# AMERICAN JOURNAL OF SOCIAL DEVELOPMENT AND ENTREPRENEURSHIP (AJSDE)

ISSN: 2836-0702 (ONLINE)

VOLUME 4 ISSUE 1 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Social Development and Entrepreneurship (AJSDE)

Volume 4 Issue 1, Year 2025
ISSN: 2836-0702 (Online),
DOI: https://doi.org/10.54536/ajsde.v4i1.5037
https://journals.e-palli.com/home/index.php/ajsde

# Dynamic Capabilities and Cyber Resilience in Supply Chains management: Insights from Case Studies across Asia.

Md. Mahbub Hasan Mahim[1], Shuvo Kumar Mallik[2*], S. K. Monirul Islam Mahadi[3]

**Article Information**

**Received:** April 10, 2025
**Accepted:** May 14, 2025
**Published:** June 05, 2025

**Keywords**

*Asia, Case Study, Cyber Resilience, Cyber Risks, Dynamic Capabilities, Supply Chain Resilience*

## ABSTRACT

Cyber incidents pose significant threats to supply chain (SC) operations by disrupting material, information, and financial flows and compromising the availability, integrity, and confidentiality of SC assets. While supply chain resilience (SCRES) has gained increasing attention, this study focuses on the capabilities required to build cyber resilience within supply chains (SCCR). Drawing on the dynamic capabilities (DC) perspective, the study explores how firms across Asia can develop resilience to cyber risks based on a nuanced understanding of SC cyber risk characteristics. This qualitative study is based on 79 in-depth interviews with managers from 28 firms across four supply chains operating in various Asian countries. Data were collected through semi-structured interviews and secondary sources and analyzed through the lens of the DC framework, emphasizing the processes of sensing, seizing, and transforming. The study identifies both general SC resilience capabilities and specific capabilities tailored to cyber risk resilience (SCCR). It reveals that SCRES capabilities must be realigned and complemented with SCCR-specific capabilities to address cyber risks effectively. Based on the findings, ten propositions for future research are presented. For practitioners in Asia, the study emphasizes the importance of collaboration among SC partners to address cyber threats, the integration of new SC partners, and the adopting of innovative approaches. The research highlights that cyber risks require distinct strategies compared to traditional SC risks. This empirical study advances the SC management literature by applying the dynamic capabilities framework to cyber risk resilience in Asian supply chains. It identifies specific DCs necessary for SCCR, provides practical insights for managers, and offers a rare perspective on SC cyber resilience through case studies in the Asian context.

## INTRODUCTION

In an era marked by rapid digital transformation and global uncertainty, supply chains (SCs) face unprecedented disruptions. Among these, cyber risks have emerged as one of the most pressing challenges due to the increasing integration of digital technologies into supply chain operations. Understanding and enhancing supply chain resilience (SCRES), the capacity to anticipate, absorb, adapt to, and recover from disruptions, has become a critical academic and managerial interest focus. As SCs become more reliant on interconnected digital platforms, cyber threats pose unique and complex risks that traditional resilience frameworks are not fully equipped to address (Salvi *et al.*, 2022).

While significant progress has been made in identifying the general capabilities necessary to build SC resilience, much of the existing literature emphasizes physical disruptions such as natural disasters or operational breakdowns. In contrast, exploring resilience in the face of cyber threats remains limited. Cyber-attacks can compromise the availability of supply chain assets and their integrity and confidentiality, often without immediate detection. Such threats can persist within systems for extended periods, potentially spreading to connected partners and disrupting entire networks. This multidimensional nature of cyber risk requires rethinking how resilience is built and maintained across SCs (Herburger *et al.*, 2024).

Despite the rising frequency and impact of cyber-attacks on organizations of all sizes and sectors, many firms still lack clear strategies for responding to these threats. This is particularly evident in supply chains where digitalization is prioritized, yet cybersecurity is not embedded in core management practices. One reason for this gap is the limited understanding of which organizational and managerial capabilities particularly dynamic capabilities (DCs), are essential for developing cyber resilience in supply chains (Chari *et al.*, 2022). Cyber risks differ fundamentally from traditional supply chain risks, and addressing them effectively requires specific and general resilience capabilities that span technical and strategic domains.

Dynamic capabilities theory provides a relevant lens to explore this challenge. It emphasizes how organizations adapt and reconfigure their resources and competencies in response to environmental changes. As cyber risks become more pervasive, firms must develop DCs to sense emerging threats, seize opportunities to strengthen security and transform their operations accordingly (Safitra *et al.*, 2023). However, there is a lack of empirical research on how these capabilities manifest in the context of cyber resilience in SCs, particularly within Asia's diverse and fast-evolving industrial landscape.



[1] Department of Finance & Real Estate, University of Texas at Arlington, USA
[2] Department of Economics, Southeast University, Dhaka, Bangladesh
[3] Department of Cyber Security, Rowan University, Glassboro, New Jersey, USA
[*] Corresponding author's e-mail: shuvomallik.info@gmail.com

This study addresses that gap by investigating how supply chains across Asia build cyber resilience through dynamic capabilities. Using a multicast study approach, data were collected from 28 firms across four industrial supply chains. These firms were selected based on their high level of digital integration and recognized vulnerability to cyber threats. The study draws insights from supply chain management and information technology perspectives to identify critical capabilities enabling firms to anticipate and respond to cyber risks.

