International Journal of Physical Distribution & Logistics Management

1

Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness

Amer Jazairy and Mazen Brho
Department of Maritime Business Administration, Texas A&M University, Galveston, Texas, USA
Ila Manuj
Department of Supply Chain Management, University of North Texas, Denton, Texas, USA, and
Thomas J. Goldsby
Department of Supply Chain Management, University of Tennessee, Knoxville, Tennessee, USA

Received 3 December 2023
Revised 17 March 2024
24 June 2024
26 July 2024
31 July 2024
Accepted 31 July 2024

Abstract

Purpose – Despite the proliferation of cyberthreats upon the supply chain (SC) at large, knowledge on SC cybersecurity is scarce and predominantly conceptual or descriptive. Addressing this gap, this research examines the effect of SC cyber risk management strategies on integration decisions for cybersecurity (with suppliers, customers, and internally) to enhance the SC's cyber resilience and robustness.

Design/methodology/approach – A research model grounded in the supply chain risk management (SCRM) literature, with roots in the Dynamic Capabilities View and the Relational View, was developed. Survey responses of 388 SC managers at US manufacturers were obtained to test the model.

Findings – An impact of SC cyber risk management strategies on internal cyber integration was detected, which in turn impacted external cyber integration with both suppliers and customers. Further, a positive effect of internal and customer cyber integration on both cyber resilience and robustness was found, while cyber integration with suppliers impacted neither.

Practical implications – Industry practitioners may adapt certain risk management and integration strategies to enhance the cybersecurity posture of their SCs.

Originality/value – This research bridges between the established domain of SCRM and the emergent field of SC cybersecurity by forming and testing novel relationships between SCRM-rooted constructs tailored to an SC cyber risks context.

Keywords Cyberattack, Cybersecurity, Supply chain integration, Relational view, Dynamic capabilities view, Survey

Paper type Research paper

1. Introduction

The cyberspace has expanded in scope, reach, and criticality as the world is becoming more connected and digitalized. In parallel, malicious actors are increasingly seeking illegal access to digital assets to attain political, economic, and social gains (Melnyk *et al.*, 2022). Year-to-year cyberattacks are rising at a record-breaking 71% (IBM, 2024), with 80% of firms being

The authors appreciate the Texas Comprehensive Research Fund (Grant No. 169500-5220) for funding this project. Thanks also extend to Johannes Lenhardt, Jonathan Kaijser, Jordan Davis and Tariq Jazairy, among others, for their invaluable feedback on pilot testing.

International Journal of Physical Distribution & Logistics Management
Vol. 54 No. 11, 2024
pp. 1-29
Emerald Publishing Limited
0960-0035
DOI 10.1108/IJPDLM-12-2023-0445

affected by cyberattacks in 2023 alone (WEF, 2023a). Heavy economic consequences accompany these attacks; the average cost of a single data breach reached up to $4.45 million (IBM, 2023), and malicious cyber activities are expected to cost the global economy $10.5 trillion annually by 2025 (CM, 2020). Consequently, the importance of cyber risks continues to escalate (Protiviti, 2023), with the Global Risks Report identifying cybercrimes as one of the top ten most critical risks for the coming decade (WEF, 2023b).

To make matters more complex, a cyberattack on one firm can impact others that are linked, directly or indirectly, to that firm—with firms becoming increasingly vulnerable as they rely on more and different technologies to manage their supply chains (SCs) (Friday *et al.*, 2024). The infamous cyberattack on SolarWinds, a large US technology firm, impacted some 18,000 entities linked to it (ZDNET, 2020). Other major cyberattacks, such as Target (in 2013), Home Depot (in 2014), and Maersk (in 2017), took place outside the boundaries of these firms, yet the said attacks severely impacted them by causing loss of sales, high insurance and recovery cost, and reputational damage (Carnovale and Yeniyurt, 2021). In percentage, 19% of cyber breaches occurred due to a compromise at a business partner (IBM, 2022). Malicious actors also target non-business entities such as non-profit organizations, governments, and individuals—using them as backdoors into influential businesses (Wieland *et al.*, 2023). Anecdotes like these consistently suggest that cybersecurity is not merely a single firm concern; rather, an SC concern (Urciuoli *et al.*, 2013). Yet, knowledge in the supply chain management (SCM) literature is scarce on how firms in the SC perceive and respond to cyberthreats—individually or with their SC partners. Indeed, most of the research on this topic is still conceptual or descriptive (Cheung *et al.*, 2021; Friday *et al.*, 2024), and a shift to a more theoretically grounded and empirically focused investigation on such a pressing matter is urgently called for (Barbieri *et al.*, 2021; Friday *et al.*, 2024; Melnyk *et al.*, 2022) [1].

Among the few empirical studies on the topic, Colicchia *et al.* (2019) studied five UK firms and found that managing SC cyber risks requires shifting from an information technology (IT)-centric focus to a holistic, SC-oriented approach. Creazza *et al.* (2022) surveyed 100 Italian firms and emphasized the need to unite people, processes, and technology to strengthen the SC's capacity to resist cyber risks. Notably, both studies primarily anchor their stances in the cybersecurity literature external to SCM, advocating for integrating IT and SCM perspectives to elucidate how SCs navigate cyber risks. Building on this discourse, we examine the topic from an SCM vantage point.

In general, the SCM literature portrays cyberattacks as *disruptions* impacting the SC's material, information, service, and financial flows that span from raw material sources to end consumers (Ghadge *et al.*, 2020). Dealing with disruptions is rooted in the supply chain risk management (SCRM) literature (Manhart *et al.*, 2020), by which risk constitutes a combination of the probability of an event and its impact on the entity (Mitchell, 1995). Three types of risks are commonly discussed in SCRM: (1) supply—or upstream—risks (e.g. stockouts) (Zsidisin *et al.*, 2004); (2) demand—or downstream—risks (e.g. seasonality) (Tummala and Schoenherr, 2011); and (3) operational—or internal—risks (e.g. machine failure) (Manuj and Mentzer, 2008). Security risks, in turn, extend across the three streams of the SC (Mentzer, 2001), and *cyber*-security risks adhere to this extension (Pandey *et al.*, 2020). Building on this understanding, SC cyber risks share similarities with traditional SC risks, such as the possibility of occurrence, the potential to cause financial, operational, and reputational repercussions, and the need for risk management strategies to address them (Colicchia *et al.*, 2019). Meanwhile, SC cyber risks also differ from traditional SC risks due to their (1) proliferation through SC interdependencies; (2) dynamism and rapid evolution over time; (3) anonymity until their impact on the business is discovered; (4) reliance on both SC and IT departments to mitigate them; (5) far-reaching ripple effects across SC tiers; (6) traceability to malicious intent and deliberate planning; and (7) targeting of both information and physical assets. Table 1 expands on the differences between traditional SC risks and SC cyber risks [2].

Aspect	Traditional SC risks	SC cyber risks	References
Interdependencies	Low; a firm-based view is prevalent in tackling traditional SC risks	High; a SC-based view is necessary to tackle SC cyber risks	Friday *et al.* (2024), Melnyk *et al.* (2022), Pandey *et al.* (2020)
Dynamism	Somewhat predictable types of threats. Experience and proactive measures are critical for mitigation	Rapidly-changing threats that can be tweaked in real time, making them extremely difficult to manage	Colicchia *et al.* (2019), Ghadge *et al.* (2020), Sawik (2022)
Anonymity	The sources and impacts of risks are often quickly recognized	The sources and impacts of risks may not be recognized until several days/weeks after the attack, if ever	Herburger and Omar (2021), Moschovitis (2018), Renaud *et al.* (2018)
IT department involvement (in addition to the SC department)	Peripheral and mainly involves providing the IT tools and infrastructure to exchange relevant information	Critical with real-time roles involved for monitoring systems and helping respond to the attacks	Colicchia *et al.* (2019), Creazza *et al.* (2022), Herburger and Omar (2021)
Ripple effects	Low due to increased physical layers and distance between SC tiers	High due to reduced physical layers and distance in the cyberspace	Friday *et al.* (2024), Ghadge *et al.* (2020), Herburger and Omar (2021)
Intention	Mostly non-intentional and caused by natural events or unforeseen errors	Mostly intentional and caused by intruders' ill-will and deliberate planning	Kumar and Mallipeddi (2022), Pandey *et al.* (2020), Wieland *et al.* (2023)
Targeted assets	Targeted assets are primarily physical	Targeted assets are both physical and soft (i.e. information-based)	Ghadge *et al.* (2020), Pandey *et al.* (2020), Wieland *et al.* (2023)

Source(s): Created by authors

Table 1. A comparison between traditional SC risks and SC cyber risks

Given such similarities and differences, we ask to what extent can we utilize extant knowledge within SCRM to understand SC cyber risks. In other words, do we need to "reinvent the wheel" to promote our knowledge of SC cybersecurity or can we utilize already established SCRM knowledge toward that end? To join this debate, we take a balanced stance by arguing that dealing with SC cyber risks should be rooted in SCRM yet *adapted* to suit the unique characteristics of such risks. This stance is informed by the problematization approach (Alvesson and Sandberg, 2011), where scholars create a "unique conceptual space" by revisiting established concepts in the field to understand an emerging phenomenon. Here, we revisit core SCRM concepts that dealt with traditional SC risks, namely SC risk management strategies, SC integration (with suppliers, customers, and internally), and SC resilience and robustness. After scrutinizing the similarities and differences between traditional SC risks and SC cyber risks, we develop tailored concepts that leverage existing SCRM knowledge while addressing the unique aspects of SC cyber risks.

Based on this rationale, the *purpose* of this research is to examine the effect of SC cyber risk management strategies on integration decisions for cybersecurity (with suppliers, customers, and internally) to enhance the SC's cyber resilience and robustness. We employ the Dynamic Capabilities View (DCV) (Teece *et al.*, 1997)—a widely embraced lens in SCRM (e.g. Brusset and Teller, 2017; Stadtfeld and Gruchmann, 2024)—to explain the sensing, seizing, and transforming of the firm's capabilities to effectively respond to evolving cyberthreats facing its SC. For joint SC efforts, we ground our inquiry in the Relational View (RV)

(Dyer and Singh, 1998)—for three reasons: (1) its widespread adoption in SCRM (e.g. Wieland and Wallenburg, 2013; Wiengarten *et al.*, 2016); (2) its tolerance to the idea that firms integrate for benefits beyond pure cost-savings (hence, cybersecurity enhancement); and (3) growing recommendations for using it to elucidate inter-firm efforts toward SC cybersecurity (Friday *et al.*, 2024; Melnyk *et al.*, 2022). For the empirical part, we designed a survey and gathered responses of 388 carefully targeted SC managers at US manufacturers to test our research model.

This research bridges the established domain of SCRM and the emergent field of SC cybersecurity by forming and testing novel relationships between SCRM-rooted constructs tailored to an SC cyber risk context. In doing so, it broadens the scope of SCRM to include the critical dimension of cybersecurity, specifically by examining the extent to which targeted risk mitigation strategies and integration decisions—both individually and in collaboration with SC partners—can prepare SCs to navigate the rapidly evolving terrain of cyber risks. As such, this research fits into the "theory expanders" category (Colquitt and Zapata-Phelan, 2007), as it departs from SCRM to build new constructs that address SC cyber risks while also testing the premises of DCV and RV in the underexplored context of SC cybersecurity. Industry practitioners may utilize the findings to adapt their risk management and integration strategies on both the firm and SC levels to improve the cybersecurity status of their SCs, enabling them to survive and thrive amid the ever-evolving landscape of cyberthreats.

2. Adapting SCRM constructs toward SC cyber risks

2.1 SC cyber risk management strategies

Over the years, several SC risk management strategies were developed to assist SCs in coping with risks, such as risk identification, risk assessment, and risk tracking (Chopra and Sodhi, 2004). These strategies should be outward-oriented and proactive in nature to deal with unforeseen risks coming from the upstream and downstream sides of the SC (Knemeyer *et al.*, 2009). Since SC cyber risks deviate from traditional SC risks (as discussed previously), tailoring risk management strategies to suit the unique characteristics of SC cyber risks has been called for (Colicchia *et al.*, 2019), with a special emphasis on the inter-firm element (Boyson, 2014). However, the literature on SC cybersecurity is still in its early theory building stage (Melnyk *et al.*, 2022), with no clear strategies found or tested to guide SCs in dealing with cyber-related risks.

