JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Impact of Cyber Security measurements adopted by supply chain management companies in Navi Mumbai

Dr. Pushpendu Rakshit,

Research Scholar, Post Doc, Singhania University, Pacheribari, Rajasthan, India.

Abstract

This study investigates how cyber-attacks affects supply chain management in the cosmopolitan city of Navi Mumbai. This is also known for its commercial value and adoption of latest trends in technology. Cybersecurity has grown to be a major worry as supply chain management uses technology more and more. In the study, the risks of cybersecurity vulnerabilities in the supply chain are examined, including third-party risks, data breaches, business disruptions, and regulatory obligations. The initiative also looks into the steps businesses can take to reduce these risks, including putting in place security procedures, routine risk assessments, and staff cybersecurity training. This study is post-doctoral in nature. The research's conclusions shed light on the significance of cybercrime for supply chain management and emphasize the necessity for businesses to give cybersecurity measures top priority in their supply chain operations.

Keywords – SCM, SCM 4.0, Cybercrimes, Cyber security, Navi Mumbai, Cyber literacy.

Introduction

Supply Chain can be defined as the flow of the goods and the services which includes the finance, data, procurement raw material supply to the delivery of the final product at the final warehouse of the particular client. The supply chain has been in a great demand for the todays century. Many of them compare the logistics with the Supply Chain which is wrong as the Logistics is one of the part of the Supply Chain. Supply Chain includes the production, distribution through different channels, logistics, warehousing, printing packaging and labelling, transportation etc. It is clear that the rate and cost of data breaches are increasing. Since 2001, the victim count has increased from 6 victims per hour to 97, a 1517% increase over 20 years.

The average cost of data breaches per hour worldwide has also increased. In 2001, the average cost per hour to individuals was $2054. Since then, the hourly loss rate has increased, standing in 2021 at $787,671. The increasing threat to organisations globally means more are taking cyber security seriously. 73% of SMBs agree that cyber security concerns now need action, with 78% saying they will increase investment in cyber security in the next 12 months.

A concerning statistic is that 67% of SMBs feel that they do not have the in-house skills to deal with data breaches. However, this issue is mitigated as increasing numbers of SMBs are working with Managed Service Providers for cyber security; 89% as of 2022, up from 74% in 2020.

In 2022, investment fraud was the most costly form of cyber crime, with an average of $70,811 lost per victim. In 2022, data breaches cost businesses an average of $4.35 million – up from $4.24 million in 2021. The pandemic affected cyber security as businesses were forced to rapidly move to remote work environments. Cyber criminals took advantage of network misalignments and security gaps as these transitions happened. In 2020, malware attacks increased 358% compared to 2019.

Covid-19 clearly impacted the number of hourly victims. 2019 cyber crime statistics show the hourly number of victims was 53. In 2020, the first full year of the pandemic, the hourly number of victims jumped to 90, an increase of 69%. 2021 saw an average of $787,671 lost every hour due to data breaches.

The acceleration towards digital-first solutions was brought upon by the COVID-19 pandemic and the worldwide supply chain disruption it caused. Without getting too bogged down in the specifics, vital paperwork – including invoices, bills of lading, compliance certificates, shipment documents, and so on – is transitioned to the cloud. As such, processes and relationships between buyers, intermediaries and suppliers that were historically fostered with face-to-face or in-person interactions became predominantly digitised.

Broadly speaking, the increased digitisation of the logistics sector has created exponentially larger and more vulnerable attack surfaces between parties throughout supply chains. Simultaneously, the threat landscape has expanded to such a degree that malicious actors and cybercriminals can execute attacks with minimal interference or detection, leaving vendors without the cyber knowledge or infrastructure to contain them, or prevent valuable assets or information from being exploited.

Post-pandemic, supply chain fraud rose by 13% year-on-year, according to recent statistics, inflicting immense financial and regulatory pressure on both suppliers and buyers within geospatially-linked supply chains. As more parties upskill in proper cyber etiquette and invest in proactive threat containment and incident response solutions, it begs the question of what each connected party within any given supply chain can do to ensure the greater protection of important data, while minimising the attack surface.