**This research is guided by the following question**

RQ1: How can supply chains sense and respond to cyber risks to facilitate resilience?

The findings offer practical insights for managers seeking to strengthen cyber resilience in SCs by highlighting the importance of developing tailored dynamic capabilities. These include proactive threat detection, rapid response coordination, and long-term transformation of processes and technologies (Repetto, 2023). The study also contributes to the theory by extending the application of dynamic capabilities to a novel risk domain within SCRES literature.

**The remainder of this article is structured as follows**

- Section 2 outlines the theoretical foundation, focusing on SC resilience, cyber risks, and dynamic capabilities.
- Section 3 presents the research methodology, including the multicast study design.
- Section 4 shares the key findings.
- Section 5 discusses the implications for theory and practice.
- Section 6 concludes with the study's contributions and suggests directions for future research.

## LITERATURE REVIEW

Cyber resilience in supply chains refers to the ability of supply chains (SCs) to prepare for, respond to, and recover from cyber disruptions while maintaining critical operations and services (Chen & Chang, 2021). The increasing digitization of SCs has exposed them to complex and evolving cyber threats that differ from conventional physical disruptions. These threats can affect the confidentiality, integrity, and availability of supply chain information and systems, impacting tangible and intangible assets. Unlike physical risks, cyber threats often remain undetected until significant harm occurs, making them difficult to manage, especially for non-experts. The interconnected nature of SCs means a breach in one area can quickly propagate throughout the network, magnifying the overall impact. As SCs become more dependent on digital infrastructures, understanding how to manage and build resilience against these threats has become an urgent concern for businesses, particularly in rapidly evolving economies across Asia.

The dynamic capabilities (DC) framework provides a theoretical lens to understand how organizations adapt to turbulent environments. DCs describe a firm's capacity to sense, seize, and transform in response to changes and threats (Ghosh *et al.*, 2022). In the context of cyber resilience, this means developing the ability to detect cyber risks, respond effectively, and reconfigure processes to mitigate future vulnerabilities. While many traditional applications of the DC framework emphasize leveraging opportunities, the focus here is on addressing threats, especially those linked to cyber risks. This approach is critical because recognizing and responding to threats can have a more immediate impact on operational continuity and long-term performance than focusing solely on opportunities .

Sensing involves identifying potential cyber threats within and outside the SC environment. Supply chains entail monitoring networks, sharing threat intelligence among partners, and developing situational awareness. Effective sensing requires visibility across the SC and integrating information systems that enable early detection. Through regular communication and reciprocal data-sharing, firms can develop the awareness necessary to identify vulnerabilities and emerging cyber risks preemptively (Haskard & Herath, 2025). This collective vigilance is essential in Asian SCs, which often involve complex cross-border collaborations and varying levels of technological maturity.

Once threats are identified, firms must act promptly to mitigate them. Seizing capabilities refer to the response mechanisms SCs develop to address detected cyber threats. These include partner collaboration, flexible operational adjustments, and agile responses to minimize disruption. Collaborative practices, such as joint incident response and shared recovery protocols, are critical in managing cyber-attacks affecting multiple SC actors. Additionally, investing in redundancies such as backup systems, excess capacity, or multiple suppliers can serve as buffers that enhance cyber resilience. Agile and flexible supply chains are better positioned to adapt quickly to digital threats, enabling businesses to minimize downtime and maintain service levels (Mallik *et al.*, 2025).

Transforming focuses on the long-term evolution of SC processes and structures to align with the new risk environment (Padovano & Ivanov, 2025). It involves reconfiguring resources, redesigning systems, and embedding resilience into the organizational fabric. In cyber resilience, transformation may include implementing secure-by-design principles, investing in cybersecurity training, and adapting supply chain designs to reduce risk exposure. These actions enable SCs to shift from reactive to proactive cyber risk management (Birkel & Müller, 2025). In Asia, where many SCs are undergoing digital transformation, embedding these practices can ensure that technological advancements are coupled with adequate cyber resilience strategies.

The dynamic capabilities framework offers a comprehensive approach to enhancing cyber resilience in SCs (Chen *et al.*, 2025). It helps explain how SCs can manage uncertainty by sensing cyber risks, seizing appropriate countermeasures, and transforming

operations to build long-term resilience. In the Asian context, where digital infrastructure development varies widely across regions, this framework can guide businesses in tailoring their cyber resilience strategies to local capabilities while maintaining global competitiveness. The increasing threat landscape demands that SCs move beyond static risk management approaches and adopt dynamic, capability-based models that foster resilience through continuous learning and adaptation.