Hence, we resorted to the practice-oriented NIST Cybersecurity Framework (NIST, 2018), given its (1) tight integration with organizational risk management principles; (2) alignment with renowned cybersecurity risk management standards (e.g. ISO/IEC 27001, COBIT 5); (3) easy-to-understand language to accommodate various stakeholders; (4) emphasis on continuous improvement to address the dynamism of cyberthreats; and (5) widespread recognition/adoption among practitioners (Culot *et al.*, 2021; Krumay *et al.*, 2018). The framework advocates "using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes" (NIST, 2018, p. v). NIST tailored five traditional risk management strategies (identify, protect, detect, respond, recover) into a cyber-specific context, promoting practices like cyber risk assessment, data security, access control, cyber awareness and training, and recovery planning. We attuned NIST's framework to an SC setting (i.e. by switching NIST's strategies from a single firm's scope to an inter-firm landscape) to represent *supply chain cyber risk management strategies (SCCRMS)*.

The NIST framework and DCV are tightly connected; while SCCRMS are outward-facing and seek to mitigate SC cyber risks (as embodied in the adapted NIST framework), the capabilities enabling the prevention of business disruptions reside within the focal firm. That

is, the focal firm must exert vision, dedicate resources, and implement actions that embody internal and external overtures to protect the enterprise. As DCV posits, dynamic capabilities involve the firm's ability to integrate, reconfigure, gain, and release resources to navigate or even instigate market changes, essential for adapting as markets transform (Eisenhardt and Martin, 2000). Here, SC cyber risks act as a potent driver of industry evolution, necessitating adaptations for firms to manage threats and potentially secure advantages. Naseer *et al.* (2024) demonstrate the application of DCV in cybersecurity through active threat reconnaissance, defense, and pervasive learning. Herberger (2022) extends DCV to include surveillance and post-incident response, positing cyber resilience as a dynamic capability that involves understanding, addressing, and transforming in response to cyberthreats. This approach is distinguished from "ordinary capabilities," which, while vital, lack the dynamic nature that allows rapid adaptation to new threats.

Building on the above, we define SCCRMS as the firm's aims to establish and maintain outward-oriented capabilities for implementing processes relevant to managing SC cyber risks.

2.2 SC cyber integration

SC integration—a frequently promoted mechanism to cope with SC risks (Zhu *et al.*, 2017)—has been defined as "comprehensive collaboration among supply chain network members in strategic, tactical and operational decision-making" (Bagchi *et al.*, 2005, p. 278). From a focal firm's perspective, SC integration takes three shapes: internal (cross-functional), with suppliers (backward, or upstream), and with customers (forward, or downstream) (Fawcett and Magnan, 2002). Extant SCM research often highlights integration as a dynamic capability, relevant both within the firm (Graham, 2018) and in relations with suppliers (Vanpoucke *et al.*, 2014) and customers (Ramos *et al.*, 2023). Examining cyber-related aspects across these forms of integration is far from pervasive but finds ready application in DCV. In describing dynamic capabilities, Eisenhardt and Martin (2000, p. 1112) note: "[they] strikingly involve the creation of new, situation-specific knowledge. This occurs by engaging in experiential actions to learn quickly and thereby compensating for limited relevant existing knowledge by creating new knowledge about the current situation," emphasizing the importance of real-time information, cross-functional relationships, and intensive communication for managing processes in rapidly changing environments. Both internal and external forms of cyber integration exhibit these attributes, given the high dynamism of cyberthreats and the relentless innovations of bad actors in identifying and exploiting vulnerabilities in SC networks (Sawik, 2022).

In turn, RV highlights how the quality of external relationships with suppliers and customers can enhance the effectiveness of integration decisions to achieve desired win-wins (Dyer and Singh, 1998). Applying RV's principles in an SC cybersecurity context emphasizes (1) leveraging relationship-specific assets, such as joint cybersecurity training programs between SC partners (Colicchia *et al.*, 2019); (2) establishing knowledge-sharing routines, such as regularly flagging potential attacks and communicating their presence to the rest of the SC (Ghadge *et al.*, 2020); (3) harnessing complementary resources, such as integrating people, processes, and technology to build a comprehensive SC cybersecurity infrastructure (Creazza *et al.*, 2022); and (4) achieving effective governance, such as curbing free-riding behavior resulting from joint cybersecurity investments (Ghadge *et al.*, 2020). Such mutual efforts may not only enhance visibility and trust between the integrating partners (Tran *et al.*, 2016) but also yield a competitive advantage through an elevated cybersecurity posture (Sobb *et al.*, 2020). As RV contends, such mutually beneficial integration mirrors strategic alliances with unique competitive strengths that are not easily replicated by others, thereby generating

relational rents (i.e. profits generated by an alliance of firms that cannot be generated by either firm in isolation) (Dyer and Singh, 1998).

Meanwhile, integration with external entities like suppliers/customers can also increase the focal firm's vulnerability to cyberthreats (Pandey *et al.*, 2020), given the proliferation of such threats across SC interdependencies (Table 1). That is, the rising adoption of interconnected systems to improve physical/information flows across SCs magnifies their vulnerability to cyber risks due to a surge in physical, technical, and human penetration points (Ghadge *et al.*, 2020). Here, malicious actors try to exploit the weakest links of the chain (including suppliers/customers) through "watering hole" and "leapfrog" attacks, using these links as backdoors to larger firms (Wieland *et al.*, 2023). Consequently, an SC system with excessive integration can create a medium for cyberattacks to spread more rapidly and aggressively, leaving SC actors in a trade-off dilemma when making integration decisions. Building on Wieland *et al.*'s (2023) "managing connectivity" principle, firms need to carefully balance the benefits and drawbacks of SC integration vis-à-vis cybersecurity outcomes. We label this balanced view of integration as *supply chain cyber integration,* defined as a set of collaborative activities within and between SC entities to explicitly enhance SC cybersecurity outcomes. This concept can be separated into *internal cyber integration (ICI)*, *supplier cyber integration (SCI)*, and *customer cyber integration (CCI)*.

2.3 SC cyber resilience

Originating in information science, cyber resilience is defined as "the capacity to recover quickly from difficulties after a cyberattack" (Sawik, 2022, p. 1371). Han *et al.* (2020) argued that it is not only the system's recovery that matters, but also its readiness and response to cyberattacks. Resemblance can be drawn here with *SC resilience*, by which a resilient SC is not only capable to quickly "bounce back" from a disruption (Sheffi and Rice, 2005, p. 41), but also to move to "a new, more desirable state" (Christopher and Peck, 2004, p. 4), based on its ability to "persist, adapt, or transform in the face of change" (Wieland and Durach, 2021, p. 316). Building on this understanding, a recovery implies returning to the pre-disruptive state while radically transforming the system to face future disruptions (Castillo, 2023), turning SCs into continuously evolving systems based on their coping and adaptive capabilities (Wieland *et al.*, 2023). This view is aligned with Baghersad and Zobel (2022), who decomposed the concept of resilience into increasing operational slack and broadening operational scope. Assuming this dynamic perspective, it is necessary to accept that unpredictability will always be present alongside unremitting interconnectivity efforts amid SC entities and the evolution of disruptive events in the modern world.

Such a dynamic view of resilience has been put forth to understand *cyber* resilience in the SC, by which (1) a "disruption" facing the SC is embodied in cyberattacks, and (2) the SC's capacity to face such cyberattacks—via adaptive cyber strategies and investments—may elevate the SC to an advanced state of cybersecurity (Melnyk *et al.*, 2022). We adopt this view because it aligns with the dynamic, unpredictable, and pervasive nature of SC cyber risks (Table 1)—given that malicious actors constantly change their hacking tactics. As such, SC actors must understand that any adopted cyber defense can become obsolete if not continuously updated to address the latest waves of cyberthreats. We label this form of resilience as *supply chain cyber resilience (SCCRe),* defined as the ability of an SC to cope, adapt, and transform in the face of cyberattacks before and during their occurrence.

2.4 SC cyber robustness

Cyber robustness—like cyber resilience—is rooted in information science, defined as the ability of a system to resist cyberattacks (Baiardi *et al.*, 2016). SC robustness differs from SC resilience in that it focuses on the SC's ability to *maintain* its function *despite* the disruption

(Brandon-Jones *et al.*, 2014); that is, being more proactive while facing disorders than reactive (Durach *et al.*, 2015). Put differently, the ability to withstand is about robustness, while the ability to recover or bounce back is about resilience (Munoz *et al.*, 2022). SC robustness can result from experiences with prior disruptions, encouraging firms to place long-term investments to make their networks less prone to the negative impact of risky events (Norrman and Jansson, 2004). As such, transformation because of prior disruptions (Wieland *et al.*, 2023) can eventually yield a robust SC in the future—leading to what Melnyk *et al.* (2014) call a "hardy supply chain." Drawing parallels between system resilience and High Reliability Theory (HRT) (another way of viewing robustness), Peters *et al.* (2023, p. 51) noted "Where resilience centers on 'recovering from disruptive events', HRT focuses on 'managing the unexpected'." The authors also contend that both anticipation and containment strategies are key to operate in uncertain environments.

Accordingly, a *cyber*-robust SC should be able to fully operate and withstand cyberattacks without needing to make adaptations because of those attacks. Reaching such a sturdy state may require SC actors to invest in state-of-the-art defensive mechanisms to uphold the SC's function at all times. Yet, one may question how SCs can possibly become proactive in addressing cyberattacks that are inherently dynamic and unpredictable (Table 1). We argue that, in fact, most SCs entertain certain degrees of cyber robustness already, given that most cyberattacks are blocked by firewalls and protection apparatuses already in place at the targeted entity (Moschovitis, 2018). A recent survey of 4,744 firms showed that only 10.7% of attempted cyberattacks were successful (Accenture, 2021)—noting, however, that successful ones often bring grave consequences. Further, many cybersecurity training programs arrange simulation exercises where participants are tasked with hacking virtual organizations to learn how to secure vulnerabilities at their entities before actual attacks occur (Colicchia *et al.*, 2019)—in line with the proactive nature of robustness.

Consequently, for an SC to achieve cyber robustness, members must establish processes that aid in blocking potential attacks, develop trust and co-learning schemes, facilitate communication streams to stay ahead of cyberthreats, and be prepared to maintain operations despite the relentless attempts at penetration. We label this shape of robustness as *supply chain cyber robustness (SCCRo),* defined as the ability of an SC to maintain its function before and during cyberattacks without the need to make unplanned adaptations. Next, we build upon the abovementioned theoretical foundations to develop our hypotheses—summarized in Figure 1.

3. Hypotheses development

As already established, a firm must adopt a holistic, SC perspective when crafting its cyber risk management strategies—given the proliferation of cyberthreats upon the SC at large. Departing from the notion that the firm's strategies should guide its actions (Porter, 1996), SCCRMS should be devised before their cross-functional dispersion inside the firm. This understanding enables viewing SCCRMS as catalysts for ICI, where functional silos in the firm are brought together to fulfill the firm's overarching agenda for cybersecurity. This approach has seen success in SCM on topics like product-market innovation (Feyissa *et al.*, 2018), and green innovation (Sun and Sun, 2021). Building on the resource-based view (RBV) principles (Barney, 1991), DCV translates strategy into resource dedication to achieve innovation through the so-called SSR triad: sensing opportunities and mitigating risks, seizing actions that fulfill opportunities, and reconfiguring the resource base to yield valuable, rare, inimitable, and non-substitutable (VRIN) capabilities (Teece, 2007). Though the preponderance of DCV research speaks to leveraging market opportunities in developing VRIN resources, we contend, like Herberger (2022), that these capabilities also apply to preparedness for threats, including non-traditional forms of the cyber variety.

Naseer *et al.* (2024) stress that technology alone is insufficient for promoting cybersecurity; it must be complemented with the right people, processes, and data to transform analytical resources into capabilities. When these capabilities effectively address the dynamic and complex environment of cyberthreats, they become dynamic capabilities. Our examination focuses on balanced integration practices aimed at elevating cybersecurity, where defending the focal firm from threats can be seen as a "team sport" at two levels: within the firm and across SC partners (suppliers and customers). At the first level of analysis, within the firm, a cross-functional assembly of SC functions (planning, procurement, logistics, production) convenes with technical functions (IT, cybersecurity) to internally understand the risk landscape, set priorities, and implement security provisions. We therefore hypothesize:

H1a. Supply chain cyber risk management strategies are positively associated with internal cyber integration.

At the second level of analysis, the focal firm implements the "team sport" premise by extending surveillance and mitigation routines toward suppliers and customers. As discussed earlier, interdependencies among SC entities create a medium for cyber risks to proliferate. Thus, firms seeking to improve their cybersecurity status need to gain control not only within their own organizations but also over their connections with other firms (Friday *et al.*, 2024). Since SCCRMS are inherently SC-oriented, firms will need to integrate with both their suppliers and customers for their facilitation. To do so, a firm may utilize its SCCRMS to persuade, encourage, or in some way stimulate its upstream and downstream partners to jointly develop and implement inter-firm routines focused on SC cybersecurity; that is, enacting SCI and CCI. These provisions call for dynamic capabilities (as opposed to ordinary routines), with an emphasis on real-time data exchange, information sharing, and learning, given the highly dynamic and unpredictable nature of cyberthreats. Our conceptualization of SCI and CCI transcends the classic view of integration—which neglects the cyber vulnerability of the practice—by incorporating a cyber-oriented perspective that explicitly targets improved cybersecurity status. Consequently, and similar to instigating ICI, SCCRMS may also stimulate SCI and CCI, leading to the hypotheses:

H1b. Supply chain cyber risk management strategies are positively associated with supplier cyber integration.