This boils down to understanding the threats to watch out for in the increasingly digital supply chains of today, recognising the potential impact they can cause, making the most informed conscious decisions on supplier relationships, and investing properly in the right cyber defence strategies to protect all parties as much as possible.

Cybersecurity in SCM

The technique of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious assaults is known as cyber security. It is also referred to as information technology security or computer data protection. The word is used in a variety of settings, ranging from business to mobile devices, and can be classified into a few general categories.

Network security is the practice of protecting a computer network from invaders, whether they are specific assailants or opportunistic viruses. Application security is concerned with keeping software and gadgets free of threats. A compromised program may allow access to the data it is supposed to safeguard. Security starts in the planning stage, long before a program or device is launched. Information security safeguards the integrity and privacy of data while it is in storage and transit.

Operational security encompasses the processes and choices used to manage and secure data assets. This includes the permissions that users have when connecting to a network as well as the processes that govern how and where data can be kept or shared. Disaster recovery and business continuity describe how an organization reacts to a

cyber- security attack or any other event that results in the loss of activities or data. Disaster recovery policies govern how an organization returns its operations and information to the same operational capability as before the incident.

As companies depend on a complicated network of suppliers, vendors, and partners to deliver products and services to consumers, cybersecurity is becoming a more crucial component of supply chain management. The process of locating, evaluating, and minimizing cybersecurity threats within the supply chain is referred to as cybersecurity in supply chain management research.

Finding possible risks is the first stage in a supply chain cybersecurity study. This can be accomplished by conducting a risk evaluation process that takes into account all of the suppliers, contractors, and partners who are a part of the supply chain, as well as the kinds of information and systems that are being exchanged among them. In the supply chain, some typical hacking threats include:

- *Cybercriminals may be able to access confidential data or systems by taking advantage of the cybersecurity flaws of third-party suppliers and partners.*
- *Employees of partners, suppliers, and contractors who have access to private information or networks and decide to abuse that access may be considered insider risks.*
- *Cybercriminals may target the supply chain directly in an effort to compromise one or more partners or vendors and obtain entry to the larger network of the supply chain.*
- *Assessing each risk's likelihood and impact comes next after the possible risks have been found. This can be achieved through a quantitative or intuitive risk evaluation method that takes into account both the probability of an event happening and its possible effects on the company.*

Finally, it's critical to create a mitigation plan to lessen the probability and effects of cybercrime risks in the supply chain after the risks have been discovered and evaluated. Implementing organizational and technological controls, such as educating staff on cybersecurity best practices and performing routine evaluations of partners and vendors, may be necessary to achieve this.

Overall, supply chain management research cybersecurity is a crucial part of contemporary company processes. By finding and reducing possible cybersecurity risks in the supply chain, businesses can help secure their confidential data and systems from hackers and ensure the ongoing success of their operations.

Why Cybersecurity is essential in the supply chain management

- Sensitive Data Protection: - Supply chain companies deal with a lot of confidential data, such as financial information, client information, and intellectual property. Cyber assaults may compromise this info, resulting in monetary loss and reputational harm to the company.
- Preventing disruption: Cyberattacks have the potential to interrupt the supply chain by causing key activities to be delayed, disrupted, or shut down. Significant financial losses and delays in the supply of products or services may result from these interruptions.
- Maintaining legal compliance: Supply chain companies must adhere to a variety of laws, rules, and guidelines, including data security laws and regulations unique to their business. To guarantee adherence to these rules, cybersecurity steps are required.
- Managing third-party risks: Supply chain companies deal with a variety of suppliers and partners from outside the company. The organization's data and systems may be compromised as a result of cyberattacks against these suppliers. By putting cybersecurity measures in place, these risks can be reduced and the organization can be shielded from the consequences of third- party attacks.

Overall, the supply chain sector needs cybersecurity to safeguard confidential information, avert disruptions, uphold legal compliance, and reduce third-party risks.

Some of the major cyber risks that can drastically affect logistics firms include (but are not limited to):

- Ransomware: A type of malware that prevents users from accessing critical systems or files until a ransom is paid. According to recent research, ransomware is one of the fastest-growing types of cybercrime and is expected to syphon $265 billion every year by 2031.

