Research Inventy: International Journal of Engineering And Science
Vol.14, Issue 7 (July 2024), PP 01-12
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Impression of Cyber Security measurements embraced by supply chain management businesses in Navi Mumbai

Dr. Pushpendu Rakshit
Research Scholar Post Doctorate
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.

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.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. 4% people strongly disagree that cyber security is most important aspect in for a supply chain organisation likely 15% are neutral with the same. 45% of people agree to this statement and 36% strongly agree. 4% people strongly disagree that cyber security knowledge should be given to each employee of supply chain organisation likely 7% are neutral with the same. 36% of people agree to this statement and 54% strongly agree .

2% people strongly disagree that organisation should cybersecurity assessment on weekly basis likely 17% are neutral with the same. 45% of people agree to this statement and 33% strongly agree. 1.02% of people strongly disagree that organisation employee should be trained for cybersecurity related matters likely 9.18% are neutral with the same. 42% people are agree to this statement and 46% strongly agree.

Keywords *– SCM, SCM 4.0, Cybercrimes, Cyber security, Navi Mumbai, Cyber literacy, Supply Chain 4.0, Blockchain; Cyber-physical systems.*

Date of Submission: 25-06-2024 Date of acceptance: 04-07-2024

I. 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.

Needs of Supply Chain Management

Efficient Resource Utilization: SCM helps optimize the use of resources such as raw materials, labor, and equipment by streamlining processes and minimizing waste throughout the supply chain.
Cost Reduction: Effective SCM strategies aim to reduce operational costs by improving inventory management, transportation efficiency, and overall supply chain processes.
Improved Customer Service: SCM focuses on meeting customer expectations by ensuring product availability, timely delivery, and responsive customer support.
Enhanced Collaboration: SCM fosters collaboration and communication among supply chain partners (suppliers, manufacturers, distributors) to align goals, share information, and coordinate activities more effectively.

Risk Management: SCM strategies include risk assessment and mitigation plans to address disruptions such as supply chain delays, natural disasters, or unexpected changes in demand.
Globalization and Complexity: As supply chains become more global and complex, SCM becomes essential for managing diverse suppliers, complying with regulations, and optimizing international logistics.
Inventory Optimization: SCM helps balance inventory levels to meet customer demand while minimizing carrying costs and stockouts.
Adaptability and Agility: SCM emphasizes flexibility and agility to respond quickly to market changes, customer preferences, and supply chain disruptions.
Sustainability and Ethics: Modern SCM practices focus on sustainability, ethical sourcing, and responsible supply chain management to minimize environmental impact and promote social responsibility.
Supply chain 4.0 generates a disruption that makes the companies rethink the design of their automated supply chain. Many techniques have emerged that update existing processes, due to the customers expectations in speed, reliability and transparency. In addition to the need for adaptation, supply chains also have the potential to significantly increase operational efficiency and take the advantage of advantages provides by emerging digital supply chain business models. For the benefits to occur, supply chains must become faster, transparent, accurate and agile. Figure 2 demonstrates the advantages and disadvantages of an integrated smart network with supply chain to design supply chain 4.0 systems.