## MATERIALS AND METHODS

This study adopted a multicast study design across diverse Asian contexts to explore how dynamic capabilities contribute to cyber resilience in supply chain management. This approach was chosen to provide an in-depth, contextualized understanding of how supply chains in various industries perceive, respond to, and transform in the face of cyber threats. Rather than building a new theory from scratch, the objective was to refine and extend existing theoretical perspectives on supply chain resilience, particularly about dynamic capabilities. Given the complexity and evolving nature of cyber risks in supply chains, case studies offer a powerful method to investigate real-world phenomena from multiple angles. This method allows for detailed exploration of dynamic and situational factors that affect how organizations sense, seize, and transform in response to cyber threats. The approach also supports capturing managers' rich, experiential knowledge in navigating cyber risk management challenges in highly interconnected and digitized supply networks. This study uncovers patterns in managerial behavior and organizational responses through data collection from multiple organizational sources—such as interviews, internal documents, and observations. The focus was on understanding how firms across Asia build cyber resilience by leveraging dynamic capabilities, such as real-time threat sensing, collaborative response mechanisms, and adaptive reconfiguration of supply chain resources and processes. The selected method provides a practical and theoretical foundation for discussing how firms can enhance cyber resilience using dynamic capabilities in the context of supply chain management.

### Case Selection

Initially, four manufacturing firms from various Asian industries were selected for this research. These firms, each of which operates in different sectors, have globally distributed supply chains, which provides an opportunity to explore differences and similarities within these industries. The selection of 24 industry supply chain partners across these firms was based on theoretical considerations to ensure diverse perspectives on supply chain resilience. The firms and their respective supply chains are highly relevant to understanding supply chain resilience in the face of cyber risks, as they are leaders in their industries. They are deeply involved in the digital transformation of their operations and supply chains, focusing on industries related to critical infrastructure and digitalized products.

Additionally, all four focal firms have recently experienced several cyber-attacks that affected their supply chains. The supply chains selected for this study were carefully chosen due to their complexity, involving multiple tiers of suppliers, which increases the likelihood of cyber-related supply chain disruptions. These case studies, with their varied supply chain configurations, aim to improve theory and understand how dynamic capabilities can enhance cyber resilience. The chosen cases allow for identifying patterns, similarities, and differences, providing valuable insights into how resilience strategies can be developed in response to cyber risks.

### Data Collection

A semi-structured interview protocol was developed to guide the interviews during the data collection process, during which 79 interviews were conducted across 28 firms in the four supply chains. The participants, who came from various roles such as supply chain management, IT, IT security, purchasing, sales, product management, and process management, were selected based on their involvement with supply chain resilience and cyber risks. The vast majority of these are taking place through digital platforms. The interviews were open-ended and exploratory, lasting between 25 and 165 minutes. The data collected was transcribed, coded, and analyzed by a team of researchers to identify emerging themes. The interviews continued until theoretical saturation was reached, meaning that no new significant themes emerged. In addition to the interviews, secondary data sources, such as company reports, industry journals, and public reports, were utilized to supplement the primary data. A comprehensive analysis of these sources allowed a thorough examination of the supply chains and the strategies to cope with cyber risks.

### Data Analysis

The data analysis followed a structured process. The interview transcripts were initially coded using an in-vivo approach to understand the data and uncover patterns deeply. The next phase of analysis involved the inductive development of open codes, followed by the further refinement of these codes into focused themes. The analysis continued until theoretical saturation was achieved, ensuring the findings were robust and comprehensive. MAXQDA, a qualitative data analysis tool, was employed to facilitate the coding and categorization. Throughout the analysis, trustworthiness criteria were adhered to, ensuring that the research process met the rigorous standards for qualitative research. In addition, feedback loops were incorporated, where the transcripts and results were shared with participants to confirm accuracy and obtain additional insights. These feedback loops helped to ensure the validity and reliability of the study's findings.

**Additional Methodological Aspects**

Before discussing the findings related to dynamic capabilities and cyber resilience in supply chain management, it is essential to clarify the understanding of cyber risks and their impact on supply chains. Although most disruptions due to cyber risks affect product and service availability, the study also highlights incidents that compromised the confidentiality and integrity of assets, areas often overlooked in academic literature and industry practices. The research emphasizes distinguishing between traditional supply chain risks and those arising from cyber threats. The cyber-attacks experienced by the case firms significantly impacted supply chain operations, leading to cascading disruptions across various sectors, including consumers, suppliers, and financial transactions. However, despite these disruptions, the integrity and confidentiality of the assets were not compromised, emphasizing the importance of availability in the context of cyber resilience.

