Process Theory of Supplier Cyber Risk Assessment

Sergeja Slapnicar
School of Business
University of Queensland
Australia

Tim Vidmar
School of Business
University of Queensland
Australia

Elinor Tsen
School of Business
University of Queensland
Australia
Email: e.tsen@uq.edu.au

Abstract

Managing cyber risk in the supply chain represents one of the most significant challenges in cyber risk management. The paper studies how organizations assess supplier cyber risk. We used a mixed-method approach. We conducted 33 semi-structured interviews with cybersecurity experts from various organizations closely involved in supplier cyber risk assessments, as well as consultants. We complemented our qualitative findings by surveying 53 security experts about their supplier cyber risk assessment. Based on the qualitative findings, we formulate a process theory of supplier cyber risk assessment. This theory explains how organizations assess supplier cyber risk and which contextual factors affect the maturity of cyber risk assessment and monitoring. The quantitative analysis supports the qualitative findings and suggests that the process can effectively identify risky suppliers. The paper sheds light on challenges and strategies associated with supply chain cyber risk assessment. The practical implications of our findings offer actionable insights for organizations seeking to enhance their cyber supply chain risk management.

Keywords: Third-party cyber risk, Supplier cyber risk, Cyber supply-chain risk management, Risk assessment, Assurance.

1 Introduction

Cyberattacks targeting suppliers[1] have become increasingly common, and several prominent cases have garnered significant attention in recent years. A common belief is that major threats come from Information and Communication Technology (ICT) suppliers, such as the attack on SolarWinds or the NotPetya attack, in which cyber criminals gained access to major global corporations and government agencies, causing extensive operational disruptions and global

[1] For clarity, we use the word supplier relating to various synonyms: supplier, which is an organization that enters into an agreement with the acquirer for the supply of a product or service, vendor, a commercial supplier of software or hardware, and a third-party provider who are service providers, system integrators, vendors, telecommunications, and infrastructure support that are external to an organization, as defined by the US National Institute of Standards and Technology (NIST): https://csrc.nist.gov/glossary/term/

Received 07 Jul 2024, accepted 02 Mar 2025 after 3 rounds of review with Humza Naseer as accepting Senior Editor, M. Davern & S. Black as Editors in Chief

damage of tens of billions of dollars (Alkhadra *et al.,* 2021; Crosignani *et al*., 2023; Wolff, 2021). However, a severe cyberattack on an organization can also be launched through a micro provider, such as a heating, ventilation and air-conditioning vendor in the attack on Target (Simon and Omar, 2020). In the analysis of 1,397 cyber incidents from 2000 to 2020, Benaroch (2021) found that suppliers caused 18% of these incidents. The attacks on the supply chain (SC) were growing proportionally with other cyber incidents but compromised a larger volume of confidential data. An organization can suffer a cyber incident through a direct attack on a supplier; a supplier being a conduit for a cyberattack; when a supplier stores another partner's data, i.e., as a partner-custodian; and when a supplier attacks the focal organization using privileged information (Deane et al. 2023).

Cyber incidents in SC are not caused only by cyberattacks. Noteworthy are also non-intentional risks committed by suppliers' employees or faulty supplier hardware or software that can have a crucial effect on the focal organization's provision of services (Ghadge *et al.*, 2019; Urciuli *et al.*, 2013; 2014). A case in point is Crowdstrike's failure, which affected 8.5 million Microsoft users and caused a global outage (Li, 2024). This incident highlights the increasing complexity of managing cyber risks in a SC, especially with global technology sourcing, system ownership, diverse legal jurisdictions, and heavy reliance on third parties for vital functions (Boyes, 2015). These risks underscore the importance of the emerging discipline known as Cybersecurity Supply Chain Risk Management (C-SCRM) (Boyson, 2014; Khan and Estay, 2015).

Recognizing which supplier is more likely to face disruptions because of a cyber incident is critical in effectively managing the impact of SC disruptions (Boyson, 2014). However, according to the 2022 Ponemon Institute survey of over 1,100 security experts, approximately two-thirds of participants are uncertain about having a comprehensive inventory of suppliers with which they share information (the Ponemon Institute, 2022). Only about one-third of respondents stated their organizations evaluate suppliers' security practices before establishing business relationships involving sensitive or confidential information sharing.

While the dominant cyber security frameworks and standards such as NIST, Control Objectives for Information and Related Technologies (COBIT 2019), the International Organization for Standardization and the International Electrotechnical Commission (ISO), and banking prudential regulation address processes of managing cyber risks in the SC, they are high-level, require significant expertise, and are costly (for their overview, see Supplement A). Complying with standards is not fit for purpose for small and medium-sized organizations (SMEs) that do not have sufficient resources (Ghadge *et al*., 2019) and for whom is also being assessed by such standards by multiple customers too costly. It is also unclear how supplier cyber risk assessment can be integrated into organizational-level cyber risk assessment, as guided by ISO/IEC 27005 and NIST SP 800-30.