H1c. Supply chain cyber risk management strategies are positively associated with customer cyber integration.

A positive effect of internal integration on both supplier and customer integration has been reported in SCM, as seen in studies on SC agility performance (Jajja *et al.*, 2018), financial performance (Yu *et al.*, 2013), and green performance (Liu *et al.*, 2018). This is rooted in the idea that inter-firm integration is contingent on intra-firm integration between customer-facing functions (e.g. marketing) and supplier-facing functions (e.g. purchasing) (Schoenherr and Swink, 2012). The SCRM literature has long adopted this view (Braunscheidel and Suresh, 2009; Munir *et al.*, 2020). Fan *et al.* (2017), for instance, argued that inter-departmental integration can enable internal, cross-functional access to risk monitoring and alerting systems. In case of a disruptive event, relevant SC partners may be alerted by the department in contact with them (via external integration mechanisms) to take necessary precautions or respond to the event (Fan *et al.*, 2017). Adapting this logic to the cyber landscape aligns with Confente *et al.*'s (2019) recommendation to inform external stakeholders about data breaches and mitigation solutions. Inspired by Ghadge *et al.* (2020), the IT department at the focal firm may flag potential cyberthreats and communicate them to customer- and supplier-facing departments, which can then circulate the detected threats across the SC to prompt joint

mitigation efforts. Lohmer *et al.* (2020) emphasize the importance of implementing timely processes to curb the spread of SC disruptions, while Naseer *et al.* (2024) highlight utilizing real-time analytics in incident response to continuously adapt to the evolving landscape of cyberthreats. We contend that such internal capabilities support the focal firm's ability to extend cyber surveillance and mitigation practices to both its upstream and downstream SC partners. Accordingly, we hypothesize:

H2a. Internal cyber integration is positively associated with supplier cyber integration.

H2b. Internal cyber integration is positively associated with customer cyber integration.

The SCM literature has recognized SC integration, with its three shapes, as an antecedent to (1) various forms of SC performance (He *et al.*, 2014), and (2) the SC's ability to manage risks (Munir *et al.*, 2020; Wieland and Wallenburg, 2013). In the cyber realm, internal integration may ingrain cyber awareness in the firm's culture and DNA (Colicchia *et al.*, 2019), leading to what Vinton Cerf (2000) calls "practicing good cyber hygiene." For instance, educating all employees at the firm about safe internet practices may foster the SC's capacity to resist, detect, respond, and recover from cyberattacks (Boyson, 2014). Such ICI-centered practices may support the SC's tendency to cope, adapt, and transform (Wieland *et al.*, 2023) in the face of cyberthreats, thus enabling SCCRe. As a result of continuous transformations and matured proactive measures (Peters *et al.*, 2023), ICI may also back the SC's ability to withstand cyberattacks, hence impacting SCCRo too. This way, dynamic capabilities in the form of ICI do not serve as ends in their own right, but rather as means to critical outcomes of enhanced cyber resilience and robustness at the SC level. Therefore, we hypothesize:

H3a. Internal cyber integration is positively associated with supply chain cyber resilience.

H3b. Internal cyber integration is positively associated with supply chain cyber robustness.

Suppliers are often seen as a source of indirect (and sometimes, direct) cyberthreats (Pandey *et al.*, 2020). Hence, cautiously integrating with suppliers—directly through information sharing and joint learning, or indirectly through third parties like IT vendors and insurance firms—may help SCs cope with SC cyber risks (Lohmer *et al.*, 2020). This can be exemplified by jointly detecting counterfeit products (Pandey *et al.*, 2020), co-training on detecting and mitigating cyberthreats (Colicchia *et al.*, 2019), responding to intellectual property violations (Tran *et al.*, 2016), or ensuring suppliers' compliance with security standards (Windelberg, 2016), like ISO/IEC 27001 (Culot *et al.*, 2021). Such buyer-supplier practices, when mutually developed into established cybersecurity programs, may activate one or more of RV's core mechanisms: relation-specific assets, knowledge-sharing routines, complementary resources, and effective governance. A strategic alliance built upon these mechanisms can create a competitive edge for the partners involved, yielding relational rents that reflect the realized synergies (Dyer and Singh, 1998). Echoing Sobb *et al.*'s (2020) proposition, we argue that this competitive edge can result from the SC's improved cybersecurity posture, facilitated by strategic integration with suppliers for cybersecurity (i.e. SCI). Further, working closely with suppliers to enhance cybersecurity may enable SCs not only to respond to immediate cyberattacks but also to adapt and cope with the evolving nature of cyberthreats (Melnyk *et al.*, 2022), thereby enhancing SCCRe. Approaching these upstream alliances proactively and preventively holds the potential to strengthen the SC's ability to withstand cyberattacks without compromising operations, positively impacting SCCRo too. Consequently, we hypothesize:

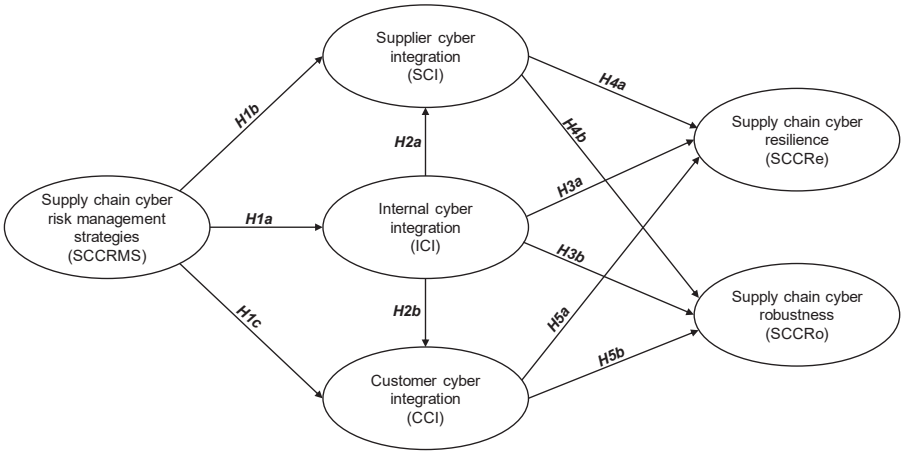
H4a. Supplier cyber integration is positively associated with supply chain cyber resilience.

H4b. Supplier cyber integration is positively associated with supply chain cyber robustness.

Just as suppliers can be a source of cyberthreats, these threats can originate from the downstream SC too (Pandey *et al.*, 2020). This highlights the importance of integrating with customers, either directly through shared information and joint learning or indirectly via third-party vendors, to mitigate SC cyber risks—while being mindful of the potential downside of integration related to increased SC vulnerability (Wieland *et al.*, 2023). Practical applications of such downstream integrations include securing customer payment gateways with the assistance of IT vendors and banks (Boyes, 2015), safeguarding customer records (Eurich *et al.*, 2010), notifying customers about data breaches and the measures taken to address them (Confente *et al.*, 2019), and ensuring adherence to data encryption standards (Colicchia *et al.*, 2019). The mature variants of these joint efforts with customers, akin to those with suppliers, can activate RV's mechanisms—relation-specific assets, knowledge-sharing routines, complementary resources, and effective governance—to carve out a distinct competitive advantage (Dyer and Singh, 1998), thereby positioning CCI as a pathway to generating relational rents due to achieved cybersecurity superiority. By ensuring downstream compliance with cybersecurity protocols, these alliances with customers not only have the potential to enhance the SC's reactivity through improved SCCRe but, when approached with foresight and prevention, may also strengthen the SC's defenses against cyberthreats, promoting SCCRo as well. As such, we hypothesize:

H5a. Customer cyber integration is positively associated with supply chain cyber resilience.

H5b. Customer cyber integration is positively associated with supply chain cyber robustness.



Source(s): Created by authors

Figure 1.
Research model

4. Methods

4.1 Survey and sample

Using Qualtrics XM, we developed a web-based survey on cyber-related risks and management strategies in the SC. The survey was designed for a single respondent working at a US manufacturer (i.e. the focal firm), with the firm representing the unit of analysis. Note that several questions addressed the respondent's view *about* his/her firm's upstream and downstream partners. We selected manufacturers because they occupy central and strategic positions within SCs, forming outsourcing relationships with local/global partners and expanding their geographic presence to local/global markets (Roh *et al.*, 2011). According to IBM's (2024) recent cybersecurity threat index, 25.7% of cyberattacks target the manufacturing segment, surpassing other segments by a significant margin. Hence, if we understand how manufacturers address cyber-related concerns in their SCs, we lay the foundation to understand which SC actors should be focused on next in our pursuit to mitigate cyber risks holistically and across SCs. Moreover, manufacturers hold a significant presence in the US marketplace, accounting for 11.39% of the total economic output and employing 8.51% of the national workforce (NAM, 2019), further motivating their selection for this study.

While we targeted single respondents, we bore in mind the arguments in favor of having multiple ones (Flynn *et al.*, 2018). Krause *et al.* (2018) stress that collecting multiple responses per firm is not always preferred as it may harm the response rate, increase the chance of nonresponse bias, and magnify the research budget. According to them, having the *right* respondent is more important than having multiple ones, but it is the researchers' responsibility to ensure that these respondents are knowledgeable about the phenomenon, have recent experience in the topic, and are willing to offer information. We followed Krause *et al.*'s (2018) guidelines, as discussed below.

Given the cross-functional nature of cybersecurity in SCs (Ghadge *et al.*, 2020), it was not intuitively clear to us which job function in the firm was more suited to answer our survey: IT or SC-related? Hence, our list of pilot testers included four SC managers and three IT managers, among others. SC managers showed greater familiarity with the topics inquired, given the questions' emphasis on SC-related strategies (internally and with SC partners) to confront cyber risks rather than technical setups to improve the firm's cybersecurity settings. Their feedback indicated not only familiarity but also practical involvement in developing and executing cybersecurity strategies at the SC level, as became evident after extended dialogues with them. One pilot tester even stressed that the IT department often prioritizes protecting the firm from cyberthreats at all costs, notwithstanding the strategic needs of the business and the importance of upholding communication channels with external SC partners to ensure smooth operations. To further ensure the knowledgeability of SC managers about the inquired topics and to protect against uninformed answers, we added the option "I don't know" in the survey for each question asked. That option was rarely chosen in the final sample (80/30,652 responses), backing the command of the respondents. Nonetheless, we still see value in replicating the study with IT managers to detect possible discrepancies between the two groups.

We hired Dynata, a professional US-based survey research firm, to distribute the survey, given the viability of this approach compared to self-administration (Schoenherr *et al.*, 2015). We also paid attention to the potential downside of this approach as it incentivizes respondents, which we countered in two steps. First, we applied strict screeners (by excluding respondents not working in manufacturing, holding job levels below middle management [3], or not in daily contact with their SC partners); 651 out of 1,039 respondents passed [4]. Second, we removed "speeders" (those answering in less than 10 min [5], $N = 249$) followed by "flatliners" (those giving similar answers or displaying repetitive patterns in their responses, $N = 14$), leaving us with 388 qualified, complete, and usable responses. These steps ensured,

as much as possible, that the final respondents were indeed the right ones, in line with Krause *et al.* (2018). Before going full-scale, we conducted a soft launch and collected 30 responses. Preliminary analysis revealed no concerns with the items or their interactions; thus, no adjustments to the instrument were needed. The soft launch also confirmed the respondents' command of the inquired topics, as evidenced by the low number of "I don't know" records in the initial sample (27/1,064 responses). The entire data collection occurred from March 11 to April 1, 2022. Table 2 shows the demographics of the respondents and their firms.

The obtained sample size ($N = 388$) is within the acceptable range for analysis with partial least squares-structural equation modeling (PLS-SEM) (Chin, 2010). It is also well above the minimum sample size of 103 recommended by Cohen (1988) (with a minimum R^2 value of 0.10, statistical power of 0.8, a probability of error of 5%, and a maximum number of predictors of 3). To assess the validity of the dataset, we checked for non-response bias by splitting the sample into early and late responses (i.e. before and after the middle date, March 21), in line with Lindner *et al.* (2001). No significant difference ($p < 0.01$) was detected for the variables characterizing the sample (firm size, sector); thus, non-response bias is unlikely. In turn, we countered common method bias (CMB) during the study design by separating dependent and independent variables, avoiding double-barreled questions, and ensuring the anonymity of respondents, as advised by Podsakoff *et al.* (2003). We also tested for CMB after data collection through two additional steps. First, by applying the Harman single-factor test; the unrotated exploratory factor analysis revealed six factors with eigenvalues greater than 1.0, with the highest variance explained by one factor being 32.53%. This is well below the critical threshold of 50% (Podsakoff *et al.*, 2003), indicating that CMB is unlikely. Second, by applying a full collinearity test, where construct-to-construct variance inflation factors (VIFs) are compared to the critical value of VIF < 3.3 to detect not serious CMB (Kock, 2017). The full collinearity test revealed VIF values between VIFmin > 1.000 and VIFmax < 2.555, further confirming the lack of CMB in our model.