**Table 1:** Case Participants and Interview Details

| Company | Participants and Firm Profile | Business Function | Cases |
|---|---|---|---|
| Case 1 | Customer Firm 1 | Industrial supplies producer | Purchasing |
| | Customer Firm 2 | Industrial supplies producer | Sales |
| | Customer Firm 3 | Industrial supplies producer | Supply Chain Management (SCM) |
| | Customer Firm 4 | Mechanical engineering | Purchasing |
| | Technology Group | Technology group | Purchasing, IT Security, SCM, IT, Sales |
| | Supplier Firm 1 | Industrial supplies | SCM |
| | Supplier Firm 2 | Media technology | CEO |
| | Supplier Firm 3 | Digital services provider | CEO |
| Case 2 | Customer Firm 5 | Critical infrastructure | IT Security |
| | Customer Firm 6 | Critical infrastructure | IT Security |
| | Supplier Firm 4 | Critical infrastructure | SCM, IT Security, Product Management |
| | Supplier Firm 5 | Electronics manufacturing | IT, Sales, Purchasing Quality Management |
| | Sub supplier Firm 1 | Board manufacturing | CEO |
| | Sub supplier Firm 2 | Equipment manufacturing | Sales, Purchasing |
| Case 3 | Customer Firm 7 | Logistics solution provider | Logistics |
| | Customer Firm 8 | Industrial supplies producer | Purchasing |
| | Customer Firm 9 | Industrial manufacturing | Purchasing |
| | Industrial Automation Producer | Industrial automation producer | SCM, Purchasing, IT, Process Management |
| | Supplier Firm 6 | Industrial automation producer | CEO, Sales |
| | Supplier Firm 7 | Industrial supplies producer | Sales |
| | Supplier Firm 8 | Industrial automation producer | Sales |
| | Supplier Firm 9 | Logistics service provider | SCM |
| Case 4 | Customer Firm 10 | Construction industry | Purchasing |
| | Customer Firm 11 | Construction industry | Digitalization |
| | Customer Firm 12 | Construction industry | Purchasing |
| | Construction Machinery Manufacturer | Construction machinery manufacturer | CEO, SCM, Logistics, IT Security, Quality Management, Product Management, Purchasing |
| | Supplier Firm 10 | Logistics service provider | IT Security |
| | Supplier Firm 11 | Industrial supplies producer | IT Security |

**Table 2:** Representative Quotes Underlying Second-Order Sensing Themes

| Second-order Theme | First-order Concepts | Representative Quotes |
|---|---|---|
| Sensing | Creating SC Cyber Risk Knowledge | Audit accordingly beforehand and see what measures are in place, what plans have been prepared for such events. Does the supplier have the appropriate safeguards, expertise, or support to recover quickly? Supplier-IT-Security |
| | | You can find out during audits what safeguards are in place, how well the supplier is prepared for cyber risks. Supplier-IT-Security |
| | | In our environment, we use a monitoring system to track suppliers and detect potential risks. Supplier-IT-Security |
| | | You need a specialized monitoring system to detect issues, but I am confident that significant problems will be identified. Supplier-Logistics |
| | | Penetration tests are conducted regularly, either organized by the customer or by us for the customer. Supplier-CEO |
| | | Our customers push us to ensure we are certified for cybersecurity. It's been a priority from the start." Supplier-IT-Security |
| | | Our cybersecurity team also actively monitors risk awareness, keeping us updated on current threats. Customer-IT-Security |
| Increasing Cyber Risk-Related SC Visibility | Improving SC Cyber Risk Awareness | We implement intrusion detection systems and monitoring tools to ensure network visibility and identify potential threats. Supplier-IT-Security |
| | | End-to-end visibility would be ideal, but it's challenging with current capabilities and resources. Customer-IT-Security |
| | | You need to have the right systems in place to ensure visibility for risk protection. Without these, you must be reactive. Supplier-IT-Security |
| Creating SC Cyber Threat Intelligence | Gathering Cyber Threat Information | We use multiple channels for cyber threat intelligence, including continuous vulnerability management scans, to stay updated on potential risks. Customer-IT-Security |
| | | We have outsourced some of our security services, such as vulnerability scanning, to a trusted partner. Customer-IT-Security |
| | | We also rely on specialist data and reports from market researchers to stay informed about emerging threats." Supplier-Logistics |
| | | Industry CERTs provide us with valuable threat intelligence feeds regularly, which helps us stay prepared for any cyber risks." Customer-IT-Security |

**Table 3:** Representative Quotes Underlying Second-Order Seizing Themes

| Second-order Theme | First-order Concepts | Representative Quotes |
|---|---|---|
| Seizing: Prioritizing Short-Term Cyber Risk-Related Supply Chain Collaboration | Customer-Driven Risk Awareness | Exactly this whole topic also plays a role in customer discussions. Then it is usually the case that our customers also ask us, have you looked at this, what is the status of this and then they ask for information. |
| | Proactive Supplier Risk Assessment | We have to make a risk assessment for each supplier if there are any risks that could arise, so that we can make appropriate arrangements with the supplier. |
| | Cross-Functional Risk Coordination | We have to weld our IT department together with that of the supplier, so that we naturally try to achieve some kind of information exchange as quickly as possible. |
| | Structured Scenario Planning | Have clear and end-to-end risk management, also in terms of failures of any kind. look at and accordingly have failure scenarios. |

| | | |
|---|---|---|
| | Emerging Risk Communication Discipline | "Between 0 and 1, risk management and non-delivery must happen." |
| Second-Order Theme | First-Order Concepts | Representative Quotes |
| Seizing: Building Cyber Risk-Related Supply Chain Flexibility | Rapid Task Force Deployment | The advantage of our SC is the flexibility in finding a task force across divisions that quickly takes care of such problems. |
| | Fast Incident Communication | The homepage was down, and the customers were informed relatively quickly on the homepage that we had been hacked. |
| | Internal Awareness Creation | I just tried to create awareness among the team quickly... it was very challenging to find a channel to reach everybody. |
| | Agile Contingency Response | On a completely different level, so we know immediately what we are doing and how. |
| | Situational Awareness and Early Detection | Our CERT is also looking at the whole issue of situation awareness. |
| Second-Order Theme | First-Order Concepts | Representative Quotes |
| Seizing: Building Supply Chain Cyber Risk Culture | Information Sharing Across Partners | If, for example, one of our partners is attacked, they inform us... then steps are initiated. |
| | Investment in Cybersecurity Training | The Cyber Range was officially inaugurated last year. you really have a piece of hardware that is there. |
| | Institutionalizing Cyber Insurance | "We have a cyber security insurance policy... which is the umbrella for everyone." |
| | Internalizing Learning from Attacks | This has also led to a rethinking of certain things, for example, the entire data security... we really only lose five minutes. |
| | Shared Departmental Understanding | A soft factor... is that you have the understanding of the department for each other and together for the customer. |