Most prior research addresses a diverse array of topics, predominantly analyzing technical solutions, standards and protocols (e.g., Akinrolabu et al. 2019; Caldwell 2015; Hao & Cai 2011), supplier cyber risk characteristics, or the financial impact of a cyber incident in a SC (Benaroch 2021; Crossignani et al. 2023). Studies analyzing *organizational approaches* to C-SCRM are scarce due to data sensitivity and because frequently, even focal organizations do not have a good understanding of cyber risks beyond their direct (Tier 1) suppliers (Colicchia et al. 2019; Gani et al. 2023; Lewis et al. 2014; Pandey et al. 2019). We identified only six such

studies, and they highlight a significant lack of proper C-SCRM (e.g., Boyens et al. 2020; Colicchia et al. 2019; Gaudenzi & Siciliano 2018; Tran et al. 2016).

Up to this point, existing research has not focused on the supplier cyber risk assessment process, nor has it examined how contextual factors influence it. It is not well understood *what process organizations employ to assess a supplier cyber risk, how contextual factors impact this process and how effective it is in identifying a risky supplier*.

Our primary goal is to develop a process theory of supplier cyber risk assessment. We adopted the Straussian grounded theory approach (Corbin & Strauss 1990), broadly based on two process theories – *life-time* and *teleological* theory. The former is concerned with the sequential steps that form a process leading to the attainment of organizational outcomes (Mohr 1982; Markus & Robey 1988), and the latter with the goals of the process and process adaptability in response to resource constraints and environmental factors (van de Ven & Poole 1995; Baskerville 2005).

Our methods of investigation are mixed. To formulate a process theory of cyber risk assessment, we conducted semi-structured interviews with 33 security experts in charge of C-SCRM in various countries. As qualitative findings cannot answer whether the process is effective, we complemented the interview findings with a survey of 53 security experts to establish whether the controls the process entails can identify riskier suppliers.

Our study makes two original contributions to the C-SCRM literature: First, we define the process theory of supplier cyber risk assessment, which explains how organizations assess supplier cyber risk and which contextual factors affect the maturity of cyber risk assessment. The interview findings provide in-depth insights into how these practices are carried out in organizations, and the survey findings suggest that the assessment process can effectively identify riskier suppliers, especially by identifying their insufficient technological controls, the lack of supplier management support to cyber security risk management, the lack of supplier's transparency and reputation, and by considering threat intelligence's red flags. Second, the practical implications of our findings offer actionable insights for organizations seeking to enhance their cyber supply chain risk management.

2 Theoretical Background

2.1 Process Theory

To develop a grounded theory of a supplier cyber risk assessment process, we draw on process theories (Langley 1999), which are at the core of theories of explanation (Gregor 2006). Process theories are frameworks that explain how organizational activities unfold over time, emphasizing the sequences of actions and interactions among actors. For our research questions, the combination of two process theories proved particularly relevant: a process theory that theorists van de Ven and Poole (1995) call *life-cycle process theory* and *teleological process theory*. Life-cycle process theory suggests that some organizational phenomena cannot be explained by a determinate cause-and-effect relationship between variables but as the outcome of a sequence of necessary action steps (Mohr 1982; Markus & Robey 1988). Instead of pinpointing single predictors of outcomes, it explores the progression of activities over time and how complex interdependencies shape the final results. This perspective is particularly relevant in fields like Information Systems (IS), organizational behavior, and management. Cyber risk management is among the phenomena that cannot be explained with variance

theories – that is, "more X leads to more Y", because risks are highly unpredictable and transient. Rather, the logic in management of cyber risk is "if not X, then not Y", implying that the outcomes depend upon a complete chain of process activities (Baskerville 2005).

The second theory is *teleological process theory* (van de Ven & Poole 1995), which stresses that processes are designed as a trajectory to an organization's intended *goal*. An organization develops a *repetitive* sequence of goal formulation, implementation, evaluation and modification of goals based on what it has learnt (van de Ven & Poole 1995, p. 516). However, while the theory stresses the purpose, it also recognizes that an organization is constrained by its resources and environment (contextual factors), which lead to its *adaptability* (Bekmeier-Feuerhahn 2009). In the context of cyber risk management, for instance, if the highest quality of controls cannot be achieved, it is desirable to have even poor quality controls in place to prevent some damage (Baskerville 2005). The development of a cyber risk management system is cyclical and agile. In explaining organizational phenomena, these two theories have been combined: corporate strategic planning and the process of drug registration are examples that highlight the importance of the goal and adaptability and of following the sequential steps (Chakravarthy & Lorange 1991; Nutt 2002).