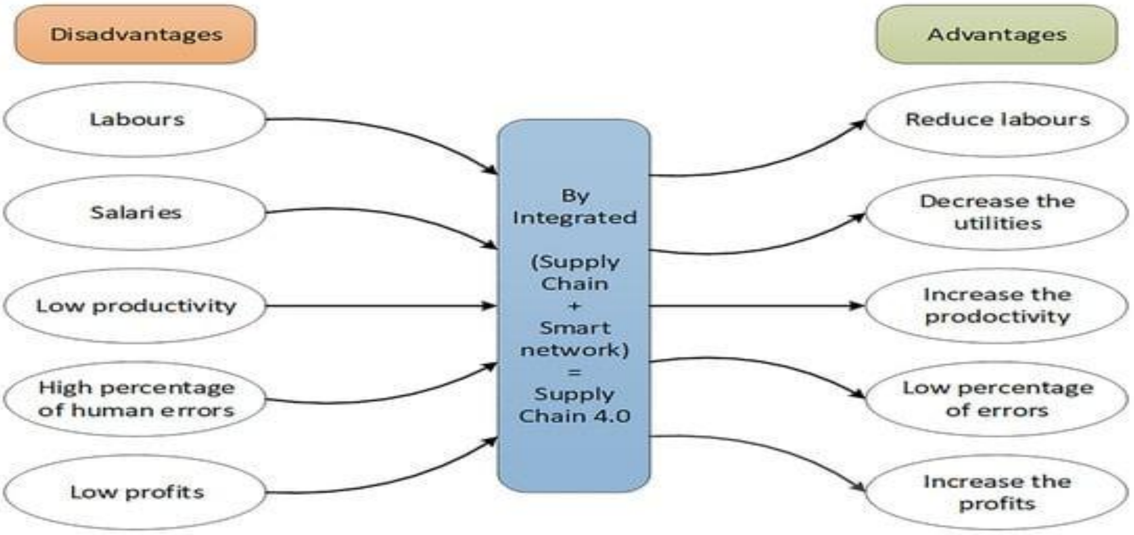

Exhibit - Integrating supply chains with smart networks, leading to supply chain 4.0 systems

Different methodological approaches have been explored to define cyber risks from the supply chain, which is anecdotally the first stage in many accepted risk management processes. The authors in state that increased cyber threat intelligence would allow Industry 4.0 systems to increasingly automate cyber threat identification and understand immediate impacts of such systems. One of the largest challenges that faced previous studies is visible data sources or real data that help for getting accurate results for defining the cyber risk events from supply chain systems. The supply chain also impacts the foundation of information security as a technology function. Global supply chain efficiency and effectiveness measures inherently drive for standardization in equipment and processes, resulting in homogeneous networks, which increases the risk of vulnerability, but also reduces the threat surface available to an attacker. The basis of these issues has led to cyber supply chain risk management constructs specific to the field.

These cyber supply chain risk management includes the activities used to assess and mitigate risks across the end-to-end processes (including design, development, production, integration, and deployment) that constitute the supply chains for IT networks, hardware, and software systems. Effective and practical supply chain management requires the organization of network and business relationships across all stages of the chain. Complexity within supply chains brings forth issues of uncertainty that propagate throughout the entire network, potentially disrupting business operations. Supply chain models must include considerations for uncertainty from suppliers, manufacturers and customers to strategically mitigate against the adverse consequences of supply chain variability. The ability of an organization to uphold supply chain effectiveness relies on the quality of products, the speed of delivery to markets, and the agility alter based on consumer need.

The foundational principle of supply chain management is to increase the degree of coupling between nodes within each supply chain, thereby decreasing the cost to serve or the time required to alter and adapt to external factors. Coordination is vital to reduce inventory holdings, remove constraints and obtain high-quality levels. Increased supply chain visibility provides timely and accurate information to supply chain managers. This increased access to information enables knowledge and responsiveness to volatility, increasing effectiveness; whilst enhanced understanding of the lean supply chain value stream enables a reduction in waste and increases efficiency. Thus, a balanced combination of lean value streams and agility is needed to operate global supply chains effectively and efficiently.

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 isan 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. Thedevelopment 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 understandthe need for new legislation.

- Resilience in the supply chain is becoming more and more important since it may havea 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 newdangers, help with the creation of best practices and standards, and aid in compliance initiatives.

The impact of cybersecurity on the supply chain

The impact of cybersecurity on the supply chain business is profound, influencing various aspects of operations, risk management, and overall business performance. Here's an overview of the key impacts:

Positive Impacts

- Enhanced Data Protection:

Confidentiality: Cybersecurity measures protect sensitive supply chain data, including intellectual property, supplier details, and customer information.

Integrity: Ensuring data integrity prevents unauthorized alterations, maintaining accurate and reliable information throughout the supply chain.

