and users' trust in Orion, the application developer.

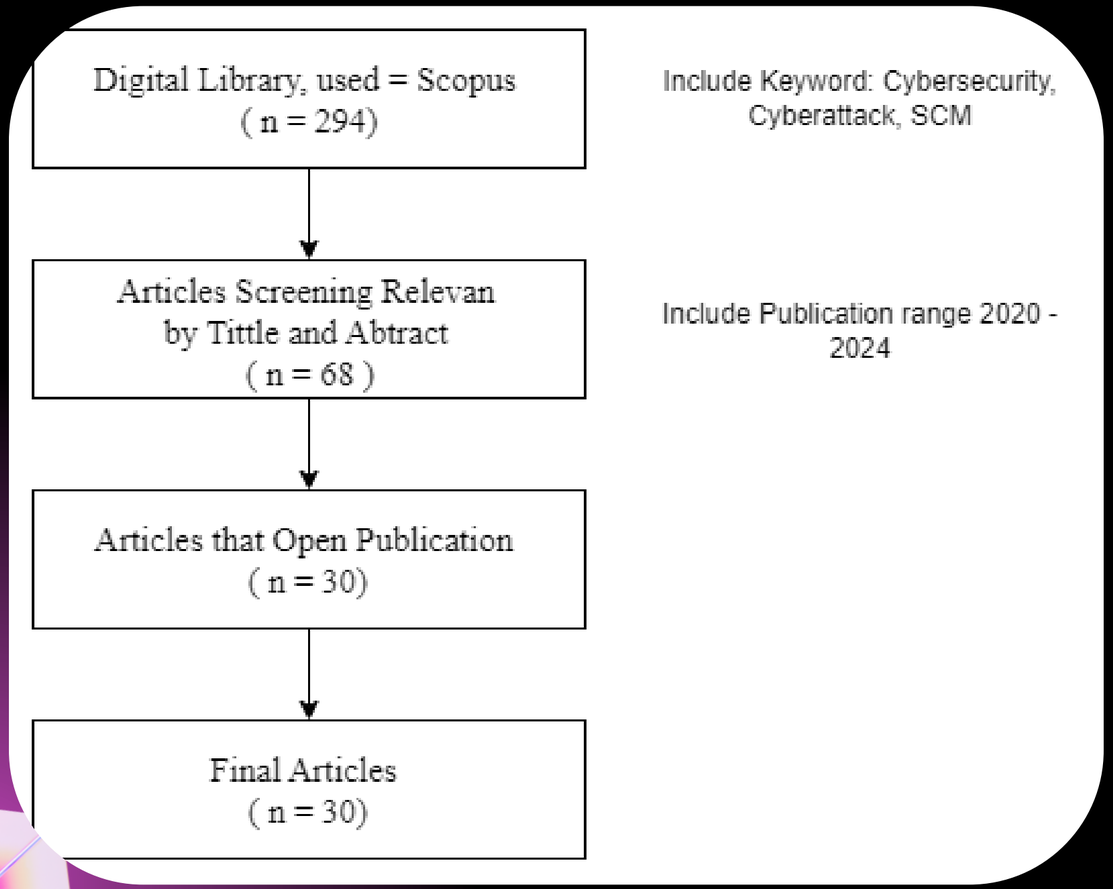
Therefore, it is necessary to develop strong cybersecurity to protect the supply chain from cyber attacks such as encrypting data, collaborating with various departments, especially cyber agencies, integrating to ensure data security, implementing cybersecurity technologies, one of which is blockchain and Digital Twin to improve data security and privacy and managing risks to mitigate cyber attacks.

PRISMA

PRISMA Process Sheets

Group 1

Flow Process



1.Unfiltered article collections
(Total = 294 articles)

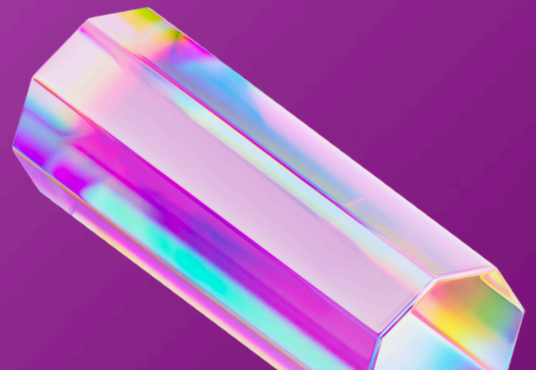
2.Title & Abstract Screening
~ Related to SCM, Cybersecurity, and Cyberattacks
(Only 65 is related)