**Table 4:** Representative Quotes Underlying Second-Order Transforming Themes

| **Second-order Theme** | **First-order Concepts** | **Representative Quotes** |
|---|---|---|
| Transforming: Prioritizing Long-Term Cyber Risk-Related Supply Chain Collaboration | Strategic Supplier Alignment | Because we have done many things where we realize that we also have a strategic component. we will have other requirements in the future. For example, patching must be faster. The processes must be adapted. we will then be in dialogue with the suppliers again. |
| | Information Proactivity Expectations | That is the key, being proactive. That you say, they have to inform much more. In reality, you only get most of the information when they ask for it. |
| | Evolving Contractual Frameworks | If necessary, there will be an adjustment to the contract. And if this should also have a monetary effect, then, of course, purchasing would be involved again. |
| Second-Order Theme | First-Order Concepts | Representative Quotes |
| Transforming: Enhancing Cyber Risk-Related Supply Chain Reconfiguration | Secure Communication Infrastructure | That is, we certainly today find faster channels, secure channels to manage. |
| | Adaptive Technology Standards | Now they are strategically going to a [new standard]. so that their software runs under A. Because with B, the whole vulnerability management is already very impracticable |
| | Internal Response Capabilities | We have an internal CERT that coordinates all the processes and takes action in the event of incident response. |
| | Availability of Expert Resources | In the area of incident response... we have on-call contracts to simply have resources with the necessary know-how available in the event of an incident. |

## RESULTS AND DISCUSSIONS

### Major Finding

The study's findings reveal several key insights into how supply chains (SCs) can build resilience to cyber risks through three micro-foundations: sensing, seizing, and transforming. These micro-foundations involve various capabilities that help SCs detect, respond to, and ultimately adapt to cyber threats and risks.

### Sensing Cyber Risks

Sensing is the first critical step in building resilience, focusing on detecting and understanding cyber threats within the SC. The study identifies three capabilities that facilitate sensing:

1. Creating SC Cyber Risk Knowledge: Broadening awareness about cyber risks and understanding their impact on SC operations. Companies must integrate cyber risk awareness across all departments and partners.
2. Increasing SC Visibility: This involves expanding visibility across the entire SC to identify vulnerabilities and detect risks that may not be immediately obvious. A comprehensive view of the SC, including both first-tier and beyond, helps mitigate potential cascading effects.
3. Creating SC Cyber Threat Intelligence: This capability involves collecting and sharing cyber threat data from external sources like CERTs, communities, and conferences. Proactively sharing this intelligence across the SC allows for better risk management and unified response strategies.

### Seizing Cyber Risks

Once threats are sensed, SCs must develop strategies to act on these risks. The study identifies three key seizing capabilities:

1. Prioritizing Short-Term Cyber Risk Collaboration: After detecting a cyber threat, SCs must collaborate quickly with partners to address vulnerabilities. This could involve audits, assessments, or the creation of specialized task forces to manage the response.
2. Building Cyber Risk-Related Flexibility: SCs must remain agile to respond to disruptions rapidly. This involves having redundant processes, backup systems, and contingency plans to ensure continuity of operations during cyber incidents.
3. Building SC Cyber Risk Culture: A strong cyber risk culture ensures all departments, not just IT, know potential risks. This culture encourages collaboration, learning from past disruptions, and continuous improvement through training and awareness campaigns.

### Transforming SCs to Enhance Cyber Resilience

In addition to responding to immediate threats, SCs must transform to adapt and future-proof their operations against evolving cyber risks. This involves:

1. Prioritizing Long-Term Cyber Risk Collaboration: SCs must engage in strategic, long-term collaborations with partners to create lasting improvements. This may involve structural changes, process realignments, and ongoing communication to ensure continuous risk mitigation.
2. Enhancing Cyber Risk-Related SC Reconfiguration: When existing partnerships or systems are insufficient to manage cyber risks, SCs must be ready to reconfigure their operations. This can include changing partners, upgrading security measures, or creating new teams focused on cyber risk management.

These three micro foundations form a comprehensive framework for enhancing SC resilience against cyber risks. Sensing, seizing, and transforming each is critical in building a robust and responsive cyber resilience strategy. Through improved knowledge, visibility, collaboration, and cultural alignment, SCs can more effectively detect, respond to, and mitigate the impact of cyber threats in the supply chain (Mallik *et al.*, 2025).