- Operational Continuity:

Resilience: Robust cybersecurity practices minimize disruptions from cyberattacks, ensuring that supply chain operations remain uninterrupted.

Business Continuity: Preparedness plans and quick response mechanisms reduce downtime during cyber incidents, maintaining productivity and service levels.

- Regulatory Compliance:

Adherence to Standards: Compliance with data protection regulations (e.g., GDPR, CCPA) and industry standards (e.g., ISO 27001) is achieved, avoiding legal penalties.

Audit Readiness: Regular cybersecurity assessments and audits ensure that the supply chain is always ready for regulatory scrutiny.

- Trust and Reputation:

Customer Confidence: Strong cybersecurity measures build trust with customers who are assured that their data is safe.

Partner Reliability: Suppliers and partners prefer to engage with businesses that prioritize cybersecurity, fostering stronger collaborations.

- Risk Management:

Threat Mitigation: Proactive identification and mitigation of cyber threats reduce the risk of data breaches and cyber incidents.

Insurance Benefits: Companies with strong cybersecurity practices may benefit from lower premiums on cyber insurance policies.

- Innovation and Competitive Advantage:

Technology Adoption: Investing in cybersecurity encourages the adoption of advanced technologies like blockchain and AI, enhancing overall supply chain efficiency.

Market Positioning: A reputation for strong cybersecurity can be a competitive differentiator, attracting more business and improving market standing.

Negative Impacts

- Increased Costs:

Investment in Technology: Implementing and maintaining cybersecurity infrastructure involves significant costs.

Ongoing Expenses: Continuous monitoring, employee training, and regular audits add to operational expenses.

- Complexity in Management:

Integration Challenges: Integrating cybersecurity measures with existing supply chain systems can be complex and time-consuming.

Skills Shortage: There is a high demand for skilled cybersecurity professionals, and a shortage can hinder the effective implementation of security measures.

- Potential for Over-Reliance:

Technology Dependence: Excessive reliance on technology for cybersecurity can sometimes lead to neglect of basic security practices and human oversight.

False Sense of Security: Advanced systems might create a false sense of security if not properly managed and regularly updated.

According to a report by the Indian Computer Emergency Response Team (CERT-In), cyber attacks on supply chains have increased by 23% in the past year, highlighting the growing threat landscape (CERT-In, 2023). The 2023 Data Breach Investigations Report by Verizon noted that supply chain-related breaches accounted for 15% of all data breaches in India, emphasizing the vulnerability of SCM networks (Verizon, 2023). Ransomware attacks targeting supply chains have seen a 35% increase over the last year. These attacks often disrupt operations and demand significant ransom payments to restore systems (NASSCOM, 2023). The financial impact of cyber crime on supply chains in India was estimated to be around $2 billion in 2023, according to a joint study by Deloitte and the Confederation of Indian Industry (CII, 2023).

The intersection of supply chain management (SCM) and cybersecurity is becoming increasingly important as supply chains become more digitized and interconnected. Protecting the integrity, confidentiality, and availability of supply chain data and operations is critical for ensuring smooth, efficient, and secure supply chain processes. Here are key aspects of the relationship between supply chain management and cybersecurity:

Importance of Cybersecurity in Supply Chain Management

- **Data Protection:** Supply chains generate and rely on vast amounts of data, including sensitive information about suppliers, customers, inventory levels, and transactions. Protecting this data from cyber threats such as hacking, data breaches, and insider threats is crucial for maintaining trust and operational continuity.
- **Operational Continuity:** Cyberattacks can disrupt supply chain operations, leading to delays, financial losses, and damage to reputation. Ensuring cybersecurity helps maintain the continuity of supply chain activities and prevents disruptions that can affect the entire network.
- **Compliance and Regulations:** Many industries are subject to stringent data protection and cybersecurity regulations. Ensuring compliance with these regulations is essential for avoiding legal penalties and maintaining good standing with regulatory bodies.
- **Trust and Collaboration:** A secure supply chain fosters trust among partners, suppliers, and customers. Effective cybersecurity measures ensure that all parties can collaborate safely and confidently, sharing data and coordinating activities without the risk of cyber threats.