2.2 Supplier Cyber Risk Factors

One of the major questions in supplier risk assessment is which factors predict the likelihood and the consequences (impact) of a cyber incident related to a supplier. Keskin et al. (2021) and Dean et al. (2023) classify supplier cyber risk factors as (i) supplier cyber risk posture characteristics and (ii) the relationship between the supplier and the focal organization.

Ad i) *Supplier cyber risk posture characteristics* that define its security posture are *technology* solutions (do Amaral & Gondim 2021; Yeo et al. 2014); *certifications* (Bartol 2014; Sindhuja & Kunnathur 2015; Wolden et al. 2015); *IT governance*, e.g., the presence of CISO, CIO and/or ICT manager roles and policies, and the alignment of the SC risk management with cyber risk management (Liu et al. 2020; Vanajakumari et al. 2021); *industry affiliation* (Akinrolabu et al. 2019; Hao & Cai 2011; Keskin et al. 2021), and an organization's *targeting factor* which depends on the type of data it possesses (e.g., technological inventions or recipes).

Supplier characteristics also comprise a *human factor* (employee negligence, misinformation from leadership, inadequate training, and inappropriate access, sharing authentication credentials) (Adams & Makramalla 2015; Boyson 2014; Boyens 2015; Collichia et al. 2019; Kweon et al. 2021; Tender, 2015). Angst et al. (2017), Giunipero and Eltantawy (2004), and Lewis et al. (2014) allude to organization *size* and *financial resources*, pointing out increased attacks targeting SMEs, often considered the weakest links in information security management. Other important factors are *geographical location* (Iovan and Iovan 2016), *foreign ownership* (Topping et al. 2021) and the *complexity of a supplier's SC* (Linton et al. 2014).

Ad ii) Among factors related to *the relationship between the supplier and the focal organization*, Keskin et al. (2021) suggested the nature of the *IT integration* in the connectivity between the two firms. The risk is significantly greater if a supplier is an ICT provider or its business is IT-based, with most activities conducted online (Benthall 2017). The second factor by Keskin *et al.* (2021) is the *type and magnitude of information sharing*, which has been found critical for SC partners' preparedness to invest in network security (Bandyopadhyay et al. 2010). In addition, *highly specific services/products* increase the criticality of the supplier to the focal organization (Bode & Wagner 2015; Crosignani et al. 2023).

While this research is highly instructive, much of it is normative (Boyson 2014; Davis 2015; Lewis et al. 2014), focuses on technical solutions, or examines a single supplier risk factor. None of these studies have analyzed how these factors are collectively assessed in the supplier cyber risk assessment process or identified which factors are most critical for identifying risky suppliers.

2.3 Organizational Approaches to Supplier Cyber Risk Assessment

In our literature review, we identified only six qualitative studies that investigated the organizational practices of C-SCRM. We review them in this section. Boyson (2014) studied two organizations and found that they assessed suppliers and formalized risk agreements but lacked centralized governance and integrated communication across functions. Tran et al. (2016) studied supplier post-onboarding monitoring and noted that organizations rely on personal relationships rather than formal monitoring. Gaudenzi and Siciliano (2018) observed minimal cyber risk management of suppliers, focusing more on protecting clients' information. They did not observe practices of stipulating security requirements in the contractual agreements with key suppliers, considering disaster recovery and business continuity plans, or backing up sensitive data. However, they noted higher investments in C-SCRM and better risk management in finance and high-tech sectors. Miscommunication and misaligned awareness between IT and supply chain managers were also identified (Siciliano & Gaudenzi 2018).

Colicchia et al. (2019) found that while organizations required partners to comply with security and privacy policies, C-SCRM initiatives were mainly reactive, focusing on response and recovery rather than proactive adaptation. Requirements related to data management, IT security tools, and operational resilience were enforced, but efforts rarely extended beyond Tier 1 partners or included audits. Business continuity and disaster recovery plans were adopted reactively. Boyens et al. (2020) reported that organizations periodically surveyed suppliers to understand their security posture using tribal knowledge, self-assessment questionnaires, early risk assessments, government watch lists, supplier criticality scores, and NIST CSF assessments. Suppliers were found to implement technical controls inconsistently, which focal organizations compensated for by training of supplier personnel and requirements of implementing controls in the future. They rarely monitored suppliers after onboarding.

Prior findings suggest that organizations employ deficient and unsystematic processes. While organizations may understand how their direct suppliers or customers interact with their information systems and manage their data, they frequently lack visibility into how these immediate partners source, transmit, and exchange data, services, and components with other companies upstream and downstream in the SC. While the reviewed studies are informative, none specifically focused on the process of supplier risk assessment and monitoring nor analyzed the contextual factors affecting its maturity. Additionally, these studies investigated a rather small number of organizations, ranging from two to eleven, which calls for additional data to provide solid evidence about the state of play in C-SCRM. This sets the stage for the investigation that is undertaken by the present study.

