International Journal of Scientific Research and Engineering Development-– Volume X Issue X, Year

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Managing Cyber Risk in Supply Chains: A Review and Research Agenda

Prarthna Sorathiya[1], Mr Samir Joshi[2]

1. (B Tech in Computer Science Engineering, Atmiya University, Rajkot, India
Email: prarthna.sorathiya@gmail.com

2. (Faculty of Engineering and Technology , Atmiya University, Rajkot, India
Email: samir.joshi@atmiyauni.ac.in

Abstract-The profound digitalization of global commerce has structurally transformed traditional logistics into interconnected "cyber supply chains" (CSCs), making cyber events a top enterprise risk. In the financial sector alone, the costs average $5.9-$6.08 million per incident. This comprehensive review, leveraging systematic literature analysis and recent empirical data, investigates the critical governance deficiencies and effective mitigation strategies required for systemic resilience.

Findings confirm that supply chain cyber risk—defined as accidental or deliberate IT events threatening infrastructure integrity and leading to cascading disruptions—must be classified holistically across five categories:

- **Physical Threats**
- **Breakdown**
- **Direct Attacks**
- **Indirect Attacks**
- **High-impact Insider Threats**

Third-party vendors are the dominant vulnerability, accounting for approximately 62% of all breaches. These often occur via software flaws (18.08%) and stolen vendor credentials (16.10%). Mitigation requires a structured, time-phased approach (Pre-, Trans-, and Post-Attack), but implementation maturity is low ; only 36% of institutions continuously monitor vendors, and 68% fail to address fourth-party risk. The solution lies in the integrated

Supply Chain Cyber Security System conceptual model, mandating the strategic alignment of IT, Organizational, and Supply Chain security systems to achieve holistic control. The review concludes by setting a rigorous research agenda focused on empirical modeling, strategic validation, and deeper exploration of behavioral and human factors.

1. Networked Vulnerability Overview

1.1. Context and Digital Transformation

Modern commerce relies on intricate, interconnected "cyber supply chains" (CSCs), where partners share data analytics, cloud platforms, and information technology (IT) systems, to achieve efficiency and competitive advantage. This reliance, however, exponentially increases the organizational attack surface by introducing complex dependencies and inter-firm dynamics-specific vulnerabilities. Cyber security is a top enterprise risk priority because, unlike traditional disruptions, cyber breaches often go unreported until they result in significant operational paralysis or financial loss.

1.2. Definition of Supply Chain Cyber Risk

Beyond simple IT security, supply chain cyber risk encompasses operational risks that compromise the CIA triad (availability, confidentiality, and integrity) of information systems. This review classifies IT events as either intentional or unintentional, putting a supply chain's infrastructure at risk and starting a domino effect of disruptions, using the definition given by Ghadge et al. (2020) . Effective management requires the integration of security considerations related to infrastructure.

1.3. Escalation of the Threat Landscape and Empirical Evidence

The financial services sector provides compelling empirical evidence for the gravity of CSC threats due to the high value of managed information. The increasing threat level is supported by data: 82% of financial institutions experienced a cybersecurity breach in the past year, with an average cost per incident ranging from $5.9 million to $6.08 million. Third-party vendors are responsible for a significant 62% of breaches, highlighting the shortcomings of firm-centric security models. Significant governance gaps exacerbate this vulnerability: 59% of organizations do not perform cybersecurity compliance checks, even though they share sensitive data with an average of 583 third parties.

1.4. Goal and Structure

The paper systematically addresses the question, "How can organisations manage cyber risks in supply chains?", considering the significant disconnect between deep third-party integration and sophisticated oversight. It synthesizes the literature to classify threats, outline mitigation strategies, develop a conceptual governance model, and recommend a robust research agenda.

---

2. The Networked Ecosystem's Changing and Growing Risks

Effective governance must address the full spectrum of supply chain vulnerabilities, including organizational and physical defects that permit spread, in addition to technical threats.

2.1. Cyber Risk Typology in the Supply Chain: Beyond the Digital World

A thorough approach is used to classify cyber risk types into five primary groups based on their origin and impact.

(Note: The five groups are Physical Threats, Breakdown, Direct Attacks, Indirect Attacks, and high-impact Insider Threats.)

2.2. Empirical Validation and Amplified Vectors

Empirical evidence indicates that insider threats and indirect attacks are actively used to exploit third-party relationships. The most frequent vector, accounting for 18.08% of incidents, is third-party software vulnerabilities, which suggests a breakdown in SBOM verification and upstream vendor monitoring. Furthermore, breaches linked to stolen vendor credentials account for 16.10% of incidents, highlighting deficiencies in vendor personnel management and access control—a clear link to insider threats and the human element. The frequency of indirect attacks supports the trend of attackers concentrating on the human layer and the inter-organizational boundary rather than attempting frontal technical assaults.

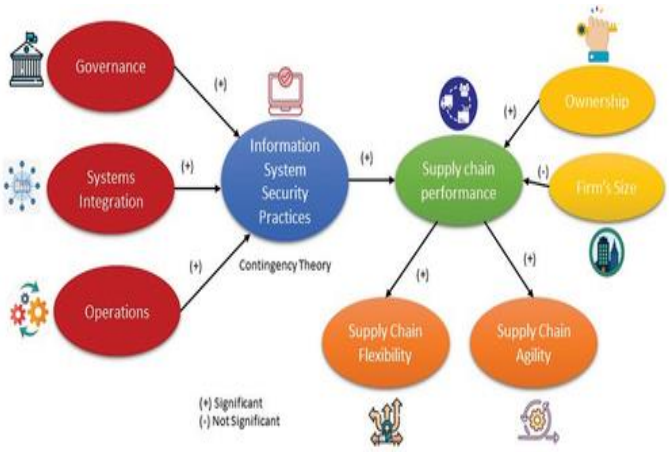
2.3. Critical Points of Penetration (PoPs) and Risk Propagation