- Phishing: A type of socially engineered cybercrime when malicious actors disguise themselves as known entities/individuals, deceiving users into divulging important logins, credentials, or financial information, or downloading malicious files that cripple systems and networks. Phishing attacks are usually executed via email, telephone, or SMS messages, or a hybrid of them all.

- Brute force: Calculated attacks triggered by malicious actors and armies of 'bots' attempting to crack login credentials and passwords ad infinitum, and gain access to sensitive files and information.
- MITM (Man-in-the-Middle) attacks: An umbrella term for situations when perpetrators position themselves between users and applications, usually in an attempt to impersonate one of the parties or eavesdrop on conversations.
- DDoS (Distributed Denial-of-Service): Malicious attempts to disrupt the normal traffic of targeted networks or servers by overwhelming the target and infrastructure with floods of 'traffic', preventing regular users from accessing systems they need.

Need for Research on Cybersecurity in Supply Chain

Research on supply chain cybersecurity is urgently needed, since the digitization of supply chain operations has raised the risk of cyberthreats and assaults. Cybersecurity in the supply chain is a serious problem that has to be addressed by academics, legislators, and business professionals. The following are some justifications for why this field needs more study:

- Rise in cyber threat risk: As supply chains grow more intricate and integrated, there is an increase in cyber threat risk. Attacks on the supply chain can have a considerable negative impact on the economy and operations, resulting in data breaches, financial losses, and delays in production and delivery.
- Lack of cybersecurity standards: It is challenging to evaluate and manage risk since there is a lack of uniform cybersecurity standards throughout the supply chain. The development of best practises and guidelines to direct supply chain players in addressing cybersecurity risks can be aided by research.
- Technology that is advancing quickly: As new technologies are incorporated into supply chain operations, supply chains are becoming more vulnerable. The development of remedies to reduce growing cybersecurity concerns can be aided by research.
- Regulatory compliance: Supply chain stakeholders must be aware of and adhere to the numerous cybersecurity legislation and compliance standards that apply to various businesses. Research may enhance compliance efforts and help lawmakers understand the need for new legislation.

Resilience in the supply chain is becoming more and more important since it may have a big impact on businesses and the overall economy. Effective management of cybersecurity risks is required to ensure the resilience of supply chains. Strategies for improving supply chain resilience in the face of cyber threats can be developed with the use of research. The management of the rising risk of cyberthreats and guaranteeing the resilience of supply chains depend on research on cybersecurity in supply chains. It may offer perceptions into new dangers, help with the creation of best practises and standards, and aid in compliance initiatives.

A literature review on cybersecurity in supply chain management reveals a growing concern for the security of interconnected systems and the potential vulnerabilities that arise from digital integration. Here's a synthesized overview of key themes and findings from recent research:

- Cyber Threat Landscape in Supply Chains:

Scholars emphasize the increasing sophistication and diversity of cyber threats targeting supply chain networks. Various attack vectors, including malware, phishing, ransomware, and supply chain manipulation, pose significant risks to organizations' operations and data integrity.

- Risk Assessment and Management:

Research underscores the importance of proactive risk assessment and management strategies to identify vulnerabilities and mitigate potential cyber threats. Scholars advocate for the adoption of risk management frameworks and methodologies tailored to the unique characteristics of supply chain environments.

- Vendor and Third-Party Risk Management:

There's a growing recognition of the need to address cybersecurity risks associated with third-party vendors and suppliers.

Studies emphasize the importance of implementing robust vendor risk management practices, including due diligence, contractual agreements, and ongoing monitoring of vendor cybersecurity posture.

- Information Sharing and Collaboration:

Collaboration among supply chain partners and stakeholders is essential for effectively managing cybersecurity risks. Scholars highlight the benefits of information sharing mechanisms, such as threat intelligence sharing platforms and collaborative defense initiatives, in enhancing collective resilience against cyber threats.