Cybersecurity is a sensitive topic, and respondents might hesitate to admit failures or expose their organizations' security vulnerabilities. This could indicate social desirability bias, which we countered by ensuring respondent anonymity, informing them in the consent letter about our confidentiality policy, and phrasing our questions neutrally—in line with Krumpal (2013).

Respondent's job level	#	%	Firm's manufacturing segment	#	%
Owner / c-level / executive	94	24	Retail and consumer goods	109	28
Senior manager	209	54	Nutrition and pharmaceuticals	90	23
Middle manager	85	22	Infrastructure and transport machinery	82	21
			Electronics and telecom equipment	56	14
			Energy and natural resources	51	13
Respondent's experience (years at firm)	**#**	**%**	**Firm's size (no. of employees)**	**#**	**%**
1–3	11	3	1–9	10	3
4–7	115	30	10–49	29	7
8–12	168	43	50–249	82	21
13–20	60	15	250–499	71	18
21–40	23	6	500–1,999	118	30
41–50	11	3	2,000–4,999	50	13
			≥5,000	28	7

Source(s): Created by authors

Table 2. Demographics of survey respondents and firms ($N = 388$)

4.2 Construct measures

Since SC cybersecurity is in its early theory-building stage (Melnyk *et al.*, 2022), we developed new scales by either (1) adapting current measures from cybersecurity practice to an SC setting or (2) adapting current measures from the SCRM literature to a cybersecurity context. We refined the scales to ensure their consistency, understandability, and logical coherence through pilot tests involving practitioners with substantial IT and SC experience (as motivated earlier) alongside academics from the SCM domain. Due to the anonymity and ripple effects of SC cyber risks (Table 1), respondents were not asked to specify a particular SC they are part of when answering the survey. Instead, a sketch of the SC with the focal firm, suppliers, customers, and third parties (e.g. IT vendors) was presented to ensure the respondents' departure from the same base while assuming the focal firm's position. Five-point Likert scales were used to assess the respondents' views of their firm's engagement in a certain practice or the applicability of a statement, ranging from "to a very small extent"/ "strongly inapplicable" (value = 1) to "to a very high extent"/"strongly applicable" (value = 5). The survey questions can be found in Appendix.

SCCRMS was measured by items reflecting NIST's Cybersecurity Framework (identify, protect, detect, respond, recover), taken from NIST (2018, p. 23) and adapted from a firm-focused stance to an outward-facing SC perspective. In turn, ICI, SCI, and CCI were measured using items reflecting RV's relational mechanisms (Dyer and Singh, 1998; Schreiner *et al.*, 2009), tailored to an intra-/inter-firm SC cybersecurity context. For instance, for SCI we asked, "To what extent do you engage in the following practices with your suppliers (directly or through third parties) to improve cybersecurity?" (item 1: Active information sharing, . . .). Since the construct of SC cyber integration, with its three variants, also holds roots in DCV, we ensured that all items under ICI, SCI, and CCI are aligned with Chowdhury and Quaddus's (2017) DCV-based measures of integration—while adding "to improve cybersecurity" as a desired outcome of these integrations. SCCRe was measured using items from the SC resilience field (Ambulkar *et al.*, 2015; Chowdhury and Quaddus, 2017; El Baz and Ruel, 2021), adapted in line with the example: "We are able to cope with changes caused by cyberattacks on our supply chain." Following the same logic, SCCRo was measured by items from the SC robustness field (Durach *et al.*, 2015; El Baz and Ruel, 2021; Wieland and Wallenburg, 2012), adapted in line with the example: "We are able to retain the same stable situation we had before cyberattacks on our supply chain." To maintain discriminant validity thresholds, we dropped the items with cross-loadings on several constructs from the final model. We also controlled for size (in terms of number of employees) and industry (using *retail and consumer goods* as a baseline for comparison against the other four industries in Table 2) to detect whether these factors affect the main endogenous constructs of SCCRe and SCCRo—see "Results." Next, we present the analysis steps of our final model.

4.3 Data analysis

While we test established theories (DCV and RV), our constructs are newly adapted to address the uniqueness of SC cyber risks, making our *model* exploratory in nature. This aligns with our stance as theory expanders, where theory building and testing intersect (Colquitt and Zapata-Phelan, 2007). We applied variance-based PLS-SEM (using SmartPLS, v. 4.0.9.1) for data analysis, given its suitability for models with (1) exploratory (theory building) purposes, (2) predictive reasoning, and (3) complex structures (Hair *et al.*, 2019). These align well with (1) our model's aim of exploring potential linkages between newly adapted constructs for SC cybersecurity, (2) our desire to predict the impact of SCCRMS on SC cyber integration and SCCRe and SCCRo, and (3) the complex structure of our model (with six interlinked constructs). Next, we present the results from PLS-SEM in three sections:

assessment of the measurement model, assessment of the structural model, and analysis of the structural model.

5. Results

5.1 Assessment of measurement model

The first step is to decide whether the measurement model is formative (latent constructs are caused by their items) or reflective (latent constructs cause their items) (Chin, 2010). In SCM, models assessing SC strategies, integration, resilience, and robustness are commonly treated as reflective (Ambulkar *et al.*, 2015; El Baz and Ruel, 2021; Wieland and Wallenburg, 2013), a logic we also adopt in our model. This choice is supported by the fact that reflective constructs indicate changes in the indicators as changes in the underlying construct, meaning any variations in the latent construct will be reflected in all its measures (Jarvis *et al.*, 2003).

Following Hair *et al.* (2019), we assessed our reflective model in four steps: item loadings, internal consistency reliability, convergent validity, and discriminant validity. Table 3a shows that nearly all the items' loadings are above the 0.7 limit recommended by Hair *et al.* (2019), and all exceed the 0.5 lower limit for new scales set by Afthanorhan (2013). In turn, the composite reliability (CR) of all constructs is above the lower limit of 0.7 suggested by Hair *et al.* (2019), indicating solid internal consistency reliability. The average variance extracted (AVE) for the constructs is above the lower limit of 0.5 proposed by Bagozzi and Yi (1988), thus, their convergent validity is accepted. However, only SCCRMS reported an AVE value slightly below the 0.5 preference, which may still be accepted since its CR value exceeds 0.6 (Fornell and Larcker, 1981). Last, we tested the discriminant validity in two steps. First, we checked whether the square root of AVE for each construct is higher than its correlation with all other constructs (Fornell and Larcker, 1981). Second, we checked whether heterotrait-monotrait ratio (HTMT) values fall below the upper limit of 0.9 specified by Henseler *et al.* (2015). Table 3b shows that both criteria are met successfully for all constructs, indicating an acceptable level of discriminant validity.

All VIF values are lower than 3 in our model, signaling a lack of collinearity (Hair *et al.*, 2019). To assess the explanatory power of the model, we examined the R^2 values of all endogenous constructs. Cohen (1988) deems R^2 values of 0.26, 0.13, and 0.02 as substantial, moderate, and weak, respectively. Following Cohen's criteria, the R^2 values of our endogenous constructs can be considered substantial (Table 3c), except for ICI ($R^2 = 0.252$), which falls at the upper bounds of moderate. Table 3c also shows that the Stone-Geisser Q^2 value for all constructs is higher than zero, indicating an acceptable predictive accuracy of the PLS model for each endogenous construct (Hair *et al.*, 2019).

5.2 Analysis of structural model

We applied PLS-SEM using the bootstrapping technique (with 5,000 subsamples) to compute the path coefficients (β values) of the hypothesized relationships and to test their significance (Figure 2). For the three hypotheses under H1 on the relationships between SCCRMS and the three forms of cyber integration (ICI, SCI, CCI), only H1a on the relationship between SCCRMS and ICI was supported, leaving H1b and H1c without empirical support. This suggests that applying SCCRMS influences the internal cyber integration of the focal firm, but not its external integration with either its upstream or downstream partners. In turn, a positive effect of ICI was found on both SCI and CCI, providing support for both H2a and H2b. This indicates that integrating *externally* for cybersecurity—with both suppliers and customers—is influenced by integrating *internally* for the same purpose. As for the SC's cyber resilience and robustness, the results showed that both SCCRe and SCCRo were positively influenced by ICI and CCI, providing support for each of H3a and H5a on SCCRe, and H3b and H5b on

a. Estimation of the measurement model parameters

Construct	Item	Mean	SD	Loading	CR	AVE
Supply chain cyber risk management strategies (SCCRMS)	RiskStra-1	3.879	0.949	0.800	0.829	0.494
	RiskStra-2	3.941	1.002	0.666		
	RiskStra-3	3.938	0.993	0.625		
	RiskStra-4	3.987	0.986	0.685		
	RiskStra-5	4.083	0.890	0.726		
Internal cyber integration (ICI)	IntInteg-1	3.814	1.019	0.797	0.881	0.596
	IntInteg-2	3.657	1.069	0.781		
	IntInteg-3	3.769	1.075	0.766		
	IntInteg-4	3.747	1.127	0.735		
	IntInteg-5	3.778	1.071	0.779		
Supplier cyber integration (SCI)	SupInteg-1	3.604	1.082	0.792	0.884	0.604
	SupInteg-2	3.593	1.172	0.767		
	SupInteg-3	3.548	1.121	0.761		
	SupInteg-4	3.414	1.230	0.768		
	SupInteg-5	3.618	1.156	0.798		
Customer cyber integration (CCI)	CustInteg-1	3.648	1.084	0.794	0.881	0.596
	CustInteg-2	3.598	1.106	0.725		
	CustInteg-3	3.510	1.191	0.765		
	CustInteg-4	3.461	1.251	0.777		
	CustInteg-5	3.593	1.136	0.798		
Supply chain cyber resilience (SCCRe)	CyResil-1	3.995	0.831	0.763	0.805	0.580
	CyResil-2	3.828	0.906	0.786		
	CyResil-3	3.898	0.957	0.734		
Supply chain cyber robustness (SCCRo)	CyRobust-1	3.862	0.930	0.778	0.778	0.540
	CyRobust-2	3.953	0.878	0.658		
	CyRobust-3	4.003	0.921	0.763		

b. Discriminant validity of constructs

	SCCRMS	ICI	SCI	CCI	SCCRe	SCCRo	Size	Ind-Nutr	Ind-Infra	Ind-Elec	Ind-Enrg
SCCRMS	*0.703*	0.632	0.496	0.435	0.746	0.718	0.239	0.104	0.121	0.182	0.067
ICI	0.502	*0.772*	0.758	0.743	0.692	0.666	0.222	0.073	0.094	0.124	0.053
SCI	0.400	0.633	*0.777*	0.890	0.589	0.563	0.170	0.070	0.128	0.147	0.040
CCI	0.348	0.618	0.741	*0.772*	0.639	0.717	0.151	0.045	0.158	0.118	0.081
SCCRe	0.518	0.504	0.433	0.466	*0.761*	0.887	0.073	0.122	0.016	0.151	0.078
SCCRo	0.468	0.463	0.392	0.500	0.538	*0.735*	0.118	0.067	0.094	0.067	0.083
Size	0.207	0.200	0.158	0.137	0.058	0.084	*1.000*	0.145	0.060	0.026	0.001
Ind-Nutr	−0.077	−0.065	−0.061	−0.024	−0.076	0.036	0.145	*1.000*	0.284	0.226	0.214
Ind-Infra	0.097	−0.087	−0.115	−0.143	−0.002	−0.066	−0.060	−0.284	*1.000*	0.213	0.201
Ind-Elec	0.154	0.112	0.136	0.107	0.120	0.051	0.026	−0.226	−0.213	*1.000*	0.160
Ind-Enrg	0.054	0.049	−0.021	−0.044	0.032	0.004	−0.001	−0.214	−0.201	−0.160	*1.000*