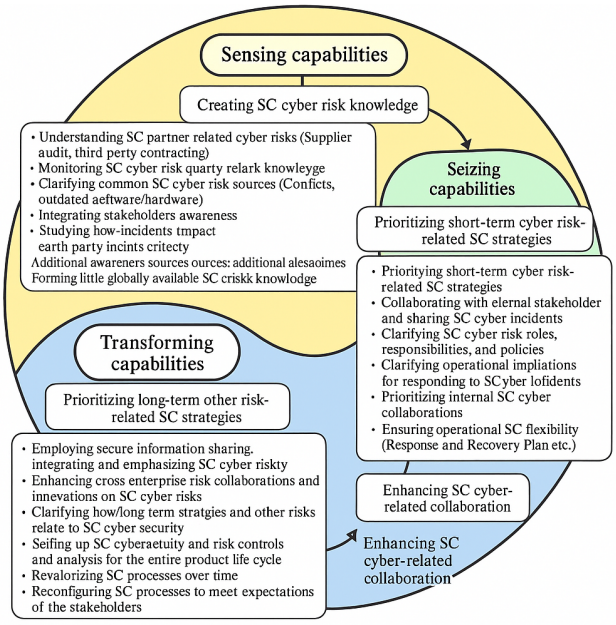


**Figure 1:** SCCR data Structure finding based on DC
*Source: Author's own work*

## Discussion

This study explores how dynamic capabilities (DCs) support the development of cyber resilience in supply chain management across diverse Asian industries. While prior studies have addressed general supply chain resilience (SCRES) and dynamic capabilities separately, this research examines their intersection in the context of cyber threats, an increasingly critical yet under-investigated domain. Our findings reveal that effectively managing cyber risks in supply chains requires synthesizing general resilience capabilities and specific cyber resilience (SCCR) practices embedded within the three clusters of DCs: sensing, seizing, and transforming. The research illustrates that the development of cyber resilience in supply chains depends on how well organizations can mobilize and coordinate internal and external resources in dynamic, vulnerable environments (Teece, 2025). Dynamic capabilities enable firms to adapt and respond to cyber disruptions that fall outside routine operations. In this context, integrating cyber-specific risk management practices into the broader framework of SCRES is essential (Mallik *et al.*, 2025). Our empirical results demonstrate that organizations across Asia actively invest in developing the ability to sense, seize, and transform in response to evolving cyber threats. Proposition 1 emerges from this analysis, suggesting that combining general SCRES and targeted SCCR capabilities strengthens cyber risk management processes and enhances cyber resilience.

Cyber threats, with their potential to compromise the confidentiality, integrity, and availability of supply chain assets, represent a distinctive class of risks. These threats often remain undetected for long periods, increasing their potential for severe and cascading disruptions. This unique nature differentiates them significantly from conventional supply chain risks and underscores the need for specialized management responses (Sadeghi *et al.*, 2025). Our findings indicate that a supply chain's orientation toward cyber risks, specifically its awareness, prioritization, and alignment of cybersecurity within broader resilience strategies, directly impacts its ability to respond to and recover from such threats.

Proposition 2 is based on this orientation: Supply chains that explicitly recognize and manage cyber threats are more likely to build and sustain robust cyber resilience.

### Sensing Capabilities for Cyber Resilience

The research identifies that a foundation for sensing cyber threats lies in cultivating a deep understanding of their characteristics and implications throughout the supply chain (Tan *et al.*, 2025). Given the complex and interconnected nature of cyber risks, traditional approaches to risk awareness are insufficient. Supply chains must acquire specialized knowledge and insights to recognize early warning signs of cyber intrusions and anticipate their downstream impacts.

Proposition 3 suggests enriching internal supply chain knowledge with specific cyber threat information enhances the sensing capabilities essential for building cyber resilience.

A key enabler of this knowledge development is visibility. By increasing transparency across the supply chain, especially in digital and operational layers, firms are better positioned to detect anomalies and map the potential spread of cyber risks. The study finds that visibility, while a known contributor to general SCRES, plays an amplified role in cyber contexts due to the latent and lateral nature of many cyber-attacks.

Proposition 4 asserts that cyber-aware supply chain visibility significantly strengthens sensing capabilities required for SCCR.

The research also highlights the importance of proactively sharing external cyber threat intelligence. Effective sensing is not confined to internal detection but involves continuously integrating external signals and collaborating with partners to interpret and disseminate threat information collectively.

Proposition 5 concludes that integrating external cyber threat information and proactively sharing it across the supply chain ecosystem enhances sensing capabilities critical for SCCR.

### Seizing Capabilities for Cyber Resilience

Once threats are detected, the ability to seize emerging opportunities for mitigation and response becomes vital. The study reveals that collaborative efforts between supply chain partners, both upstream and downstream, play a key role in managing cyber incidents (Zhang *et al.*, 2025). Organizations that engage in joint planning, incident tracking, and transparent communication across a product's lifecycle are better equipped to contain and recover from cyber events.

Proposition 6 posits that proactive collaboration among supply chain partners improves the ability to seize upon detected cyber risks, thus enhancing SCCR.

Further, the research emphasizes the value of diversity in response mechanisms. Supply chains incorporating functional and operational flexibility, such as redundant systems, alternative suppliers, and diverse cybersecurity protocols, can adapt under pressure. Such diversity ensures a tailored and agile response to various forms of cyber disruption.

Proposition 7 suggests that cultivating response and functional diversity in cyber risk management supports supply chain flexibility and bolsters seizing capabilities.