- Technological Solutions and Innovations:

Advances in cybersecurity technologies, such as blockchain, encryption, intrusion detection systems, and artificial intelligence, offer promising avenues for enhancing supply chain security. Research explores the potential applications of these technologies in securing supply chain data, ensuring data integrity, and mitigating cyber risks.

- Regulatory Compliance and Standards:

Regulatory requirements and industry standards play a crucial role in shaping cybersecurity practices within supply chains. Scholars examine compliance frameworks, such as GDPR, NIST, ISO 27001, and industry-specific regulations, and their implications for supply chain security management.

- Organizational Culture and Awareness:

Building a cybersecurity-aware culture within organizations and across supply chain networks is essential for mitigating human-related risks, such as insider threats and social engineering attacks. Research emphasizes the role of training, awareness programs, and stakeholder engagement in fostering a cybersecurity-conscious workforce.

- Resilience and Incident Response:

Supply chain resilience involves the ability to withstand and recover from cyber incidents effectively. Scholars explore strategies for enhancing supply chain resilience, including contingency planning, incident response preparedness, and post-incident recovery efforts.

Challenges and Future Directions:

Despite ongoing efforts to improve supply chain cybersecurity, several challenges persist, including resource constraints, interoperability issues, and the evolving nature of cyber threats.

Resource Constraints

High Costs: Implementing advanced cybersecurity measures can be expensive, which may be a barrier for small and medium enterprises (SMEs) (Kumar & Reddy, 2020).

Lack of Skilled Personnel: There is a shortage of cybersecurity professionals with expertise in SCM, which hinders effective implementation of security measures (Joshi & Naik, 2021).

Rapid Technological Changes

Keeping Up with Emerging Threats: The fast pace of technological advancements and evolving cyber threats require continuous updates and improvements in cybersecurity measures (Mehta & Patel, 2020).

Complexity of Supply Chains

Interconnected Systems: The interconnected nature of modern supply chains makes it challenging to secure all points of vulnerability, especially with multiple third-party vendors involved (Deshmukh & Shukla, 2019).

The need for cybersecurity in supply chain management has become increasingly critical due to several factors:

- Interconnectedness and Complexity: Modern supply chains are highly interconnected and complex, involving multiple stakeholders, partners, and systems. This interconnectedness increases the potential attack surface for cyber threats, as vulnerabilities in one part of the supply chain can cascade and affect others.
- Dependency on Digital Technologies: The digitalization of supply chain processes has led to increased reliance on digital technologies, such as cloud computing, Internet of Things (IoT) devices, and data analytics. While these technologies offer benefits such as improved efficiency and visibility, they also introduce new cybersecurity risks, including data breaches, malware attacks, and supply chain manipulation.
- Data Protection and Privacy Concerns: Supply chains involve the exchange of sensitive information, including intellectual property, customer data, and financial records. Protecting this data from unauthorized access, theft, or tampering is essential to maintain trust and compliance with data protection regulations, such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Protection Act).
- Globalization and Outsourcing: Globalization has led to the expansion of supply chains across geographic boundaries, involving suppliers, manufacturers, and distributors from diverse regions. This globalization increases the complexity of supply chain cybersecurity, as organizations must manage risks associated with partners operating in different regulatory environments and with varying cybersecurity maturity levels.
- Third-Party Risks: Supply chains often rely on third-party vendors, suppliers, and service providers to deliver goods and services. However, these third parties can introduce cybersecurity risks if their systems or processes are compromised. Managing third-party risks requires organizations to implement robust vendor risk management practices and ensure that suppliers adhere to cybersecurity standards.
- Regulatory Requirements: Governments and regulatory bodies are increasingly imposing cybersecurity requirements and regulations on organizations to protect sensitive information and mitigate cyber threats.

Non-compliance with these regulations can lead to financial penalties, legal liabilities, and reputational damage for organizations operating within supply chains.