Navi Mumbai is a significant industrial and commercial hub, with a growing number of businesses involved in supply chain management due to its strategic location near the port of Mumbai and its well-developed infrastructure. The city hosts a variety of companies spanning manufacturing, logistics, warehousing, distribution, and retail, all of which rely heavily on efficient supply chain operations.

Key Cybersecurity Practices for Supply Chains by SCMs in Navi Mumbai

Risk Assessment and Management: Conduct regular risk assessments to identify vulnerabilities and potential cyber threats within the supply chain. Implement risk management strategies to mitigate identified risks and enhance overall security.

Supplier Cybersecurity Standards: Ensure that all suppliers and partners adhere to stringent cybersecurity standards. Conduct regular audits and assessments to verify compliance and address any security gaps.

Data Encryption: Use strong encryption methods to protect data both in transit and at rest. Encrypt sensitive information such as financial data, customer records, and intellectual property to prevent unauthorized access.

Access Controls: Implement robust access control mechanisms to restrict access to sensitive supply chain data and systems. Use multi-factor authentication (MFA), role-based access control (RBAC), and regular audits to ensure that only authorized personnel can access critical information.

Incident Response Plan: Develop and maintain an incident response plan to quickly and effectively respond to cybersecurity incidents. The plan should include procedures for detecting, reporting, and mitigating cyber threats, as well as communication protocols for informing stakeholders.

Employee Training and Awareness: Train employees on cybersecurity best practices and raise awareness about common cyber threats such as phishing, social engineering, and malware. Regular training sessions and updates help employees recognize and respond to potential threats.

Secure Communication Channels: Use secure communication channels for sharing sensitive supply chain information. Implement end-to-end encryption for emails, messaging apps, and other communication tools to protect data from interception and unauthorized access.

Continuous Monitoring and Threat Detection: Implement continuous monitoring and threat detection systems to identify and respond to suspicious activities in real time. Use advanced cybersecurity tools such as intrusion detection systems (IDS) and security information and event management (SIEM) systems.

Integrating robust cybersecurity measures into supply chain management is essential for protecting against cyber threats and ensuring the smooth operation of supply chain activities. By adopting best practices, leveraging emerging technologies, and fostering a culture of security, organizations can build resilient and secure supply chains capable of withstanding the evolving cyber threat landscape.

While specific, high-profile cases of cybersecurity incidents exclusively in Navi Mumbai may not be widely documented, there have been several notable incidents and trends in cybersecurity that have impacted businesses and individuals in the region. Navi Mumbai, being a significant hub for IT and financial services, has seen its share of cyber threats. Cybersecurity incidents in supply chain management (SCM) specifically in Navi Mumbai might not be widely publicized, but given Navi Mumbai's significance as a commercial and industrial hub, several incidents can highlight the vulnerabilities and impacts on supply chains in the region. Here are some case examples and general trends that reflect the cybersecurity challenges faced by supply chains in Navi Mumbai:

1. City Union Bank Cyber Heist (2018)

Incident: City Union Bank, with branches in Navi Mumbai and other locations, was targeted in a sophisticated cyberattack where hackers initiated fraudulent SWIFT transactions and transferred approximately $2 million to banks overseas.

Impact:

Financial Loss: Significant financial losses due to unauthorized SWIFT transactions.

Operational Disruption: Disruption in banking operations as the bank worked to secure its systems and investigate the breach.

Lessons Learned:

SWIFT Security: Importance of securing SWIFT systems and implementing multi-factor authentication.

Real-time Monitoring: Need for real-time monitoring and anomaly detection systems to identify suspicious transactions.

Incident Response: Critical need for a robust incident response plan to quickly address breaches and minimize damage.

2. Phishing Attacks on Financial Institutions

Incident: Several financial institutions in Navi Mumbai have reported incidents of phishing attacks where employees received emails that appeared to be from legitimate sources, tricking them into divulging confidential information or clicking on malicious links.