3 Methods and Data

Given the exploratory stage of this research area, we relied on the concurrent embedded mixed method design (Creswell 2009). Our primary method was qualitative – semi-structured

interviews - which explores the processes experienced by individuals in charge of supplier cyber risk assessment. It allowed us to gain an in-depth and holistic understanding of the research questions and conceptualize organizations' processes to assess a supplier's cyber risk. The secondary method – a quantitative analysis - provided support to the primary method and enabled a statistical analysis of the question of how effective the process of supplier cyber risk assessment is in the identification of risky suppliers. Concurrent design relates to the simultaneous data collection with interviews and a survey. The reason for the concurrent data collection is the significant challenge of recruiting interviewees in relevant positions willing to discuss such a sensitive topic. This process requires considerable time and effort. The data collection for the interviews lasted over a year, from March 2023 to June 2024. A survey was carried out simultaneously to ensure that the data related to the same time period and did not become outdated in this fast-developing discipline. We embed the findings of quantitative research within the findings of qualitative research (Creswell 2009).

3.1 Qualitative method

3.1.1 Sample

We conducted interviews with 33 cybersecurity experts, encompassing cybersecurity professionals, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), IT managers, vendor managers, and consultants from various organizations, industries and countries (Table 1). We recruited them via our professional network: ISACA Brisbane Chapter and ISACA Slovenia Chapter, Women in Cyber Security (Australia), and AusCert (Australia). Among our 33 interviewees, 23 come from 18 for-profit and government organizations, and 10 are consultants providing supplier risk assessments to various clients. Each interview lasted from 45 minutes to one hour. Interviews were audio-recorded and subsequently transcribed using the Zoom platform. In cases where consent for recording was not given, detailed notes were taken. The study has obtained ethical clearance from the authors' university. All recorded videos were deleted after transcription and coding to safeguard the identity of participants and the confidentiality of the information. The interview data yielded invaluable insights into the multifaceted realm of cyber security risk assessment during the supplier selection process and after onboarding.

Participant #	Role	Experience in security (years)	Organization size (employees)	Industry	Country
P1	Principal Analyst	25	15	Consulting	Australia
P2	IT Consultant	5	Less than 10	Consulting	Slovenia
P3	CISO	25	300	Employment & Training	Australia
P4	Executive Vice President	>30	400	Cloud security	Singapore
P5	CISO	25	Over 7,000	Transportation (Critical infrastructure)	Australia
P6	Discipline Head of Business Resilience	15	Over 7,000	Transportation (Critical infrastructure)	Australia
P7	Security Sales Specialist	4	Over 1,000	Consulting	Australia

P8	Cyber Security Consultant in Governance, Risk and Compliance	2	Over 1,000	Consulting	Australia
P9	Cyber Security Consultant and Founder	18	Self-employed	Consulting	Australia
P10	Chief Technology Officer	>20	50	Software development	New Zealand
P11	Security Analysts, Specialist in 3rd party CS risk	2	Over 2,500	Consulting	Australia
P12	Security Director	9	Over 1,300	Banking	Slovenia
P13	Chief IT Internal Auditor	8	Over 1,300	Banking	Germany
P14	Cyber Security Architect	7	Over 7,000	Tertiary education	Australia
P15	Consultant, Developer	7	Less than 10	Consulting	Australia
P16	CIO	7	Over 200	Banking	Slovenia
P17	Cyber Security Consultant and Founder	20	self-employed + subcontractors	Cyber security and assurance company	Slovenia
P18	Cyber Security Consultant	15	Over 200	Vendor assessment	Australia
P19	CISO	8	Over 1,000	Insurance	Slovenia
P20	CISO of a subsidiary	19	Over 3,000	Banking	Austria
P21	Cyber Security Manager	20	Over 2,000	Municipality	Australia
P22	CISO	20	Over 5,000	Insurance	Central Europe
P23	Analyst of operational risk	6	Over 5,000	Insurance	Central Europe
P24	Manager in support of IT systems	14	Over 5,000	Insurance	Central Europe
P25	Chief IT officer	25	Over 7,000	University Hospital	Central Europe
P26	CISO	20	Over 3,000	Energy trading	Central Europe
P27	Lawyer	5	Over 3,000	Energy trading	Central Europe
P28	CISO	23	Over 700	Banking	Slovenia
P29	Chief Technology Auditor	20	Over 13,000	Insurance	Australia
P30	Vendor risk manager	14	Over 3,000	Tertiary education	Australia
P31	Cyber Security Consultant	31	self-employed + sub-contractors	Cyber security and assurance consulting	Australia
P32	Head of IT architecture and cyber security	15	Approx. 60	Primary and secondary education servicing over 700 schools	Australia
P33	Information Security Manager	15	About 500	Financial, legal and IT consulting	Australia

N=33	Consultants = 10 Experts/managers in organisations = 23	Organizations= 18	

Table 1: List of interview participants

3.1.2 Data analysis

The aim to develop a process theory of cyber risk assessment warranted the employment of the Straussian variant of grounded theory (Corbin & Strauss 1990; Glaser & Strauss 2017), which focuses on the interplay between data and process theory, with a more structured coding process. The key features of this approach are the detailed procedure and three steps of coding (open, axial, and selective), as well as the emphasis on context and integration with the existing literature.