- Cyber Threat Landscape: The evolving nature of cyber threats poses a significant challenge to supply chain security. Threat actors, including hackers, cybercriminals, and nation-state actors, continuously develop sophisticated attack techniques to exploit vulnerabilities in supply chain systems and networks. Organizations must stay vigilant and adapt their cybersecurity defenses to address emerging threats effectively.
- Business Continuity and Resilience: Supply chain disruptions caused by cyber incidents can have severe consequences for business continuity and resilience. Cyberattacks, such as ransomware, distributed denial-of-service (DDoS) attacks, or supply chain manipulation, can disrupt operations, lead to financial losses, and damage brand reputation. Ensuring the resilience of supply chains against cyber threats requires proactive risk management and contingency planning. Cybersecurity is essential in supply chain management to protect sensitive data, ensure business continuity, maintain regulatory compliance, and mitigate the growing threats posed by cyberattacks and digital vulnerabilities. Organizations must prioritize cybersecurity as an integral part of their supply chain strategy to effectively manage risks and safeguard the integrity and resilience of their supply chain networks.

How To Defend Against Supply Chain Fraud and Criminal Activity

- The rising number of cyber threats that affect supply chains worldwide is not to be overlooked. Immediate and decisive countermeasures must be implemented if importers, exporters, and intermediaries are to have any hope of maintaining stability in a volatile and competitive digital ecosystem.
- Enforce strict onboarding controls and due diligence checks on third-party vendors and suppliers, validating their financial robustness, compliance with relevant anti-fraud, anti-money laundering (AML) legislation, and internal security policies.
- Conduct regular risk assessments to evaluate whether your existing security protocols, policies, and processes are effective and whether new vulnerabilities need to be addressed. If possible, expand this to validate third parties in your supply chain.
- Commit to regularly monitoring your suppliers through periodic transaction reviews, audits, and policy compliance checks. Deploy enterprise-grade data analysis to detect anomalies and false positives, while bolstering your threat intelligence efforts.
- Mutually agree on baseline protection methods like multi-factor authentication, patching regimes, SSL certification, and email security to minimise the attack surface within tools and software you and your suppliers ?use every day.
- Invest in cross-departmental training initiatives to make sure employees are continually aware of risks, possible signs of fraudulent behaviour and risk identification and reporting steps. This is crucial to developing improved cyber hygiene amongst geographically dispersed vendors and suppliers.

While it’s difficult to foresee anything other than a grim and challenging outlook as far as supply chain management and security are concerned, implementing the steps above will drastically reduce both your and your vendors’ attack surface. Proactive and definitive action today will ensure long-term stability and protection of assets vital to your supply chains and customers. It’s better to collaborate now and strengthen our collective cyber resilience if we are to see the true benefits of continued – and safe – digital transformation.

Future Directions

Government Initiatives

Digital India Program: Government initiatives aimed at digitizing various sectors, including logistics and supply chain, are expected to drive IT adoption (Singh & Singh, 2021).

Infrastructure Development: Investments in improving internet connectivity and transportation infrastructure will facilitate better SCM practices (Bhatia & Batra, 2020).

Emerging Technologies

5G Technology: The rollout of 5G networks will enhance real-time data transmission, enabling more sophisticated SCM solutions (Sharma & Das, 2022).

IoT and Big Data Analytics: Continued advancements in IoT and big data analytics will provide deeper insights and predictive capabilities, further optimizing supply chain operations (Jha et al., 2020).

Sustainability and Green SCM

Eco-friendly Practices: Increasing focus on sustainability is driving the adoption of green supply chain practices, supported by IT solutions that optimize resource use and reduce waste (Yadav et al., 2017).

Future research directions include exploring emerging technologies, addressing regulatory complexities, and advancing interdisciplinary collaborations to address supply chain cybersecurity challenges effectively.

Conclusion

According to research, supply chain assaults can have severe repercussions, such as the destruction of vital infrastructure, the stealing of intellectual property, and monetary losses. These assaults have an effect not only on specific businesses but also on entire sectors and even whole countries.

According to study, a multi-layered strategy is required to handle these risks. This strategy should include both technological and non-technical solutions, such as vendor risk management and staff training, as well as access controls, encryption, and intrusion detection systems. Collaboration and information exchange within the supply chain are also considered to be key components in improving safety. Overall, it is evident that supply chain hacking is a challenging area that needs constant study and consideration. Organizations must be constantly on the lookout for threats, take steps to reduce them, and collaborate to improve supply chain security.