Another key finding is the role of a shared cyber risk culture. When cyber risks are understood and accepted as a collective responsibility across organizational functions, not just confined to IT departments, the supply chain is more likely to respond coherently and quickly to cyber incidents.

Proposition 8 introduces the idea that embedding a cyber-aware risk culture throughout the supply chain enhances the organization's ability to seize and address cyber threats effectively.

**Transforming Capabilities for Cyber Resilience**

Beyond sensing and seizing, the ability to transform supply chain structures and strategies in response to cyber risks is essential (Rana *et al.*, 2025). This includes reallocating resources, developing new capabilities, and long-term collaboration with partners to prevent future incidents. The study finds that sustained strategic collaboration enables supply chains to move from reactive responses to forward-looking adaptations that mitigate systemic vulnerabilities.

Proposition 9 underscores that long-term collaboration focused on aligning supply chain resources to combat cyber risks directly enhances SCCR's transforming capabilities.

Additionally, the study finds that transformative responses often require reconfiguration of the supply chain. This includes rethinking the design, partner network, and even governance models to incorporate cyber resilience as a core criterion in decision-making. Trust, innovation, and external expertise are central to this reconfiguration process.

Proposition 10 asserts that reconfiguring the supply chain in response to identified cyber risks strengthens transforming capabilities necessary for SCCR.

Based on these insights, we propose a conceptual model illustrating the relationship between dynamic capabilities and cyber resilience in supply chains. Unlike previous frameworks that address resilience in broader terms, this model maps explicitly how sensing, seizing, and transforming capabilities interact to improve SCCR. It offers a novel lens for future research and practical applications to strengthen the cyber resilience of complex, globally distributed supply chain.

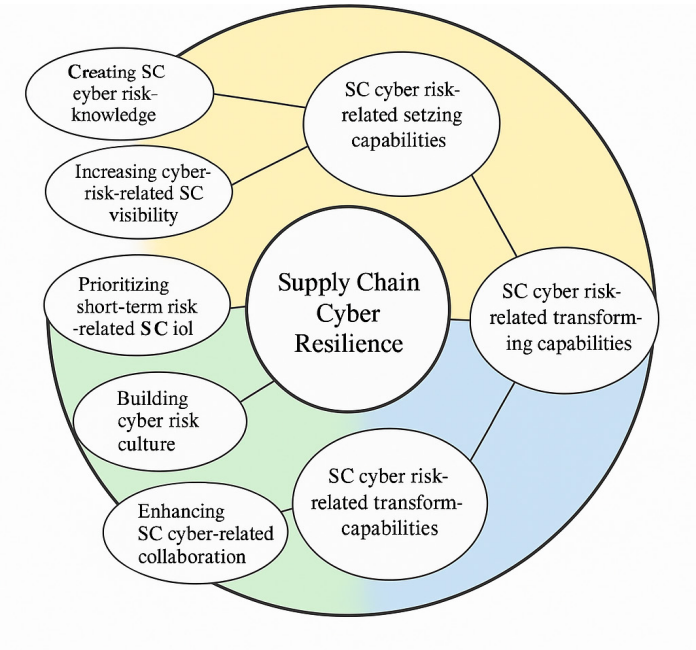


**Figure 2:** Supply chain cyber resilience
*Source: Author's own work*

The study identifies key capabilities that contribute to enhancing Supply Chain (SC) Cyber Resilience. These capabilities are categorized into three main dimensions: sensing, seizing, and transforming. These capabilities are crucial for managing and mitigating cyber risks within supply chains. As Figure SCCR Model illustrates, SC cyber risk-related sensing capabilities involve creating cyber risk knowledge and increasing visibility across the supply chain to detect threats early. Seizing capabilities include prioritizing short-term risks, building a proactive cyber risk culture, and fostering cyber-related collaboration. Meanwhile, transforming capabilities focus on long-term adaptation by changing systems, processes, and strategies to address evolving cyber threats. These findings emphasize a dynamic approach where organizations must sense risks, seize opportunities for rapid response, and continuously transform to maintain resilience in the face of cyber disruptions.

**Theoretical Implications**

1. Extension of DC Theory: The study adapts DC theory, particularly the sensing, seizing, and transforming framework, to the cyber risk context, offering a refined theoretical lens for examining SCRES.

2. Novel Capabilities: It identifies micro foundations tailored explicitly to cyber risk management, representing a significant extension of existing DC literature.

3. Temporal Dimension: It highlights SC collaboration as a dynamic, evolving process central to long-term resilience.

4. Dynamic Nature of Resilience: SCRES is framed as a dynamic property that evolves in response to cyber

threats.

5. Cross-disciplinary Integration: It emphasizes the integration of cybersecurity expertise in SCs, bridging SC and IT domains.

6. Empirical Validation: The study strengthens the DC theory's empirical grounding and demonstrates its practical application in SC cyber resilience.

**Managerial Implications**

1. Actionable Guidance: The proposed DC-based framework helps managers identify, prioritize, and sequence resilience-building activities.

2. Inter-organizational Collaboration: Emphasizes co-evolution of capabilities among SC partners and the role of trust and transparency.

3. Cybersecurity Integration: Managers should build internal or external cyber expertise and consider forming dedicated cyber threat teams.