Note(s): Diagonal values: square roots of AVE; below diagonal values: correlations; above diagonal values: HTMT

c. Quality of the structural model

	SCCRMS	ICI	SCI	CCI	SCCRe	SCCRo
R^2	–	0.252	0.410	0.384	0.309	0.295
Q^2	–	0.238	0.144	0.107	0.161	0.134

Source(s): Created by authors

Table 3. Model parameters, validity and quality tests

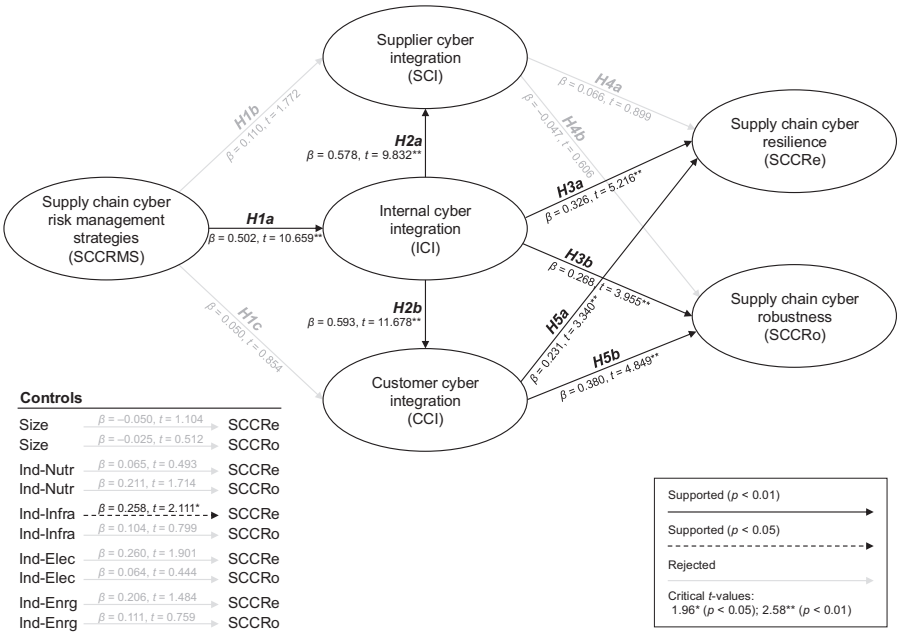


Figure 2.
Results

Source(s): Created by authors

SCCRo. In contrast, no significant impact of SCI was detected on either SCCRe or SCCRo, thus rejecting both H4a and H4b. This indicates that it is the firm's internal cyber integration as well as that with its customers that impact the SC's cyber resilience and robustness, but not its cyber integration with suppliers.

Figure 2 further shows that the effect of firm size was not supported on either SCCRe or SCCRo. This signals that despite large firms' superior access to resources and the sophistication of their cyber practices (Ghadge *et al.*, 2020), small firms seem to offset the effect of size with their greater agility and responsiveness to cyberthreats—despite their limited investment capacity in cybersecurity assets (Melnyk *et al.*, 2022). Moreover, Figure 2 reveals a marginally significant impact ($p < 0.05$) of the *infrastructure and transport machinery* industry [Ind-Infra] on SCCRe, while belonging to the other industries had no effect. This may suggest that firms within this segment implement more advanced cyber risk measures due to larger available investments and stricter regulatory mandates.

Finally, we performed post-hoc tests to detect the indirect effects in our model (Table 4). The results confirmed our primary findings by revealing an indirect effect of SCCRMS on SCCRe and SCCRo when mediated by ICI alone or together with CCI, while joint mediation of ICI and SCI between SCCRMS and both SCCRe and SCCRo was not supported.

6. Discussion

Our findings suggest that when focal firms devise SC-oriented strategies for managing SC cyber risks—pursuing elements from NIST's framework (identify, protect, detect, respond, recover) tailored to an SC context—they tend to prioritize implementing these strategies internally rather than extending them to SC partners. This preference may stem from a desire to reach a "cyber hygiene" state through internal, cross-functional integration for SC

Path	β	t-value	Significance
SCCRMS → ICI → SCCRe	0.164	4.227	**
SCCRMS → ICI → SCCRo	0.134	3.408	**
SCCRMS → SCI → SCCRe	0.007	0.670	n
SCCRMS → SCI → SCCRo	−0.005	0.544	n
SCCRMS → CCI → SCCRe	0.012	0.739	n
SCCRMS → CCI → SCCRo	0.019	0.799	n
SCCRMS → ICI → SCI → SCCRe	0.019	0.894	n
SCCRMS → ICI → SCI → SCCRo	−0.014	0.584	n
SCCRMS → ICI → CCI → SCCRe	0.069	3.264	**
SCCRMS → ICI → CCI → SCCRo	0.113	4.334	**

Note(s): Critical t-values 1.96^{*} ($p < 0.05$); 2.58^{**} ($p < 0.01$)
Source(s): Created by authors

Table 4.
Post-hoc tests: indirect effects

cybersecurity (e.g. firm-wide training on data privacy protocols for the SC)—yet without transferring such strategies to external entities. A potential explanation here is that firms began differentiating between firm-level cyber risks and SC-level cyber risks that spread through SC interdependencies (Confente *et al.*, 2019), leading them to deem external integration for cybersecurity strategies unnecessary. This may also indicate SC managers' hesitance to share SCCRMS with external parties due to the sensitive nature of cybersecurity, thus limiting their joint efforts. Nonetheless, we find this surprising, given that SCCRMS are inherently SC-oriented (outward-facing), yet external SC partners—who may play key roles in executing these strategies (Colicchia *et al.*, 2019)—do not seem *directly* involved for their fulfillment. This rejects the notion that focal firms impetuously rush to their SC partners to cope with cyberthreats coming from both streams of their SCs (given their worrisome rise lately); and instead, follow a calculative "get your cyberspace in order before you cyber integrate with the world" approach. While this result supports DCV's premise on the focal firm's flexibility to actively engage in reconnaissance, defense, and pervasive learning to deal with cyberthreats (Naseer *et al.*, 2024), it places less emphasis on the "team sport" element that advocates for extending surveillance and mitigation ambitions to suppliers and customers.

In terms of cyber resilience and robustness, our results revealed a positive effect of ICI and CCI on both SCCRe and SCCRo, while SCI affected neither. The revealed effects of ICI may signal a vital need for the focal firm's internal integration to enable cyber resilience and robustness at the SC level—even if cyberattacks tend to occur several tiers away from the focal firm (Pandey *et al.*, 2020). In fact, one may argue that ICI occupies a central orchestrating role for SC cybersecurity altogether, given its all-rounded impact on SCI, CCI, SCCRe, and SCCRo (Figure 2). When it comes to external SC partners, we saw that only cyber integration with customers had an impact on SCCRe and SCCRo, leaving suppliers untended on both fronts. These results, in aggregate, provide partial empirical support to Melnyk *et al.*'s (2022) conceptual suggestion by fully backing *intra*-firm alignment for enhanced SC cybersecurity and partially backing *inter*-firm alignment toward that end. The results also partially validate Friday *et al.*'s (2024) proposition by showing that relational ties, especially with customers, may indeed influence SC cybersecurity. However, our findings also reflect the challenging nature of achieving meaningful cyber integration with suppliers, despite the common belief that (traditional) upstream integration enhances SC performance more effectively than downstream integration (Jajja *et al.*, 2018; Yu *et al.*, 2013).

Dissecting the results further, the positive effect of ICI on SCI signals a growing buyer-supplier integration (backed by intra-buyer integration) in dealing with cyberthreats coming from the upstream SC. To exemplify, IT staff at a focal firm may collaborate with supplier-facing

staff (e.g. purchasing, operations) to formulate "cyber-informed" Supplier Code of Conduct (CoC) and Standard Operating Procedures (SOPs). These measures may prepare supplier-facing staff to enact relational mechanisms with suppliers (directly or through third parties) for SC cybersecurity. Examples include jointly securing supplier portals (Boyes, 2015) or performing regular security audits on them (Windelberg, 2016). However, these measures were not found to enhance either SCCRe or SCCRo, suggesting that: (1) cyber integration with suppliers may be ineffective for regaining or maintaining the SC's cyberhealth, (2) today's SCs have not yet reached an advanced level of upstream cyber maturity, (3) it could be difficult to manage suppliers with varying degrees of cyber readiness, and/or (4) focal firms simply switch suppliers that do not adhere to their security mandates (e.g. ISO/IEC 27001) before an impact on the SC's cyberhealth occurs. An RV-informed reader might also deduce that SCI did not function as expected to leverage the SC's competitive edge through a superior cybersecurity posture. In other words, SCI practices appear to have not matured sufficiently to establish cybersecurity programs capable of generating relational rents indicative of a significant competitive advantage. This partially rejects Sobb *et al.*'s (2020) view by disregarding upstream integration as a medium for promoting the SC's competitive advantage based on its cybersecurity status.

Considering downstream partners, the positive effect of ICI on CCI signals increased awareness of focal firms and their customers alike about the harms cyberattacks may bring to both of their entities. This brings an update to Jensen's (2015) note that customers did not often ask about cybersecurity concerns when striking the deal. To exemplify intra- and inter-firm cyber integration with customers, the focal firm's IT staff may be working jointly with its customer-facing staff (e.g. sales, marketing) to create Service Level Agreements (SLAs) that cover protecting customers' records (e.g. credit card information) from being compromised. This may lay the foundation for external integration with customers for cybersecurity, such as tailoring collaborative interfaces for secure data sharing (Colicchia *et al.*, 2019) or adjusting SLAs to meet both parties' expectations. Since CCI played a significant role in enhancing both SCCRe and SCCRo (in contrast to SCI), such joint-customer measures may assist the SC to bounce back, adapt, and transform in the face of cyberattacks as well as maintain its function despite the attacks—leading to what could possibly be called a "cyber hardy" SC. This brings conformity with RV on the downstream side of the SC, suggesting that enacting relational mechanisms—particularly with customers—may indeed create benefits (or relational rents) for the SC beyond mere cost savings, represented here by an enhanced cybersecurity posture that is possibly unique enough to contribute to the SC's competitiveness.

7. Conclusions

7.1 Theoretical contributions

In this research, we hypothesized and tested the paths through which a company's SC cyber risk management posture translates into dynamic capabilities in the form of SC integration that could, then, yield meaningful cyber protections for the SC. Specifically, we examined the relationships between SCCRMS, SC cyber integration (with suppliers–SCI; customers–CCI; and internally–ICI) and SCCRe and SCCRo. The results revealed an impact of SCCRMS on ICI, which, in turn, impacted external cyber integration with both suppliers (SCI) and customers (CCI). Further, a positive effect of ICI and CCI on both SCCRe and SCCRo was found, while SCI impacted neither.

This research bridges the established domain of SCRM and the emergent field of SC cybersecurity by forming and testing novel relationships between SCRM-rooted constructs tailored to an SC cyber risk context. In doing so, it moves the investigation of SC cybersecurity a vital step beyond mere conceptualization or description, thus responding to

urgent calls from the SCM community (Barbieri *et al.*, 2021; Friday *et al.*, 2024; Melnyk *et al.*, 2022). Further, our work falls into the "theory expanders" category—where theory testing and building intersect (Colquitt and Zapata-Phelan, 2007)—as it introduces new constructs to SCRM while grounding its predictions in established DCV and RV theories.

Starting with theory building, we introduced new (or hybrid) constructs to the SCRM field to address the unique challenges of SC cyber risks. This was achieved by either adapting prominent measures from the cybersecurity practice to SCRM or modifying existing measures from SCRM to a cybersecurity context. For instance, SCCRMS was rooted in the practice-oriented NIST Cybersecurity Framework, which we tailored to create outward-facing strategies to deal with SC cyber risks. In turn, SCCRe and SCCRo were rooted in the concepts of SC resilience and robustness from SCRM, which we subsequently adapted by specifying cyberattacks as an explicit form of SC disruptions. We demonstrated, both conceptually and empirically, the utility of our new constructs and their effectiveness in dealing with SC cyber risks. Conceptually, we provided definitions for each construct after tracing their respective evolution in the SCRM literature to reflect an SC cyber risk understanding. Empirically, the positive relationships detected in our model (with high item-loadings and 7 out of 11 supported hypotheses) verify the coherence and interdependence of our constructs, making them ready to operationalize in further research. In light of this, we urge SCM scholars to avoid "reinventing the wheel" when investigating the SC cybersecurity phenomenon and, instead, ground future inquiry in established, albeit adapted, SCRM knowledge.

Moving toward theory testing, this research tested the premises of DCV and RV—two widely used theoretical lenses in SCRM—in the underexplored context of SC cybersecurity. Starting with the former, while DCV has been applied to a variety of SC practices and phenomena, its use in the cyber risk context, in particular, is far more limited, with notable exceptions (e.g. Herburger, 2022; Naseer *et al.*, 2024). In our investigation, DCV offered a vital lens through which internal and external integration capabilities fulfilled the VRIN tenets of RBV, but in a preventive mode toward mitigation of losses. Rather than pursuing upside potential, which is common to most DCV studies related to opportunity-seeking behaviors in highly dynamic environments, we sought to underscore the need and viability of preventing losses through coordinated efforts to control and manage SC cyber risks in real time. Conceptually, the sensing/seizing/maintaining approach to opportunities (per DCV) lends itself to addressing the problem identification and resolution processes common to SC resilience, a parallel acknowledged in previous research (Stadtfeld and Gruchmann, 2024). Empirically, testing DCV in the pursuit of SCCRe and SCCRo through cyber integration mechanisms, in light of the distinctions between traditional SC risks and SC cyber risks, provides a new take of DCV and lays the foundation for further research in this area.