The Points of Penetration (PoPs) through which threats enter the supply chain are divided into three primary categories:

- **Technical Points of View**: Focus on hardware and software defects that are often exacerbated by outsourcing important systems (e.g., improperly configured cloud infrastructure, as exemplified in the Capital One hack).
- **Human PoPs**: Employees and subcontractors who are frequently the target of phishing (Indirect Attacks) because of a lack of proper training or a negligent security breach. The consequences of internal human error are often severe and difficult to define.
- **Physical PoPs**: Include tangible items and non-IT systems that are used to gain access to networks, such as the login credentials used by the HVAC contractor in the 2013 Target hack.

3. A Time-Phased Strategy and Mitigation Approach to Resilience

Effective mitigation requires not only static prevention but also a systematic, time-phased approach that gives priority to dynamic detection and recovery capabilities.



3.1. Challenges with Constant Commitment and Strategic Alignment

In essence, persistent strategic and behavioural problems make it difficult to operationalise mitigation:

- **Inter-organizational trust** requires collaborative, trust-based relationships and shared security objectives to prevent partners from "free-riding" on security investments.

- **Employee Information**: Lack of specialised skills and reluctance to invest in continuous training are persistent vulnerabilities exploited by cybercriminals.
- **The Deficit in Commitment**: Because of the constantly changing threat landscape, cyber risk management necessitates ongoing dedication, which runs counter to managers' attention to short-term performance goals.

4. Frameworks and Governance: Including Systemic Resilience

Mature governance frameworks that employ Strategic Third-Party Risk Governance (TPRG) and an integrated conceptual model are necessary for systemic resilience.

4.1. Components of Strategic Third-Party Risk Governance (TPRG)

Currently, 75% of financial institutions use TPRM, the operational framework for managing external risk throughout the vendor lifecycle. Crucial elements consist of:

- **Risk Tiering and Due Diligence**: Prioritizing high-risk IT, carefully vetting low-risk non-IT vendors, and implementing a risk-based strategy mandated by agencies like the US Office of the Comptroller of the Currency (OCC) are a few examples.
- **Contractual Integrity and Audit Requirements**: Legally binding contracts must include explicit cybersecurity provisions, demand comprehensive software supply chain audits, and specify compliance requirements.

4.2. Regulatory Requirements and Implementation Gaps

Improved vendor management, risk classification, and ongoing monitoring are required by regulatory frameworks such as DORA (EU) and updated OCC guidance (US). Despite mandates and increased investment (60 percent of global banks increased their TPRM spending in 2023), only 29% of institutions believe their governance models are very effective. This is largely due to the severe failure to manage fourth-party risk. Sixty-eight percent of financial organizations lack the mechanisms required to address this deeper tier, a structural weakness that structurally permits widespread risk propagation.

5. Research Outline and Findings

5.1. Combining Basic Findings

As per the analysis, cyber risk is inherently present in the digitalisation of commerce, mainly due to external third-party vulnerabilities that exploit software flaws and human access controls. Effective management must identify the five primary risk categories, and dynamic capability must take the place of compliance. Current governance is characterized by a critical commitment deficit (low continuous monitoring rates) and systemic gaps in fourth-party visibility. Resilience requires implementing the integrated conceptual model and coordinating IT security, organizational, and supply chain systems to ensure coordinated ecosystem control.

References

1. Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Reviewing Third-Party Risk Management: Best Practices in Accounting and Cybersecurity for Superannuation Organizations.

   Finance & Accounting Research Journal, 6(1), 21–39.

2. Baker, W. H., Smith, G. E., Watson, K. J., & Pokorski Ii, J. A. (2007). Security and cooperation in the IT-enabled supply chain are crucially balanced.

   International Journal of Production Research, 45(11), 2595–2613.

3. Barnum, C. (2014). Target breach highlights need for better third-party risk management. Gartner Research.
4. Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems.

   Technovation, 34(7), 342–353.

5. Dani, S., Ghadge, A., and Kalawsky, R. (2012). Risk management in the supply chain: current and future perspectives.

   The International Journal of Logistics Management, 23(3), 313–339.

6. Deane, J. K., Ragsdale, C. T., Rakes, T. R., & Rees, L. P. (2009). Managing supply chain risk and disruption from IT security incidents.

   Operations Management Research, 2(1-4), 4–12.

7. EIOPA. (2023). Guidelines on the implementation of the Digital Operational Resilience Act (DORA). European Insurance and Operational Pensions Authority.
8. Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events?

   European Journal of Operational Research, 272(3), 1109–1119.

9. Faisal, M. N., Banwet, D. K., & Shankar, R. (2007). A framework for evaluating and mitigating information risks in supply chains.

   Enterprise Information Management Journal, 20(6), 677-699.

10. Ghadge, A., Wilding, R., Caldwell, N. D., & Weiß, M. (2020). A review and research agenda for supply chain cyber risk management.

    An International Journal of Supply Chain Management, 25(2), 223–240.

11. Hintsa, J., Urciuoli, L., Männistö, T., & Khan, T. (2013). Possible risks to supply chain cyber security.

    Details & Security: An International Journal, 29, 51–68.

12. Joseph, S. A., Ogunmolu, A. M., Ejiofor, V. O., Kolo, F. H. O., & Oyekunle, S. M. (2025). Using strategic third-party risk governance frameworks to reduce cybersecurity risks in financial institutions.

    Journal of Engineering Research and Reports, 27(5), 173–193.