Adopting the approach of Corbin and Strauss (1990), the interview data was initially analyzed using *open* coding. In addition to the codes emerging from the data, we sought to relate to concepts from the theoretical background to guide the coding process. These concepts included supplier risk factors from prior C-SCRM research, and concepts from the leading international cybersecurity frameworks (Supplement A).

Data was uploaded to NVivo. Two authors coded the interviews. The first author conducted all the interviews and coded them using the open coding method, while the second author played a supporting role in open coding and was intensively engaged in *axial* coding, in which we qualitatively and substantively compared the emerging codes, discussed and elaborated them, and organized related codes into second order codes and aggregate dimensions based on similarities, differences, and relationships between the codes (Gioia et al., 2013). This method enabled us to systematically analyze qualitative data and identify key elements of the process.

Finally, we employed a *selective* coding process in which we unified all dimensions and categories in the process of supplier cyber risk assessment with the sequence of its elements and the contextual factors impacting the process (Corbin & Strauss 1990; Mohr 1982; Markus & Robey 1988; Baskerville 2005), presented in Figure 1. We did not explicitly code against process theory. However, it broadly guided the search for the process's sequential steps, contextual factors and the identification of the risk-based principle as the form of adaptability to constrained resources. We constructed a data structure of 126 first-order codes that are grouped into 38 second-order concepts, which are further grouped into 24 aggregated dimensions on four levels to conceptualize the process of supplier cyber risk assessment. Table 2 presents the structure of the data (for the sake of brevity, we present only examples of first order codes). When constructing the process, we elevated some second order codes to higher dimensions based on the position they present in the process.

Level 1 Dimensions	Level 2 Dimensions	Level 3 Dimensions	Level 4 Dimensions	Second order codes	First order codes
Selection process	Risk identification	Identification of suppliers		Shadow IT	Open-source platforms
				Lack of central procurement	Thresholds for onboarding a supplier
	Risk analysis	Criticality of a supplier	Criticality to focal organization's process	Concentration risk	Number of suppliers of the same service
				Specificity of services/products	Provision of critical services

				Annual spending for a supplier	Percentage of revenues spent
			Data sensitivity the supplier hosts	Type of information (such as personal vs non-personal)	Personal, sensitive, non-personal
				Jurisdiction in which data is stored	Foreign or domestic jurisdiction
			IT integration	Nature of services/products or technology provided	Software-as-a-Service
		Supplier cyber risk assessment	Risk assessment methods	General due diligence	Legal, financial, operational due diligence
				Cyber security due diligence	Scanning of outward-looking technology
				Questionnaires	Self-made incorporating financial regulation
					Templates by the government/sector
					Log reviews
			Supplier cyber risk posture characteristics	Technology	Data protection (data storage management, encryption, cryptography frameworks)
				Processes	Presence of the information security role
				People	Employee security awareness program
				Regulation and industry standards	Data protection laws and regulations
				Past incidents	Occurrence of a past incident
				Complexity of supplier's supply chain	Multi-layered and complex supply chain
				Foreign operations/ ownership/location	Foreign operations
				Targeting factor	Government supply chain
				Business characteristics	Financial health
				Reputation	Customer's references
			Assurance	Requirement of reports and certifications	Pen test reports
				No validation of information	Trust in suppliers' security employees
	Evaluation	Determining supplier risk level	Acceptance of a supplier	Scoring (expert judgment, formulaic determination)	Score: low risk
			Provisional acceptance	Scoring (expert judgment, formulaic determination)	Score: high to medium risk
			Rejection of a supplier	Scoring (expert judgment, formulaic determination)	Score: high risk

Level 1 Dimensions	Level 2 Dimensions	Level 3 Dimensions	Level 4 Dimensions	Second order codes	First order codes
Monitoring after onboarding	*Risk mitigation*	Uplifting a supplier's security posture		Collaboration with a supplier to improve their cyber posture	Discussions of necessary upgrades
				Master agreements with timelines	Investments in security
				Training of supplier personnel	Cost-benefit principle