In turn, our testing of RV revealed the role of external SC cyber integration (i.e. with suppliers and customers) in promoting the SC's cybersecurity posture. This brought new nuances to previous SCRM research that utilized RV to understand joint efforts tackling (traditional) SC disruptions. For instance, Wieland and Wallenburg (2013) did not detect a positive effect of SC integration (which was measured by a combined construct on both suppliers and customers) on traditional SC robustness. In the cyber domain, our findings show that cyber integration does impact cyber robustness, particularly via integrating internally and with customers. This indicates that RV functions differently under SC cyber risks—thus empirically verifying the need to treat such risks differently as proposed in our work. Further, this research brings attention to the fact that integration can have both benefits and drawbacks with respect to SC cybersecurity, challenging the core assumption of RV that only considers joint relationships as a means of positive outcomes embodied in relational rents. In other words, the contingency of SC cyber risks upon SC interdependencies

can turn integration efforts (e.g. open communication, IT coupling) into a negative precursor to relational rents, since cyberthreats can traverse across the established links to cause negative consequences for the collaborating partners. We carefully utilized this notion while building our SC cyber integration constructs, calling for a balanced (or "wise") form of integration that accounts for the risks and rewards of integration on both the SC's performance and its cyberhealth.

7.2 Managerial implications

This research offers several managerial implications. First, while industry practitioners have accumulated years of experience in managing traditional SC risks stemming from both man-made and natural events, they are still grappling with the full implications of cyberthreats on their firms and SCs. This research supports their journey in understanding and planning for cybersecurity events by highlighting how SC cyber risks deviate from traditional SC risks across the dimensions of interdependencies, dynamism, anonymity, IT department involvement, ripple effects, intentions, and targeted assets. This understanding may enable practitioners to adapt their risk management strategies, resources, protocols, and relationships (both internally and externally) to address the unique nature of SC cyber risks.

Second, this research revealed the importance of SCCRMS as a facilitator of internal, cross-functional integration for SC cybersecurity. Although these strategies are—and arguably should be—outward-oriented to embrace an inter-firm scope (given the proliferation of cyberattacks across the SC), we noted that focal firms disperse such strategies internally without directly involving their external SC partners for their fulfillment. Nonetheless, we advise focal firms to involve IT managers together with managers from customer-facing functions (e.g. marketing) and supplier-facing functions (e.g. purchasing) when devising their SCCRMS, given the technical nature of SC cybersecurity and the revealed impact of ICI on both SCI and CCI. Such intra- and inter-firm involvements may be carried out by leveraging dynamic capabilities and knowledge-sharing routines to handle cybersecurity concerns, e.g. through continuous co-training on data privacy protocols and joint decision-making on security audits.

Third, since ICI and CCI played important roles in enhancing SCCRe and SCCRo, firms may consider intensifying their internal integration efforts alongside those with their customers (directly, or through third-party vendors) to preserve the cyberhealth of their SCs. Here, all relevant departments at the focal firm may co-develop SCCRMS to prepare the department in contact with customers with cyber-informed SLAs covering coordinated and measurable protocols to jointly identify, protect, detect, respond, and recover from cyberattacks. As empirically found, this might not only help their SC to bounce back and adapt in the face of cyberattacks (SCCRe), but also promote the SC's ability to withstand future cyberthreats (SCCRo).

In turn, since SCI did not have an impact on either SCCRe or SCCRo, we urge focal firms to revisit their relationships with suppliers to identify possible reasons why their joint upstream efforts are not contributing to their SC's cyberhealth. Here, it is important to note that suppliers—especially SMEs—may lack the knowledge or resources necessary to improve their cybersecurity status. Moreover, suppliers that are expected to make investments in cybersecurity assets may not directly benefit from them, creating responsibility versus accountability riddles in tackling cyberthreats amid SCs. In light of this, a recent report highlights ongoing debates over a potentially controversial law to shift liability for cybersecurity failures to the companies that caused them (Newman, 2023). But currently, suppliers that are forced to comply with cyber mandates tend to make immediate changes, delay compliance, create a false pretense of compliance, or leave the SC (Friday *et al.*, 2024). The latter scenario can be particularly challenging due to

the time-consuming process of onboarding a new supplier and the potential loss of unique capabilities possessed by the departing supplier. To address this, focal firms may encourage SCI by providing financial and technical support to improve their suppliers' cyber readiness and incorporating cyber risk measures into their requests for proposals, CoCs, and supplier evaluation processes.

7.3 Limitations and further research

Several limitations should be noted in this research. First, we only covered the views of focal firms (given their central position in SCs)—though we asked respondents *about* their SC partners. Other SC actors may offer a different take on the topic, especially SME suppliers who are typically most vulnerable to cyberthreats (Melnyk *et al.*, 2022). This is especially important since these suppliers often lack the know-how related to cybersecurity and the financial capacity to invest in cyber assets. Second, response bias may still exist since we approached single respondents with SC-related expertise only. Despite carefully targeting these respondents through strict screening and data cleaning measures, other functions in the firm, like IT, may offer a different view—given the cross-functional nature of cybersecurity. This limitation could also be rectified through in-depth case studies involving various functions in the firm or by analyzing archival data on SC cyberbreaches and mitigation procedures. Third, although this research recognizes that integration with external partners can have both risks and benefits with respect to SC cybersecurity, the findings revealed only the beneficial side of the concept. This opens the door for further research to investigate when integration is advised to enhance SC cybersecurity and when it should be limited to protect the focal firm. Fourth, firms today might still be learning how to deal with cyberthreats in their SCs, making one wonder if this investigation was conducted a bit too early. Here, we deem the timeframe of this study highly suitable, since most firms have already witnessed cyberthreats in one way or another (IBM, 2024). Yet, we also encourage further research to replicate the analysis in the near future to see whether the results hold when cybersecurity practices across SCs are further established. Fifth, more research is needed to understand why the infrastructure and transport machinery sector has a greater influence on SCCRe compared to other sectors, as found in this study. Lastly, although we covered a large sample of US manufacturers, we recommend replicating the analysis in other sectors/countries to see if similar results can be obtained.

Notes

1. See Supplementary Material for details about the contributions of this research compared to extant literature.
2. See Supplementary Material for extended discussion on the differences and similarities between traditional SC risks and SC cyber risks.
3. We chose middle managers (or above) for the job level because these are more likely to be (1) informed about their firm's SC strategy, (2) in contact with their firms' suppliers, customers, and other third-party vendors, and (3) acquainted with their firm's agreement with its SC partners.
4. One may note a high number of screened-out respondents, which could be unexpected given that screening criteria were initially implemented by the survey management firm. The rationale here is that most screened-out respondents belonged to junior management or were not in contact with SC partners on a daily basis—two criteria that are rather hard to fully detect in a subscribers list of a given survey research firm.
5. The 10-min threshold was decided after extensive tests by volunteering experts and the authors themselves.

References

Accenture (2021), "State of Cybersecurity Resilience 2021", available at: https://www.accenture.com/content/dam/accenture/final/a-com-migration/custom/us-en/invest-cyber-resilience/pdf/Accenture-State-Of-Cybersecurity-2021.pdf#zoom=40

Afthanorhan, W.M.A.B.W. (2013), "A comparison of partial least square structural equation modeling (PLS-SEM) and covariance based structural equation modeling (CB-SEM) for confirmatory factor analysis", *International Journal of Engineering Science and Innovative Technology*, Vol. 2 No. 5, pp. 198-205.

Alvesson, M. and Sandberg, J. (2011), "Generating research questions through problematization", *Academy of Management Review*, Vol. 36 No. 2, pp. 247-271, doi: 10.5465/amr.2009.0188.

Ambulkar, S., Blackhurst, J. and Grawe, S. (2015), "Firm's resilience to supply chain disruptions: scale development and empirical examination", *Journal of Operations Management*, Vol. 33 No. 1, pp. 111-122, doi: 10.1016/j.jom.2014.11.002.

Bagchi, P.K., Ha, B.C., Skjoett-Larsen, T. and Soerensen, L.B. (2005), "Supply chain integration: a European survey", *The International Journal of Logistics Management*, Vol. 16 No. 2, pp. 275-294, doi: 10.1108/09574090510634557.

Baghersad, M. and Zobel, C.W. (2022), "Organizational resilience to disruption risks: developing metrics and testing effectiveness of operational strategies", *Risk Analysis*, Vol. 42 No. 3, pp. 561-579, doi: 10.1111/risa.13769.

Bagozzi, R.P. and Yi, Y. (1988), "On the evaluation of structural equation models", *Journal of the Academy of Marketing Science*, Vol. 16 No. 1, pp. 74-94, doi: 10.1177/009207038801600107.

Baiardi, F., Tonelli, F., Bertolini, A. and Montecucco, M. (2016), "Metrics for cyber robustness", *NATO Science and Technology Organization*, pp. 1-18.

Barbieri, P., Ellram, L., Formentini, M. and Ries, J.M. (2021), "Guest editorial: emerging research and future pathways in digital supply chain governance", *International Journal of Operations and Production Management*, Vol. 41 No. 7, pp. 1021-1034, doi: 10.1108/ijopm-07-2021-903.

Barney, J. (1991), "Firm resources and sustained competitive advantage", *Journal of Management*, Vol. 17 No. 1, pp. 99-120, doi: 10.1177/014920639101700108.

Boyes, H. (2015), "Cybersecurity and cyber-resilient supply chains", *Technology Innovation Management Review*, Vol. 5 No. 4, pp. 28-34, doi: 10.22215/timreview/888.

Boyson, S. (2014), "Cyber supply chain risk management: revolutionizing the strategic control of critical IT systems", *Technovation*, Vol. 34 No. 7, pp. 342-353, doi: 10.1016/j.technovation.2014.02.001.

Brandon-Jones, E., Squire, B., Autry, C.W. and Petersen, K.J. (2014), "A contingent resource-based perspective of supply chain resilience and robustness", *Journal of Supply Chain Management*, Vol. 50 No. 3, pp. 55-73, doi: 10.1111/jscm.12050.

Braunscheidel, M.J. and Suresh, N.C. (2009), "The organizational antecedents of a firm's supply chain agility for risk mitigation and response", *Journal of Operations Management*, Vol. 27 No. 2, pp. 119-140, doi: 10.1016/j.jom.2008.09.006.

Brusset, X. and Teller, C. (2017), "Supply chain capabilities, risks, and resilience", *International Journal of Production Economics*, Vol. 184, pp. 59-68, doi: 10.1016/j.ijpe.2016.09.008.

Carnovale, S. and Yeniyurt, S. (Eds.) (2021), *Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions*, World Scientific.

Castillo, C. (2023), "Is there a theory of supply chain resilience? A bibliometric analysis of the literature", *International Journal of Operations and Production Management*, Vol. 43 No. 1, pp. 22-47, doi: 10.1108/ijopm-02-2022-0136.

Cerf, V. (2000), "Vinton Cerf's statement to the United States Congress Joint Economic Committee on 23 February 2000", available at: https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm

Cheung, K.F., Bell, M.G. and Bhattacharjya, J. (2021), "Cybersecurity in logistics and supply chain management: an overview and future research directions", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 146, 102217, doi: 10.1016/j.tre.2020.102217.

Chin, W.W. (2010), "How to write up and report PLS analyses", in *Handbook of Partial Least Squares*, Springer, pp. 655-690.

Chopra, S. and Sodhi, M.S. (2004), "Supply-chain breakdown", *MIT Sloan Management Review*, Vol. 46 No. 1, pp. 53-61.

Chowdhury, M.M.H. and Quaddus, M. (2017), "Supply chain resilience: conceptualization and scale development using dynamic capability theory", *International Journal of Production Economics*, Vol. 188, pp. 185-204, doi: 10.1016/j.ijpe.2017.03.020.

Christopher, M. and Peck, H. (2004), "Building the resilient supply chain", *The International Journal of Logistics Management*, Vol. 15 No. 2, pp. 1-13, doi: 10.1108/09574090410700275.

CM (Cybercrime Magazine) (2020), "Cybercrime to cost the world $10.5 trillion annually by 2025", available at: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Cohen, J. (1988), *Statistical Power Analysis for Behavioral Sciences*, 2nd ed., Lawrence Erlbaum Associates, Hillsdale.

Colicchia, C., Creazza, A. and Menachof, D.A. (2019), "Managing cyber and information risks in supply chains: insights from an exploratory analysis", *Supply Chain Management: An International Journal*, Vol. 24 No. 2, pp. 215-240, doi: 10.1108/scm-09-2017-0289.