References

1. Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. International Journal of Production Research, 60(1), 162-183.
2. Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. Procedia computer science, 149, 65-70.
3. Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. Electronics, 9(11), 1864.
4. Urciuoli, L., Männistö, T., Hintsa, J., & Khan, T. (2013). Supply chain cyber security–potential threats. Information & Security: An International Journal, 29(1).
5. Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. Technology Innovation Management Review, 5(4), 28.
6. Carnovale, S., & Yeniyurt, S. (Eds.). (2021). Cyber Security And Supply Chain Management: Risks, Challenges, And Solutions (Vol. 1). World Scientific.
7. Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing.
8. Gupta, N., Tiwari, A., Bukkapatnam, S. T., & Karri, R. (2020). Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks. IEEE Access, 8, 47322-47333.
9. Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management, 66, 102520.

10. Patil, V., & Suresh, A. (2020). Bridging the skill gap in the Indian logistics sector: Strategies and initiatives. Journal of Supply Chain Management, 56(2), 110-126.
11. Sharma, S., & Das, R. (2022). Impact of 5G technology on Indian supply chains. Telecommunications Policy, 46(1), 102112.
12. Sharma, V., Singh, A., & Mittal, R. K. (2021). Industry 4.0 and supply chain management: A systematic review. Journal of Manufacturing Technology Management, 32(4), 755-778.
13. Singh, N., & Singh, R. (2021). Digital India and its impact on supply chain management. International Journal of Indian Culture and Business Management, 24(2), 150-167.
14. Soni, G., & Kodali, R. (2016). A critical review of supply chain management frameworks: Towards an integrated approach. Benchmarking: An International Journal, 23(3), 650-676.
15. Srinivasan, R., & Swink, M. (2015). Leveraging supply chain integration through planning comprehensiveness: An organizational information processing theory perspective. Decision Sciences, 46(5), 823-861.
16. Yadav, G., Agrawal, R., & Singh, S. P. (2017). Analyzing barriers of green supply chain management using integrated ISM-fuzzy MICMAC approach. Journal of Modelling in Management, 12(3), 453-475.
17. Banerjee, S., & Sengupta, A. (2019). Impact of IT on retail supply chain management: A study in Navi Mumbai. International Journal of Retail & Distribution Management, 47(4), 362-379.
18. Deshmukh, V., & Shukla, A. (2018). Real-time tracking in supply chain management using IoT: A case study of Navi Mumbai. Journal of Supply Chain Management, 12(3), 245-256.
19. Joshi, P., & Patel, R. (2021). AI and ML applications in supply chain management: Innovations and challenges in Navi Mumbai. Journal of Operations and Supply Chain Management, 14(2), 87-101.
20. Joshi, R., & Naik, S. (2024). Integrating cyber awareness into digital transformation strategies: Insights from Navi Mumbai. Journal of Information Security, 23(1), 78-92.
21. Kumar, A., & Patel, R. (2024). Leveraging AI and ML for effective cyber awareness training in supply chains. Journal of Artificial Intelligence Research, 32(1), 100-115.
22. Mehta, R., & Desai, K. (2024). Strategies for effective cyber awareness in supply chain management: Insights from Navi Mumbai. International Journal of Cyber Law & Information Technology, 26(1), 210-225.
23. Patel, S., & Sharma, V. (2024). The role of advanced technologies in enhancing cyber awareness in supply chains. Journal of Supply Chain Management, 15(1), 110-123.
24. Rao, P., & Singh, R. (2024). The impact of leadership involvement on cyber awareness in SCM. Journal of Public Policy and Administration, 24(1), 200-215.
25. Reddy, S., & Gupta, A. (2024). Case study: Cyber awareness in a leading logistics firm in Navi Mumbai. Journal of Logistics and Supply Chain Management, 19(1), 55-70.
26. Sharma, V., & Joshi, M. (2024). Resource constraints and their impact on cyber awareness in SMEs. International Journal of Small Business Cybersecurity, 13(1), 88-103.