	Monitoring	Monitoring methods		Compliance with contractual requirements	Compliance with contractual requirements checked regularly
				Face-to-face meetings with a supplier	
				On-site visits	
				Obligation to report incidents and changes	Performance reviews
				Requirement of reports	Penetration tests
				Continuous monitoring with intrusive methods	Vulnerability scanning
				Shared monitoring by a consortium of organizations	Shared on-site audit of the three largest cloud providers
				Monitoring after termination of the contract	Checking for data being deleted
		Frequency of monitoring			Depends on criticality
Contextual factors				Regulation/Industry	Critical infrastructure industry
				Size	Large organizations vs SMEs
				IT Governance	Top leadership support
				Efficiency (costs vs resources)	Costs

Note: Next to the first-order codes emerging from the interviews, we also related to the concepts from the theoretical background (supplier risk factors from prior C-SCRM research, and concepts from the leading international cybersecurity frameworks). The examples of codes from the C-SCRM literature are the second order codes related to Criticality of a supplier (e.g., specificity of products/services, annual spending for the supplier) and codes related to Supplier cyber security posture (e.g., technology, people, processes, targeting factor). The codes related to leading international cybersecurity frameworks are Level 2 dimensions (Risk identification, Analysis, Evaluation, Mitigation, Monitoring).

Table 2: Data structure

3.2 Quantitative Method

3.2.1 Sample

As our secondary method, we conducted a survey (the questionnaire is provided in Supplement B). We recruited respondents with the assistance of ISACA Slovenia and ISACA Brisbane Chapter Australia, who posted invitations to participate in our research to their members. Moreover, we promoted the survey to the participants of the AusCERT conference on Gold Coast, Australia, in May 2023. We also invited individuals through our professional networks. We ended up with 71 completed questionnaires but excluded 18 because it was uncertain if they were involved in supplier cyber risk management (4 were academics and 14 were managers without specifying the area), resulting in 53 completed questionnaires. We collected responses from May 2023 till October 2023 via Qualtrics. The respondents have, on average, 23 years of experience and 11 in cyber security; their median age is in the 35-44 years category, and the average sales revenues are in the 2-10 million EUR category. They come from various countries (Australia, China, and Europe) and industries. The most frequent industries are finance and insurance (10 respondents) and IT and other information services (7).

3.2.2 Data analysis

The survey data was complementary to our interview data as the qualitative data does not allow us to analyze whether the process of supplier cyber risk assessment is effective, that is, whether it identifies risky suppliers. The small number of respondents allowed us to perform only descriptive analyses of association, such as Analysis of variance and χ^2 tests. We analysed this question by comparing the mean differences in scores on controls between suppliers that suffered an incident vs those who did not. Furthermore, we also evaluated the support of our qualitative findings (with ANOVA and correlations).

4 Process Theory of Supplier Cyber Risk Assessment

Based on our findings, we developed a process theory of supplier cyber risk assessment presented in Figure 1. The theory explains:

1. how organizations assess a supplier cyber risk, which supplier cyber risk posture characteristics are being assessed and how they are synthesized in an overall assessment of a supplier cyber risk level,
2. which contextual factors affect the maturity of cyber risk assessment and monitoring, and
3. whether the process is effective – does it identify risky suppliers?