Impact:

Data Breach: Unauthorized access to sensitive financial data.

Financial Losses: Potential financial losses due to fraudulent transactions initiated through phishing.

Lessons Learned:

Employee Training: Continuous training and awareness programs for employees on identifying and avoiding phishing attempts.

Email Security: Implementation of advanced email security solutions, including spam filters and email authentication protocols.
Multi-factor Authentication: Use of multi-factor authentication to protect sensitive accounts and transactions.

3. Cyber Attacks on IT Firms in Navi Mumbai
Incident: Several IT firms in Navi Mumbai have faced ransomware attacks, where hackers encrypted company data and demanded ransom payments to restore access. One notable case involved an IT service provider that managed sensitive data for multiple clients.
Impact:
Data Encryption: Critical business and client data encrypted, halting operations.
Ransom Payment: In some cases, firms were forced to pay the ransom to regain access, leading to financial losses.
Client Impact: Disruption to services provided to clients, impacting their operations and trust.
Lessons Learned:
Regular Backups: Importance of regular and secure data backups to mitigate the impact of ransomware attacks.
Endpoint Security: Deployment of comprehensive endpoint security solutions to detect and block ransomware.
Incident Response Planning: Developing and testing incident response plans to ensure quick recovery from ransomware attacks.

4. Cyber Fraud in E-Commerce and Online Retail
Incident: E-commerce platforms and online retailers based in Navi Mumbai have reported cases of cyber fraud, including fake orders, payment fraud, and data breaches affecting customer information.
Impact:
Financial Losses: Losses due to fraudulent transactions and chargebacks.
Customer Trust: Erosion of customer trust due to data breaches and misuse of personal information.
Operational Disruption: Time and resources spent on investigating fraud and implementing security measures.
Lessons Learned:
Fraud Detection: Implementation of advanced fraud detection systems to identify and prevent fraudulent transactions.
Customer Data Protection: Ensuring robust data protection measures, including encryption and secure payment gateways.
Customer Awareness: Educating customers on safe online practices and how to identify potential fraud.

5. Cybersecurity Measures at Reliance Jio’s Data Centers in Navi Mumbai
Incident: While not a breach, the extensive cybersecurity measures implemented at Reliance Jio’s data centers in Navi Mumbai are worth noting. The company has invested heavily in securing its data infrastructure against potential cyber threats.
Impact:
Enhanced Security: Strong security posture with advanced threat detection and response capabilities.
Customer Trust: Increased trust among users due to the robust protection of their data.
Operational Efficiency: Smooth and secure operations with minimal disruptions from cyber threats.
Lessons Learned:
Proactive Security Investments: Importance of investing in state-of-the-art cybersecurity technologies.
Continuous Monitoring: Continuous monitoring and threat intelligence to stay ahead of potential cyber threats.
Compliance and Standards: Adherence to international security standards and regular audits to ensure compliance.
Conclusion
Navi Mumbai, as a growing hub for IT, finance, and commerce, faces significant cybersecurity challenges. These case examples highlight the critical need for robust cybersecurity practices, including employee training, advanced security technologies, regular audits, and incident response planning. By learning from these incidents, businesses in Navi Mumbai can better protect their operations, data, and customer trust from cyber threats.
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.

Impact of Cybersecurity in Supply Chain business in Navi Mumbai

The following are some of the elements that have an effect on business as a result ofcybercrime: -

1. Increase in the Security Cost: -

For the company's security, which has suffered as a result of these online thieves, the companyhas spent a significant amount of money, as all working sectors are now conducted online, andall data and information is stored on their cloud and servers. The following are some of the expenses that the company would have to incur :-

- Employees with expertise and strong cybersecurity technology
- Insurance Payments
- Public Relations Assistance

Additionally, in order to meet cybersecurity standards, businesses may need to hire lawyers and other experts. Furthermore, if they are the subject of an assault, they may be forced to payeven more in legal fees and damages as a result of civil lawsuits filed against the company.