3.Only 30 articles can be opened & accessed, the other were privately access

4.All 30 articles are related and has been stated as the collection of reviewed articles

Problem Objectives

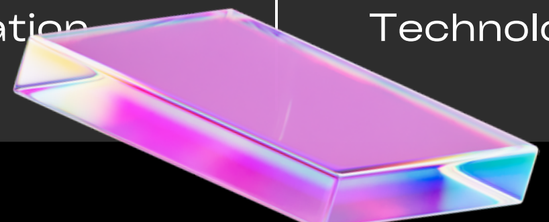
- **Identify, analyze, and provide solutions to cybersecurity challenges in the supply chain** with a focus on emerging technologies such as blockchain, IoT, and cloud computing.
- **Implement new approaches to cyber risk mitigation** through the application of advanced technology, dynamic theory, and collaboration between various parties.
- **Improve supply chain resilience and reliability by mitigating cyber** threats that can damage a company's operations, finances, and reputation.



Back to Agenda Page

Critical Factor Issues

Collaboration	Technology	AI & IoT Integration	Organization & People
Involves effective cooperation among stakeholders to enhance security and mitigate risks. • Supplier-Organization Collaboration • Increasing coordination and transparation	The use of digital tools to support efficiency, security, and transparency. • Quantum Computing • Blockchain • Encryption Cybersecurity • Big Data Technology • Cryptography Technology	Combines AI and connected devices to improve threat response and operational efficiency. • AI-Powered Attacks Detector • IoT connected in manage and controlling supply chain	Involves readiness and involvement of the organization and its employees in cybersecurity efforts. • Routine Staff Training • Transparency in Management and Monitoring • Comprehensive Risk Mitigation



Group 1

Research Questions

Based on the Critical Factors

1. How can multi-actor collaboration in the supply chain effectively enhance cybersecurity?
2. What is the impact of technology usage on transparency and data security in supply chain management?
3. How can the integration of AI and IoT optimize real-time response to cybersecurity threats?
4. What are the key factors influencing the effectiveness of risk mitigation strategies in the context of cybersecurity within the supply chain?

Group 1

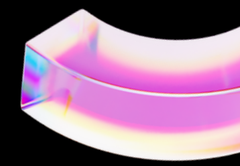
Answer of Research Questions

1

Strong collaboration between actors in the supply chain, such as suppliers, distributors and customers, has proven effective in improving cybersecurity. This is achieved through real-time exchange of threat information, implementation of common security standards, and strengthening training and awareness of potential attacks. Technologies such as blockchain strengthen this collaboration by creating transparency and accountability in transactions.

2

The use of modern technologies such as blockchain, big data analytics, and AI has a significant impact on data transparency and security. On the one hand, these technologies improve data logging reliability and threat detection capabilities. However, on the other hand, the implementation of technology also presents new challenges, such as the need to protect IoT devices that are prone to attack.



Group 1

Answer of Research Questions

3

The combination of AI and IoT provides an effective solution for dealing with cyber threats in real-time. Continuous monitoring by IoT and AI-based predictive analytics enable early detection and automated response to threats. This speed and accuracy reduces the negative impact of attacks on supply chain operations.

4

The success of cybersecurity risk mitigation in the supply chain is influenced by several key factors. Support from organizational leadership plays a critical role in ensuring adequate resource allocation for addressing cybersecurity challenges. Additionally, a comprehensive risk evaluation, which involves identifying and prioritizing risks across the entire supply chain, helps organizations gain a thorough understanding of potential threats. The use of reliable security technologies, such as firewalls, intrusion detection systems, and data encryption, is essential for protecting systems. Collaboration with external parties, including cybersecurity service providers, also contributes to more effective threat management. On the human resources side, capacity building through regular training equips employees to better recognize and handle cybersecurity threats. Lastly, compliance with applicable security standards and regulations ensures that risk mitigation strategies align with legal requirements. Together, these factors form the foundation for effective cybersecurity risk mitigation within the supply chain.

Conclusion

Strong collaboration among supply chain actors, supported by technologies like blockchain, big data analytics, and AI, enhances cybersecurity through real-time threat sharing, standardized security measures, and improved awareness. These technologies boost data transparency, threat detection, and automated responses while posing new challenges, such as securing IoT devices. The integration of AI and IoT enables real-time monitoring, early detection, and swift action, minimizing the impact of cyber threats on supply chain operations.

Recommendation

BeaCukai Mobile UI/UX Design Prototype

Figma Prototype

Future Works

For future research, it is expected to develop the prototype that has been made into an application / website

Thank You!

Do you have any question?

Cybersecurity in Protecting Supply Chain Management from Cyberattacks

Group 1