4. Training and Education: Ongoing cyber risk training for managers is essential to stay ahead of emerging threats.

5. Enhanced Information Sharing: Cybersecurity demands new levels of information exchange, secure technological integration, and standardized security agreements.

**Limitations and Future Research**

1. Scope Limitation: Focused on European industrial SCs, which may limit generalizability.

2. Incident-Based Analysis: Future research could study SCs affected by significant cyber incidents (SolarWinds attack).

3. Temporal Dynamics: Longitudinal studies are needed to understand how SCRES evolves in response to cyber risks over time.

4. Emerging Digital Threats: Continued digitization invites new cyber threats, creating fertile ground for studying novel DCs.

5. Performance Outcomes: Future work should explore the relationship between SCCR and overall SC performance.

## CONCLUSION

This study reveals that managing cyber risks in supply chains (SCs) is a dynamic and complex process that requires specific supply chain resilience (SCRES) capabilities grounded in dynamic capabilities (DC) theory. SCs must cultivate sensing, seizing, and transforming capabilities to respond to evolving cyber threats effectively. The findings enhance understanding of how SCs can build supply chain cyber resilience (SCCR) through purposeful managerial actions aimed at reconfiguring and coordinating supply chain activities in the face of cyber risks. This approach enables SCs to adapt, recover, and thrive despite the growing challenges in the digital supply chain landscape.

## REFERENCE

Birkel, H., & Müller, J. M. (2025). Resilient by nature or technology? How Industry 4.0 enhances Supply Chain Resilience until 2035. *Supply Chain Management: An International Journal*.

Chari, A., Niedenzu, D., Despeisse, M., Machado, C. G., Azevedo, J. D., Boavida-Dias, R., & Johansson, B. (2022). Dynamic capabilities for circular manufacturing supply chains—Exploring the role of Industry 4.0 and resilience. *Business Strategy and the Environment, 31*(5), 2500-2517.

Chen, L. M., & Chang, W. L. (2021). Supply-and cyber-related disruptions in cloud supply chain firms: Determining the best recovery speeds. *Transportation Research Part E: Logistics and Transportation Review, 151*, 102347.

Chen, X., Shi, Q., Tiong, R. L., & Xiao, C. (2025). Resilience-Oriented Analysis and Enhancement of Smart Infrastructure Using a Cyber-Physical-Social Dynamic Metanetwork Approach. *Journal of Management in Engineering, 41*(4), 04025019.

Ghosh, S., Hughes, M., Hodgkinson, I., & Hughes, P. (2022). Digital transformation of industrial businesses: A dynamic capability approach. *Technovation, 113*, 102414.

Haskard, A., & Herath, D. (2025). Secure Robotics: Navigating Challenges at the Nexus of Safety, Trust, and Cybersecurity in Cyber-Physical Systems. *ACM Computing Surveys, 57*(9), 1-48.

Herburger, M., Wieland, A., & Hochstrasser, C. (2024). Building supply chain resilience to cyber risks: a dynamic capabilities perspective. *Supply Chain Management: An International Journal, 29*(7), 28-50.

Mallik, S. K., Ali, M. R., Nahiduzzaman, D. M., Shoumik, S. C., & Torikul, M. (2025). *Sustainable textile industry: Balancing growth and environmental concerns in Bangladesh*.

Mallik, S. K., Islam, M. R., Uddin, I., Ali, M. A., & Trisha, S. M. (2025). Leveraging artificial intelligence to mitigate money laundering risks through the detection of cyberbullying patterns in financial transactions. *Global Journal of Engineering and Technology Advances, 22*(01), 094-115.

Mallik, S. K., Uddin, I., Trisha, S. M., Hasan, M. M., & Rahman, M. A. (2025). *Econometric advances in causal inference: The machine learning revolution*.

Padovano, A., & Ivanov, D. (2025). Towards resilient and viable supply chains: a multidimensional model and empirical analysis. *International Journal of Production Research*, 1-39.

Rana, J., Daultani, Y., Goswami, M., & Kumar, S. (2025). *Exploring the Impact of Supply Chain Digital Transformation on Supply Chain Performance: An Empirical Investigation*. Business Strategy and the Environment.

Repetto, M. (2023). Adaptive monitoring, detection, and response for agile digital service chains. *Computers & Security, 132*, 103343.

Sadeghi R, K., Ojha, D., & Azadegan, A. (2025). *Data systems in supply chain resilience: moderated moderating effects of enterprise resource planning*. Industrial Management & Data Systems.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), 13369.

Salvi, A., Spagnoletti, P., & Noori, N. S. (2022). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security, 112*, 102507.

Tan, Z., Parambath, S. P., Anagnostopoulos, C., Singer, J., & Marnerides, A. K. (2025). Advanced Persistent Threats Based on Supply Chain Vulnerabilities: Challenges, *Solutions & Future Directions. IEEE Internet of Things Journal.*

Teece, D. J. (2025). The multinational enterprise, capabilities, and digitalization: governance and growth with world disorder. *Journal of International Business Studies*, 1-16.

Zhang, P., Bian, S., & Ju, S. (2025). Manufacturing Industrial Chain and Supply Chain Resilience in the Yangtze River Economic Belt: Evaluation and Enhancement Under Digitalization and Greening. *Sustainability, 17*(9), 3768.