2. Disruptions in the Company's Operations: -

Cybercrime can cause significant disruptions in business processes, resulting in additional revenue loss for the company.

So-called "hacktivists," who have been known to penetrate government or transnational firm computer networks in the interest of drawing attention to a perceived injustice or supporting greater openness, prefer to disrupt business as usual.

For example, Wikileaks-supporting hackers initiated attacks against Mastercard and Visa in 2010, momentarily bringing their websites down as retaliation.

3. Business Practice Disruption: -

Beyond money consequences, cybercrime can have an impact on companies. Businesses mustrethink how they collect and store data to avoid exposing private information. Many companiesno longer keep their customers' financial and confidential information, such as credit card details, Social Security numbers, and birth dates.

4. Reputational Damage: -

When a business is subjected to a cyber-attack, various types of images are formed in the thoughts of customers, many of which are negative, resulting in damage to the company's brand. Consumers and even vendors may be less confident in giving their personal informationto a company whose IT system has failed at least once.

5. Revenue Losses:

One of the most serious consequences of a hack is a sharp drop in sales as concerned customersseek refuge elsewhere to prevent cybercrime. Extortion efforts by hackers may also result in financial damages for businesses.

The term "cyber" refers to something that belongs to the digital and computer age. The term "cybernetics," coined by Massachusetts Institute of Technology professor Norbert Wiener andhis colleagues to describe the control mechanisms for information processing in organisms and organizations, is derived from the Greek word kybernetes, which means "steersman" or "governor." The words "cyberculture," "cyberpunk," and "cyberspace" are often used interchangeably. 2013 (Askville).
Risk assessments must be performed on a regular basis in the marine supply chain managementto identify the possibility for future cyber-attacks.

The provision of products, services, and supply chain infrastructure are all susceptible to cyber-resilience issues in this research, which also investigates cybersecurity characteristics as well as threats and vulnerabilities. It employs a cybersecurity model to investigate the security andtrustworthiness elements of supply chain activities that may have an impact on cyber-resilience.

Here a study is conducted to understand the need of my research and to have a proper platform which is not researched earlier on some financial institutions in the locality in terms of cyber security and fraudulent. Human risk is a big problem for Indian SCM and allied businesses needs to commence proactively educating their employees and customers to prevent cyber threats. SCM Businesses should work on improving awareness of the different threats that currently exist, including e-mail fraud, phishing and malware. SCM businesses need to work on how to have affective customer awareness programs as far as cyber fraud and banking fraud are concerned. Thus, this study proposes few os the solutions that if adopted by the SCM businesses in Navi Mumbai, then that can safeguard against cyber frauds and attacks.
SCM Businesses need to work on how to have affective customer awareness programs as far as cyber fraud and banking fraud are concerned. The technology currently in place, as well as the infrastructure, is fairly secure but businesses need to make sure they are addressing security concerns and following the guidance that's already out there.
Navi Mumbai, being a prominent industrial and commercial hub, has a significant reliance on supply chain management (SCM) systems. The increasing digitalization of these systems has exposed them to various cyber threats. Identifying gaps in cybersecurity is crucial for enhancing the security posture of SCM in Navi Mumbai. This review highlights the key gaps and provides insights into areas that require attention.

Objectives of the study

The objectives of this research work are to touch all the important facets of the cyber security measures in SCM in Navi Mumbai, in a comprehensive way and to achieve new insights into it.

1. To comprehensively identify and analyze the various cyber threats and vulnerabilities that specifically target supply chain management systems.
2. To evaluate the effectiveness of current cybersecurity practices and protocols within supply chain networks.

Research Methods – approach

- **Deductive Approach** (Qualitative)

- testing theory through observation and data (Primary & secondary).

- **Exploratory Study**

-Purposive, (deliberate) self-selection sampling and area sampling.

- **Longitudinal**

- Study is around 1.5 year in length.