Colquitt, J.A. and Zapata-Phelan, C.P. (2007), "Trends in theory building and theory testing: a five-decade study of the Academy of Management Journal", *Academy of Management Journal*, Vol. 50 No. 6, pp. 1281-1303, doi: 10.5465/amj.2007.28165855.

Confente, I., Siciliano, G.G., Gaudenzi, B. and Eickhoff, M. (2019), "Effects of data breaches from user-generated content: a corporate reputation analysis", *European Management Journal*, Vol. 37 No. 4, pp. 492-504, doi: 10.1016/j.emj.2019.01.007.

Creazza, A., Colicchia, C., Spiezia, S. and Dallari, F. (2022), "Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era", *Supply Chain Management: An International Journal*, Vol. 27 No. 1, pp. 30-53, doi: 10.1108/scm-02-2020-0073.

Culot, G., Nassimbeni, G., Podrecca, M. and Sartor, M. (2021), "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", *The TQM Journal*, Vol. 33 No. 7, pp. 76-105, doi: 10.1108/tqm-09-2020-0202.

Durach, C.F., Wieland, A. and Machuca, J.A. (2015), "Antecedents and dimensions of supply chain robustness: a systematic literature review", *International Journal of Physical Distribution and Logistics Management*, Vol. 45 Nos 1/2, pp. 118-137, doi: 10.1108/ijpdlm-05-2013-0133.

Dyer, J.H. and Singh, H. (1998), "The relational view: cooperative strategy and sources of interorganizational competitive advantage", *Academy of Management Review*, Vol. 23 No. 4, pp. 660-679, doi: 10.5465/amr.1998.1255632.

Eisenhardt, K.M. and Martin, J.A. (2000), "Dynamic capabilities: what are they?", *Strategic Management Journal*, Vol. 21 Nos 10-11, pp. 1105-1121, doi: 10.1002/1097-0266(200010/11)21:10/11<1105::aid-smj133>3.0.co;2-e.

El Baz, J. and Ruel, S. (2021), "Can supply chain risk management practices mitigate the disruption impacts on supply chains' resilience and robustness? Evidence from an empirical survey in a COVID-19 outbreak era", *International Journal of Production Economics*, Vol. 233, 107972, doi: 10.1016/j.ijpe.2020.107972.

Eurich, M., Oertel, N. and Boutellier, R. (2010), "The impact of perceived privacy risks on organizations' willingness to share item-level event data across the supply chain", *Electronic Commerce Research*, Vol. 10 No. 3, pp. 423-440, doi: 10.1007/s10660-010-9062-0.

Fan, H., Li, G., Sun, H. and Cheng, T.C.E. (2017), "An information processing perspective on supply chain risk management: antecedents, mechanism, and consequences", *International Journal of Production Economics*, Vol. 185, pp. 63-75, doi: 10.1016/j.ijpe.2016.11.015.

Fawcett, S.E. and Magnan, G.M. (2002), "The rhetoric and reality of supply chain integration", *International Journal of Physical Distribution and Logistics Management*, Vol. 32 No. 5, pp. 339-361, doi: 10.1108/09600030210436222.

Feyissa, T.T., Sharma, R.R.K. and Lai, K.K. (2018), "The impact of the core company's strategy on the dimensions of supply chain integration", *The International Journal of Logistics Management*, Vol. 30 No. 1, pp. 231-260, doi: 10.1108/ijlm-03-2017-0080.

Flynn, B., Pagell, M. and Fugate, B. (2018), "Survey research design in supply chain management: the need for evolution in our expectations", *Journal of Supply Chain Management*, Vol. 54 No. 1, pp. 1-15, doi: 10.1111/jscm.12161.

Fornell, C.G. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50, doi: 10.2307/3151312.

Friday, D., Melnyk, S.A., Altman, M., Harrison, N. and Ryan, S. (2024), "An inductive analysis of collaborative cybersecurity management capabilities, relational antecedents and supply chain cybersecurity parameters", *International Journal of Physical Distribution and Logistics Management*, Vol. 54 No. 5, pp. 476-500, doi: 10.1108/ijpdlm-01-2023-0034.

Ghadge, A., Weiß, M., Caldwell, N.D. and Wilding, R. (2020), "Managing cyber risk in supply chains: a review and research agenda", *Supply Chain Management: An International Journal*, Vol. 25 No. 2, pp. 223-240.

Graham, S. (2018), "Antecedents to environmental supply chain strategies: the role of internal integration and environmental learning", *International Journal of Production Economics*, Vol. 197, pp. 283-296, doi: 10.1016/j.ijpe.2018.01.005.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to use and how to report the results of PLS-SEM", *European Business Review*, Vol. 31 No. 1, pp. 2-24, doi: 10.1108/ebr-11-2018-0203.

Han, Y., Chong, W.K. and Li, D. (2020), "A systematic literature review of the capabilities and performance metrics of supply chain resilience", *International Journal of Production Research*, Vol. 58 No. 15, pp. 4541-4566, doi: 10.1080/00207543.2020.1785034.

He, Y., Lai, K.K., Sun, H. and Chen, Y. (2014), "The impact of supplier integration on customer integration and new product performance: the mediating role of manufacturing flexibility under trust theory", *International Journal of Production Economics*, Vol. 147, pp. 260-270, doi: 10.1016/j.ijpe.2013.04.044.

Henseler, J., Ringle, C.M. and Sarstedt, M. (2015), "A new criterion for assessing discriminant validity in variance-based structural equation modeling", *Journal of the Academy of Marketing Science*, Vol. 43 No. 1, pp. 115-135, doi: 10.1007/s11747-014-0403-8.

Herburger, M. (2022), "Supply chain resilience: a concept for coping with cyber risks", *Copenhagen Business School PhD Series N*, Vol. 23, p. 2022.

Herburger, M. and Omar, A. (2021), "Connecting supply chain management to cybersecurity", in *Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions*, pp. 13-30.

IBM (2022), "Cost of a data breach 2022", available at: https://www.ibm.com/security/data-breach

IBM (2023), "IBM security X-Force threat intelligence index 2023", available at: https://www.ibm.com/reports/threat-intelligence

IBM (2024), "X-Force threat intelligence index 2024", available at: https://www.ibm.com/downloads/cas/L0GKXDWJ

Jajja, M.S.S., Chatha, K.A. and Farooq, S. (2018), "Impact of supply chain risk on agility performance: mediating role of supply chain integration", *International Journal of Production Economics*, Vol. 205, pp. 118-138, doi: 10.1016/j.ijpe.2018.08.032.

Jarvis, C.B., MacKenzie, S.B. and Podsakoff, P.M. (2003), "A critical review of construct indicators and measurement model misspecification in marketing and consumer research", *Journal of Consumer Research*, Vol. 30 No. 2, pp. 199-218, doi: 10.1086/376806.

Jensen, L. (2015), "Challenges in maritime cyber-resilience", *Technology Innovation Management Review*, Vol. 5 No. 4, pp. 35-39, doi: 10.22215/timreview889.

Knemeyer, A.M., Zinn, W. and Eroglu, C. (2009), "Proactive planning for catastrophic events in supply chains", *Journal of Operations Management*, Vol. 27 No. 2, pp. 141-153, doi: 10.1016/j.jom.2008.06.002.

Kock, N. (2017), "Common method bias: a full collinearity assessment method for PLS-SEM. Partial least squares path modeling", in *Basic Concepts, Methodological Issues and Applications*, pp. 245-257.

Krause, D., Luzzini, D. and Lawson, B. (2018), "Building the case for a single key informant in supply chain management survey research", *Journal of Supply Chain Management*, Vol. 54 No. 1, pp. 42-50, doi: 10.1111/jscm.12159.

Krumay, B., Bernroider, E.W. and Walser, R. (2018), "Evaluation of cybersecurity management controls and metrics of critical infrastructures: a literature review considering the NIST Cybersecurity Framework", *Secure IT Systems: 23rd Nordic Conference, Proceedings 23. NordSec 2018, Oslo, Norway, November 28-30, 2018*, Springer, pp. 369-384.

Krumpal, I. (2013), "Determinants of social desirability bias in sensitive surveys: a literature review", *Quality and Quantity*, Vol. 47 No. 4, pp. 2025-2047, doi: 10.1007/s11135-011-9640-9.

Kumar, S. and Mallipeddi, R.R. (2022), "Impact of cybersecurity on operations and supply chain management: emerging trends and future research directions", *Production and Operations Management*, Vol. 31 No. 12, pp. 4488-4500, doi: 10.1111/poms.13859.

Lindner, J.R., Murphy, T.H. and Briers, G.E. (2001), "Handling nonresponse in social science research", *Journal of Agricultural Education*, Vol. 42 No. 4, pp. 43-53, doi: 10.5032/jae.2001.04043.

Liu, Y., Blome, C., Sanderson, J. and Paulraj, A. (2018), "Supply chain integration capabilities, green design strategy and performance: a comparative study in the auto industry", *Supply Chain Management: An International Journal*, Vol. 23 No. 5, pp. 431-443, doi: 10.1108/scm-03-2018-0095.

Lohmer, J., Bugert, N. and Lasch, R. (2020), "Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: an agent-based simulation study", *International Journal of Production Economics*, Vol. 228, 107882, doi: 10.1016/j.ijpe.2020.107882.

Manhart, P., Summers, J.K. and Blackhurst, J. (2020), "A meta-analytic review of supply chain risk management: assessing buffering and bridging strategies and firm performance", *Journal of Supply Chain Management*, Vol. 56 No. 3, pp. 66-87, doi: 10.1111/jscm.12219.

Manuj, I. and Mentzer, J.T. (2008), "Global supply chain risk management", *Journal of Business Logistics*, Vol. 29 No. 1, pp. 133-155, doi: 10.1002/j.2158-1592.2008.tb00072.x.

Melnyk, S.A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J.F. and Friday, D. (2022), "New challenges in supply chain management: cybersecurity across the supply chain", *International Journal of Production Research*, Vol. 60 No. 1, pp. 162-183, doi: 10.1080/00207543.2021.1984606.

Melnyk, S.A., Zobel, C.W., Macdonald, J.R. and Griffis, S.E. (2014), "Making sense of transient responses in simulation studies", *International Journal of Production Research*, Vol. 52 No. 3, pp. 617-632, doi: 10.1080/00207543.2013.803626.

Mentzer, J.T. (Ed.) (2001), *Supply Chain Management*, Sage Publications, Thousand Oaks, CA.

Mitchell, V.W. (1995), "Organizational risk perception and reduction: a literature review", *British Journal of Management*, Vol. 6 No. 2, pp. 115-133, doi: 10.1111/j.1467-8551.1995.tb00089.x.

Moschovitis, C. (2018), *Cybersecurity Program Development for Business: The Essential Planning Guide*, John Wiley & Sons.

Munir, M., Jajja, M.S.S., Chatha, K.A. and Farooq, S. (2020), "Supply chain risk management and operational performance: the enabling role of supply chain integration", *International Journal of Production Economics*, Vol. 227, 107667, doi: 10.1016/j.ijpe.2020.107667.

Munoz, A., Billsberry, J. and Ambrosini, V. (2022), "Resilience, robustness, and antifragility: towards an appreciation of distinct organizational responses to adversity", *International Journal of Management Reviews*, Vol. 24 No. 2, pp. 181-187, doi: 10.1111/ijmr.12289.

NAM (National Association of Manufacturers) (2019), "2019 United States manufacturing facts", available at: https://www.nam.org/state-manufacturing-data/2019-united-states-manufacturing-facts/

Naseer, H., Desouza, K., Maynard, S.B. and Ahmad, A. (2024), "Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics", *European Journal of Information Systems*, Vol. 33 No. 2, pp. 200-220, doi: 10.1080/0960085X.2023.2257168.

Newman (2023), "The high-stakes blame game in the white house cybersecurity plan", available at: https://www.wired.com/story/white-house-national-cybersecurity-strategy/

NIST (2018), "Framework for improving critical infrastructure cybersecurity", available at: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

Norrman, A. and Jansson, U. (2004), "Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident", *International Journal of Physical Distribution and Logistics Management*, Vol. 34 No. 5, pp. 434-456, doi: 10.1108/09600030410545463.

Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A. (2020), "Cyber security risks in globalized supply chains: conceptual framework", *Journal of Global Operations and Strategic Sourcing*, Vol. 13 No. 1, pp. 103-128, doi: 10.1108/jgoss-05-2019-0042.

Peters, E., Knight, L., Boersma, K. and Uenk, N. (2023), "Organizing for supply chain resilience: a high reliability network perspective", *International Journal of Operations and Production Management*, Vol. 43 No. 1, pp. 48-69, doi: 10.1108/ijopm-03-2022-0167.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. and Podsakoff, N.P. (2003), "Common method biases in behavioral research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879-903, doi: 10.1037/0021-9010.88.5.879.