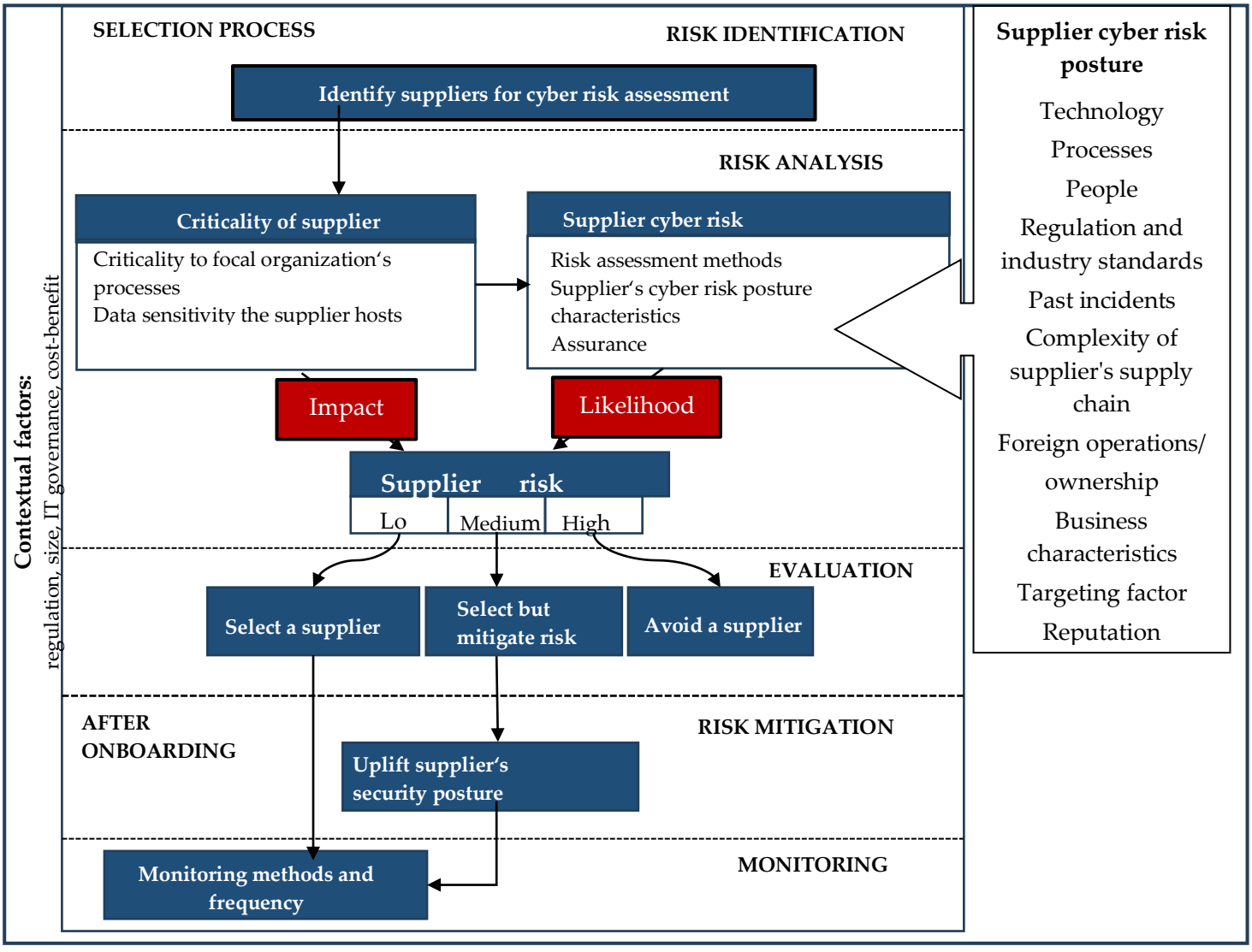

Figure 1: Process theory of supplier cyber risk assessment and monitoring.

We analyzed the first two questions using interview data (Sections 4.1.-4.3.) and the last question using survey data (Section 4.4.).

The process of supplier cyber risk assessment consists of two broad phases: cyber risk assessment (i) in the *selection process* and (ii) *after the onboarding* of a supplier.

Ad i) Supplier cyber risk assessment in the selection process starts with *comprehensively identifying suppliers*, followed by establishing a *supplier's criticality*, which then determines the scope and the depth of *supplier risk assessment*. The scope is related to the number of *assessment methods* and the number of assessed *suppliers' risk posture characteristics*. The depth is related to the *assurance* of information. This is then followed by *determining* the *supplier risk level* that leads to the decision of whether a supplier will be onboarded.

Ad ii) Cyber risk assessment after onboarding comprises *uplifting a supplier's risk posture* if a medium risk supplier was onboarded and risk *monitoring methods* after onboarding.

We then consider how this process fits to a general cyber risk assessment guided by ISO 27005 and NIST SP 800-30 and their phases of risk identification, risk analysis, evaluation, risk mitigation, and monitoring of cyber risks. In the following sections, we describe these phases in detail.

4.1 Cyber Risk Assessment in the Selection Process

4.1.1 Identification of Suppliers

One of the most challenging steps in the process of supplier cyber risk assessment is a comprehensive identification of suppliers. One challenge is the presence of shadow IT, which in the past has involved employees installing applications without the awareness of the central procurement or the IT department. Now, shadow IT has moved to cloud computing, where employees take data out of corporate applications and upload it onto free websites, like generative AI applications or cloud computing services. "*I'm aware of one organisation putting the data of 2 million Australians into some cheap Cloud Service, where some executive used a credit card doing some data analytics for $50 a month*" (P31). Mature organizations address this challenge by communicating the risk of exposing data to their employees or by blocking such actions technically.

The lack of central procurement is another problem in the identification of suppliers. Some organizations have policies in which only suppliers above certain thresholds are subject to due diligence, while those below may be onboarded by business units. Risk assessors could find out about all suppliers by obtaining information about credit card payments from the accounting department. A third problem is open-source software components, which are not even billed. *"One of the root causes developers are downloading components from other frameworks to add to their software is culture. I mean, most developers feel like they're under massive delivery time pressures*[2]*. So, it's better to borrow another component from somewhere else"* (P31). Requiring a software bill of materials, as mandated by the US Federal Government for software provided to the federal government (Biden's Executive Order on Improving the Nation's Cybersecurity, EO 14028, 2021), would contribute to the identification of all software components. However, we have not observed this practice in the organizations we analyzed.