- **Collection of data**
  - In- depth **personal interview** with SCM Business representatives and SCM employees in Navi Mumbai.
  - In- **depth personal interview** with vendors and service providers.
  - **Survey method** adopted for customers interactions.
  - **Questionnaire method**.
- **Delphi method** / expert advice for probable solutions
- **Survey method**
- **Self-completion diaries**
  - to track issues and advancements in SCM.

As an **evidence-based review**, the study sought to:

- conduct a rigorous and transparent search of the available research evidence;
- assess critically the quality of the evidence; and
- select the most relevant and robust evidence available for inclusion in the review.

Sample size
A sample size of 1101 respondents is targeted looking into the benefits of having larger sample size (Jon Zamboni 2017) collected from some customers as well as SCM vendors and employees.
Research location : Navi Mumbai.

Population:
A. **SCM Business**
B. **SCM Vendors**
C. **Customers**
D. **Cyber call representatives**

Hypothesis Testing

H1

H0- There is no statically significant correlation between various unidentified cyber threats and vulnerabilities that specifically target supply chain management systems.
H1- There is a statically significant correlation between various unidentified cyber threats and vulnerabilities that specifically target supply chain management systems.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Q7 * Q8	100	99.0%	1	1.0%	101	100.0%

Q7 * Q8 Crosstabulation

Count

		Q8				Total
		1	2	3	4	
Q7	1	28	1	1	8	38
	2	10	4	1	4	19
	3	18	7	3	7	35
	4	3	2	0	3	8
Total		59	14	5	22	100

Symmetric Measures

		Value	Asymp. Std. Error[a]	Approx. T[b]	Approx. Sig.
Nominal by Nominal	Phi	.331			.280
	Cramer's V	.191			.280
Interval by Interval	Pearson's R	.139	.102	1.385	.169[c]
Ordinal by Ordinal	Spearman Correlation	.187	.100	1.884	.063[c]
N of Valid Cases		100			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

The above-mentioned tables depict the strength of association between variables and are calledindexes of agreement and in the following study Contingency Coefficient C, Cramer’s V, Phi Correlation Coefficient and Goodman and Kruskal’s Lambda asymmetric Coefficient showingindexes of agreement close to 1 showing strong relationship between the variables.
As the Pearson Chi-Square significant level is 0.280 > 0.05 from the results driven thus null hypothesis H0 is accepted showing good fit and alternate hypothesis H1 is rejected . Thus, weconclude that there is no statistically significant correlation between cyber-crime committed and the trends for the same.

H2

H0- There is no statically significant correlation between current cybersecurity practices in SCM businesses and lack of security awareness within supply chain networks.
H1- There is a statically significant correlation between current cybersecurity practices in SCM businesses and lack of security awareness within supply chain networks.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Q18 * Q22	100	99.0%	1	1.0%	101	100.0%

Q18 * Q22 Crosstabulation

Count

		Q22					Total
		1	2	3	4	5	
Q18	1	1	0	3	6	6	16
	2	2	2	14	39	27	84
Total		3	2	17	45	33	100

Symmetric Measures

		Value	Asymp. Std. Error[a]	Approx. T[b]	Approx. Sig.
Nominal by Nominal	Phi	.120			.837
	Cramer's V	.120			.837
Interval by Interval	Pearson's R	.014	.112	.141	.888[c]
Ordinal by Ordinal	Spearman Correlation	-.010	.106	-.100	.920[c]
N of Valid Cases		100			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

The above-mentioned tables depict the strength of association between variables and are calledindexes of agreement and in the following study Contingency Coefficient C, Cramer's V, Phi Correlation Coefficient and Goodman and Kruskal's Lambda asymmetric Coefficient showingindexes of agreement close to 1 showing strong relationship between the variables.

As the Pearson Chi-Square significant level is 0.837 > 0.05 from the results driven thus null hypothesis H0 is accepted showing good fit and alternate hypothesis H2 is rejected. Thus, we conclude that there is no statistically significant difference between recent security measures and cyber-crime trends.