Porter, M.E. (1996), "What is strategy?", *Harvard Business Review*, Vol. 74 No. 6, pp. 61-78.

Protiviti (2023), "The top risks for 2023: a global view", available at: https://www.protiviti.com/us-en/newsletter/bp159-top-risks-2023#:~:text=Cybersecurity%20and%20data%20privacy%20remain,story%20of%20a%20changing%20world

Ramos, E., Patrucco, A.S. and Chavez, M. (2023), "Dynamic capabilities in the 'new normal': a study of organizational flexibility, integration and agility in the Peruvian coffee supply chain", *Supply Chain Management: An International Journal*, Vol. 28 No. 1, pp. 55-73, doi: 10.1108/scm-12-2020-0620.

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P. and Orgeron, C. (2018), "Is the responsibilization of the cyber security risk reasonable and judicious?", *Computers and Security*, Vol. 78, pp. 198-211, doi: 10.1016/j.cose.2018.06.006.

Roh, J.J., Min, H. and Hong, P. (2011), "A co-ordination theory approach to restructuring the supply chain: an empirical study from the focal company perspective", *International Journal of Production Research*, Vol. 49 No. 15, pp. 4517-4541, doi: 10.1080/00207543.2010.497506.

Sawik, T. (2022), "A linear model for optimal cybersecurity investment in Industry 4.0 supply chains", *International Journal of Production Research*, Vol. 60 No. 4, pp. 1368-1385, doi: 10.1080/00207543.2020.1856442.

Schoenherr, T. and Swink, M. (2012), "Revisiting the arcs of integration: cross-validations and extensions", *Journal of Operations Management*, Vol. 30 Nos 1-2, pp. 99-115, doi: 10.1016/j.jom.2011.09.001.

Schoenherr, T., Ellram, L.M. and Tate, W.L. (2015), "A note on the use of survey research firms to enable empirical data collection", *Journal of Business Logistics*, Vol. 36 No. 3, pp. 288-300, doi: 10.1111/jbl.12092.

Schreiner, M., Kale, P. and Corsten, D. (2009), "What really is alliance management capability and how does it impact alliance outcomes and success?", *Strategic Management Journal*, Vol. 30 No. 13, pp. 1395-1419, doi: 10.1002/smj.790.

Sheffi, Y. and Rice, J.B. Jr (2005), "A supply chain view of the resilient enterprise", *MIT Sloan Management Review*, Vol. 47 No. 1, pp. 41-48.

Sobb, T., Turnbull, B. and Moustafa, N. (2020), "Supply chain 4.0: a survey of cyber security challenges, solutions and future directions", *Electronics*, Vol. 9 No. 11, p. 1864, doi: 10.3390/electronics9111864.

Stadtfeld, G.M. and Gruchmann, T. (2024), "Dynamic capabilities for supply chain resilience: a meta-review", *The International Journal of Logistics Management*, Vol. 35 No. 2, pp. 623-648, doi: 10.1108/IJLM-09-2022-0373.

Sun, Y. and Sun, H. (2021), "Green innovation strategy and ambidextrous green innovation: the mediating effects of green supply chain integration", *Sustainability*, Vol. 13 No. 9, p. 4876, doi: 10.3390/su13094876.

Teece, D.J. (2007), "Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance", *Strategic Management Journal*, Vol. 28 No. 13, pp. 1319-1350, doi: 10.1002/smj.640.

Teece, D.J., Pisano, G. and Shuen, A. (1997), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18 No. 7, pp. 509-533, doi: 10.1002/(sici)1097-0266(199708)18:7<509::aid-smj882>3.0.co;2-z.

Tran, T.T.H., Childerhouse, P. and Deakins, E. (2016), "Supply chain information sharing: challenges and risk mitigation strategies", *Journal of Manufacturing Technology Management*, Vol. 27 No. 8, pp. 1102-1126, doi: 10.1108/jmtm-03-2016-0033.

Tummala, R. and Schoenherr, T. (2011), "Assessing and managing risks using the supply chain risk management process (SCRMP)", *Supply Chain Management: An International Journal*, Vol. 16 No. 8, pp. 474-483, doi: 10.1108/13598541111171165.

Urciuoli, L., Männistö, T., Hintsa, J. and Khan, T. (2013), "Supply chain cyber security–potential threats", *Information and Security: An International Journal*, Vol. 29 No. 1, pp. 51-67, doi: 10.11610/isij.2904.

Vanpoucke, E., Vereecke, A. and Wetzels, M. (2014), "Developing supplier integration capabilities for sustainable competitive advantage: a dynamic capabilities approach", *Journal of Operations Management*, Vol. 32 Nos 7-8, pp. 446-461, doi: 10.1016/j.jom.2014.09.004.

WEF (World Economic Forum) (2023a), "The ransomware warning sign we should all have on our radar", available at: https://www.weforum.org/agenda/2023/11/the-ransomware-warning-sign-we-should-all-have-on-our-radar/

WEF (World Economic Forum) (2023b), "The global risks report 2023", the 18 Edition, available at: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Wieland, A. and Durach, C.F. (2021), "Two perspectives on supply chain resilience", *Journal of Business Logistics*, Vol. 42 No. 3, pp. 315-322, doi: 10.1111/jbl.12271.

Wieland, A. and Wallenburg, C.M. (2012), "Dealing with supply chain risks: linking risk management practices and strategies to performance", *International Journal of Physical Distribution and Logistics Management*, Vol. 42 No. 10, pp. 887-905, doi: 10.1108/09600031211281411.

Wieland, A. and Wallenburg, C.M. (2013), "The influence of relational competencies on supply chain resilience: a relational view", *International Journal of Physical Distribution and Logistics Management*, Vol. 43 No. 4, pp. 300-320, doi: 10.1108/ijpdlm-08-2012-0243.

Wieland, A., Stevenson, M., Melnyk, S.A., Davoudi, S. and Schultz, L. (2023), "Thinking differently about supply chain resilience: what we can learn from social-ecological systems thinking", *International Journal of Operations and Production Management*, Vol. 43 No. 1, pp. 1-21, doi: 10.1108/ijopm-10-2022-0645.

Wiengarten, F., Humphreys, P., Gimenez, C. and McIvor, R. (2016), "Risk, risk management practices, and the success of supply chain integration", *International Journal of Production Economics*, Vol. 171, pp. 361-370, doi: 10.1016/j.ijpe.2015.03.020.

Windelberg, M. (2016), "Objectives for managing cyber supply chain risk", *International Journal of Critical Infrastructure Protection*, Vol. 12, pp. 4-11, doi: 10.1016/j.ijcip.2015.11.003.

Yu, W., Jacobs, M.A., Salisbury, W.D. and Enns, H. (2013), "The effects of supply chain integration on customer satisfaction and financial performance: an organizational learning perspective", *International Journal of Production Economics*, Vol. 146 No. 1, pp. 346-358, doi: 10.1016/j.ijpe.2013.07.023.

ZDNET (2020), "SEC filings: SolarWinds says 18,000 customers were impacted by recent hack", available at: https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/

Zhu, Q., Krikke, H. and Caniëls, M.C. (2017), "Integrated supply chain risk management: a systematic review", *The International Journal of Logistics Management*, Vol. 28 No. 4, pp. 1123-1141, doi: 10.1108/ijlm-09-2016-0206.

Zsidisin, G.A., Ellram, L.M., Carter, J.R. and Cavinato, J.L. (2004), "An analysis of supply risk assessment techniques", *International Journal of Physical Distribution and Logistics Management*, Vol. 34 No. 5, pp. 397-413, doi: 10.1108/09600030410545445.

Corresponding author
Amer Jazairy can be contacted at: jazairy.a@tamu.edu

Supplementary material

The supplementary material for this article can be found online at: https://doi.org/10.1108/IJPDLM-12-2023-0445

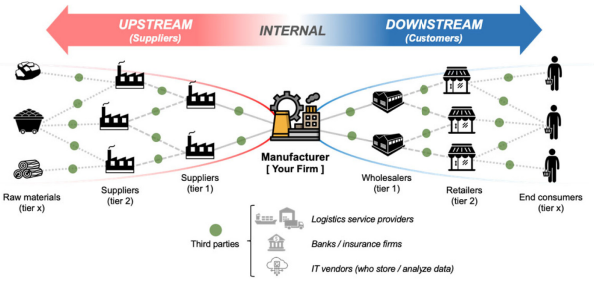
Appendix

Questionnaire (items used in this study)

In this Survey,

- A **Supply Chain** refers to a set of three or more entities (firms or individuals) directly involved in the upstream and downstream flows of products, services, finances, and/or information from raw materials to end consumers.
- A **Cyberattack** is any intentional or unintentional action or assault (using a computer, network, or hardware device) on the supply chain system that may compromise its processes, procedures, and delivery of products, information flows, and services.

Below is a graphical example of a typical supply chain in today's modern business. Please consider your firm as the "Manufacturer" when answering the survey questions.



Supply chain cyber risk management strategies *(adapted from NIST Cybersecurity Framework – NIST, 2018)*
From a supply chain cyber risk management perspective, which of the following statements apply to your **strategy**?
(1 – strongly inapplicable; 5 – strongly applicable).

- **[RiskStra-1]** We aim to **identify** cyberattacks targeting our supply chain (using, e.g., asset management, business environment, governance, risk assessment, risk management).
- **[RiskStra-2]** We aim to **protect** ourselves from cyberattacks targeting our supply chain (using, e.g., access control, awareness & training, data security, info protection processes & procedures, maintenance, protective technology).
- **[RiskStra-3]** We aim to **detect** cyberattacks targeting our supply chain (using, e.g., animalities and events, security continuous improvement, detection processes).
- **[RiskStra-4]** We aim to **respond** to cyberattacks targeting our supply chain (using, e.g., response planning, communications, analysis, mitigation, improvements).
- **[RiskStra-5]** We aim to **recover** from cyberattacks targeting our supply chain (using, e.g., recovery planning, improvements, communications).

Internal cyber integration *(adapted from Chowdhury and Quaddus, 2017; Dyer and Singh, 1998; Schreiner et al., 2009)*
To what extent do you **internally** engage in the following practices **to improve cybersecurity**? (1 – to a very small extent; 5 – to a very large extent)

- **[IntInteg-1]** Active information sharing.
- **[IntInteg-2]** Attaining mutual understanding.
- **[IntInteg-3]** Joint decision-making.
- **[IntInteg-4]** Integrating IT systems.
- **[IntInteg-5]** Learning from each other / joint learning.

Supplier cyber integration *(adapted from Chowdhury and Quaddus, 2017; Dyer and Singh, 1998; Schreiner et al., 2009)*
To what extent do you engage in the following practices **with your suppliers** (directly or through third parties) **to improve cybersecurity**? (1 – to a very small extent; 5 – to a very large extent)

- **[SupInteg-1]** Active information sharing.
- **[SupInteg-2]** Attaining mutual understanding.
- **[SupInteg-3]** Joint decision-making.
- **[SupInteg-4]** Integrating IT systems.
- **[SupInteg-5]** Learning from each other / joint learning.

Customer cyber integration *(adapted from Chowdhury and Quaddus, 2017; Dyer and Singh, 1998; Schreiner et al., 2009)*
To what extent do you engage in the following practices **with your customers** (directly or through third parties) **to improve cybersecurity**? (1 – to a very small extent; 5 – to a very large extent)

- **[CustInteg-1]** Active information sharing.
- **[CustInteg-2]** Attaining mutual understanding.
- **[CustInteg-3]** Joint decision-making.
- **[CustInteg-4]** Integrating IT systems.
- **[CustInteg-5]** Learning from each other / joint learning.

Supply chain cyber resilience *(adapted from Ambulkar et al., 2015; Chowdhury and Quaddus, 2017; El Baz and Ruel, 2021)*
From a supply chain perspective, which of the following statements apply to your cybersecurity performance? (1 – strongly inapplicable; 5 – strongly applicable)

- **[CyResil-1]** We are able to **cope** with changes caused by cyberattacks on our supply chain.
- **[CyResil-2]** We are able to **adapt** to changes caused by cyberattacks on our supply chain.
- **[CyResil-3]** We are able to **develop** a variety of possible solutions to changes caused by cyberattacks on our supply chain.

Supply chain cyber robustness *(adapted from Durach et al., 2015; El Baz and Ruel, 2021; Wieland and Wallenburg, 2012)*
From a supply chain perspective, which of the following statements apply to your cybersecurity performance? (1 – strongly inapplicable; 5 – strongly applicable)

- **[CyRobust-1]** We are able to **retain the same stable situation** we had before cyberattacks on our supply chain.
- **[CyRobust-2]** We have **sufficient time to develop a reasonable reaction** to changes caused by cyberattacks on our supply chain.
- **[CyRobust-3]** We are able to **maintain our operational capacity** despite changes caused by cyberattacks on our supply chain.