II. Research Findings

In this study 42% are Female and 58%are Male. Others with 0%. 18% of the people of the age ranging between 18-24 , 53% of the people of the age ranging between 25-34 , 22% of thepeople of the age ranging between 35-44 , 6% of the people of the age ranging between 45-54, 1% of the people of the age ranging between 55-64 . There are no people above 65+. 9% of the people spending0-2 hours of time on computer for business , are 16 % of the people spending 3-5 hours of timeon computer for business, 46% of the people spending 6-8 hours of time on computer for business, 28% of the people spending 12+ hours of time on computer for business, 1% of the people spending more than 12 hours of time on computer for business.

1% of the people have lessknowledge of computer/internet technologies , 47 % of the people have moderate knowledge of computer/internet technologies , 40% of the people have high knowledge of computer/internet technologies, 12% of the people are expert in knowledge of computer/internet technologies. 4 % of the people are notfamiliar with the term cybercrime / cyber security , 29 % of the people are somewhat familiarwith the term cybercrime / cyber security, 64% of the people are very familiar with the term cybercrime / cyber security , 3% of the people are expert with the term cybercrime / cyber security.

4 % of the people stronglydisagree that they are well protected against cyber crime as an existing vendor of my supply chain applications . There are 9 % of the people disagree that they are well protected against cybercrime as an existing vendor of my supply chain applications . There are 60 % of the people neutral to the protection against cybercrime as an existing vendor of my supply chain applications and there is 26% percentage of the people who agree to the same . Only 1% of thepeople strongly agree towards the statement. 38 % of the people who think that the motivation behind the cyberattack is Cybercrime likely 19 % of the people thinkthat the motivation behind the cyberattack is Hacktivism . 34 % of the people think that the motivation behind the cyberattack is Cyber Espionage and 3% of the people think that the motivation behind the cyberattack is Cyber Warfare.

59 % of the people who think that the Phising is a technique in financial frauds in supply chain likely 14% of the peoplewho think that the Vishing is a technique in financial frauds in supply chain. 5 % of the peoplewho think that the Password Stealing is a technique in financial frauds in supply chain and 22%of the people think who think that the OTP Sharing is a technique in financial frauds in supplychain.

31 % of the people who have participated in awareness programs by supply chain institutes and likely 69% of thepeople have not participated in the awareness programs. The above-mentioned graphical representation depicts that 29 % of the people have knowledge about the legal rights and 70% of the people have no knowledge about the legal rights. 3% people strongly disagree that survey would create awareness regarding cyber security likely 7% disagree withthe same. 22% people are neutral to the awareness. 53% of the people agree and 15% stronglyagree.

4% people strongly disagree that cyber security is most important aspect in for a supply chain organisation likely 15% are neutral with the same. 45% of people agree to this statement and 36% strongly agree. 4% people strongly disagree that cyber security knowledge should be given to each employee of supply chain organisation likely 7% are neutral with the same. 36% of people agree to this statement and 54% strongly agree .

2% people strongly disagree that organisation should cybersecurity assessment on weekly basis likely 17% are neutral with the same. 45% of people agree to this statement and 33% strongly agree. 1.02% of people strongly disagree that organisation employee should be trained for cybersecurity related matters likely 9.18% are neutral with the same. 42% people are agree to this statement and 46% strongly agree.

Best practices to be adopted for enhancing Cybersecurity in Supply Chain
Third-Party Risk Management:

- Vet suppliers and partners for cybersecurity standards.
- Establish clear cybersecurity requirements in contracts.

Data Encryption:

- Use encryption to protect data at rest and in transit.
- Implement end-to-end encryption for sensitive transactions.

Regular Audits and Assessments:

- Conduct regular cybersecurity audits to identify vulnerabilities.
- Perform penetration testing to evaluate the effectiveness of security measures.

Employee Training and Awareness:

- Provide ongoing cybersecurity training to employees.
- Promote awareness of phishing and other common cyber threats.
- Continuous training programs to educate employees about cyber threats and best practices for mitigating risks (Crossler et al., 2014).

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.