[2] More about the impact of time pressure on cybersecurity behaviours in Chowdhury et al. (2019).

4.1.2 Criticality

Once suppliers are identified, organizations assess their criticality by considering the following three factors: (i) *the criticality of a supplier to the focal organization's business processes*, defined by the concentration risk (number of suppliers of the same service that an organization relies on), specificity of services/products, and annual spending for a certain supplier; (ii) *the data sensitivity the supplier hosts or has access to* (type of data, management of data in its entire life-cycle, jurisdiction in which the data is stored); and (iii) *IT integration,* which is associated with the nature of services, product and/or technology provided by a supplier, such as Software-as-a-service (SaaS), Infrastructure-as-a-service (IaaS), or Platform-as-a-service (PaaS). In the EU banking sector, prudential regulation (the European Banking Authority) mandates a clear distinction between regular and critically important suppliers, with an assessment process that matches the level of criticality. Consequently, banks follow the most rigorous processes of supplier criticality classification, formally linking it to Business Impact Analysis. Organisations generally rate suppliers using qualitative scores for criticality, such as critical, high, medium, and low. However, not all organizations have a defined process and key risk indicators in place and determine supplier criticality by a rule of thumb.

Organizations tend not to spend resources on suppliers of low criticality; our interviewees suggest that in some organizations, they are entirely left out of cyber risk assessment. The size of a prospective supplier is also considered – if it is small and does not have many resources and dedicated security staff, it won't be able to complete an in-depth risk assessment process.

4.1.3 Risk assessment methods

Our findings suggest that organizations primarily assess suppliers via three methods undertaken in different sequences by different organizations. Not all organizations rely on all methods and the extent to which each method is applied varies based on the supplier's criticality.

General due diligence checks a supplier's financial, operational and strategic risks, such as legal, geopolitical, environmental, social, and governance risks, the quality of service, and the supply chain complexity. This information is sought from a supplier or is based on its annual reports and public information. It is carried out by various organizational units (e.g., strategic procurement, risk management, legal or compliance department). *"If an organization is financially non-viable, or non-viable in any other respect, it does not even get to be assessed for cyber risks but is rejected immediately"* (P26). Internal auditors might also be involved at this stage; however, mostly to ensure that in the focal organisation *"all the right risk people or legal and compliance people have been involved and done their sign-offs … We review risk artefacts before they sign the contract. From our point of view, it doesn't make sense to review things after the arrangement has been done because then you can't change the contract."* (P29).

A second method is cyber security due diligence based on public information about cyber risks. Organizations double-check in the registers whether suppliers have security certifications. They rely on threat intelligence, providing information about past incidents and the activity on the dark web related to a prospective supplier, and scan the supplier's outward-looking technology. Some interviewed organizations (belonging to critical infrastructure) have the capability of a cloud access security broker (CASB) or rely on a third-party provider: "We use public information prior to onboarding and after onboarding. The simplest procedure for that is Qualys - scanning of their vulnerabilities based on public

information. We analyze a partner's cyber posture - viruses, vulnerabilities, protocols that are public, everything that is possible to get publicly about the partner" (P20).

The third method is to collect information via questionnaires, which cover a wide range of questions (from roughly 8 to 150) about supplier characteristics. Questionnaires are subdivided into the assessment of the common core of controls, relevant for all suppliers, and supplements that depend on the service provided or supplier criticality. "For software companies, our questionnaire comprises 119 questions, for others only 8." (P11). They are either self-made, based on guidelines, open-source standards, and regulation, imposed by a parent company; or provided, for example, by a government (e.g., Australian Signals Directorate). While there might be a considerable variation in suppliers' maturity of certain controls, the variation is not captured in most organisations as the checklists provide only yes or no answers. Only the most mature organizations rely on a maturity scale for each question (among our interviewees, those were the banks).

Some organizations integrate questionnaires into a vendor management platform or rely on a specialized third-party provider. These providers possess the expertise and capability to perform the assessment more effectively than if an organization performs it in-house. The advantage is that third-party providers collect large amounts of information about organizations via online questionnaires, which they supplement with public information and information on past incidents, based on which they develop quantitative scores or even prediction models of a cyber incident. The second advantage is that they can also provide basic risk information for the suppliers beyond Tier 1 (suppliers of suppliers).

4.1.4 Supplier cyber security posture characteristics

In assessing the supplier's cyber security posture, our interviewees suggested that *Technology* is a key characteristic of a supplier's cyber security posture. Technology questions cover all main controls related to protection, detection, response and recovery (the most important controls relate to data management, authentication and encryption methods, and identity and access management). However, the technological requirements and their checking widely differed among organizations and across suppliers: while some stated that technological requirements could not be too high, as they could then not find any supplier in a country, others were frustrated because they were unable to check the libraries within the software. Most organizations impose mandatory requirements that would be a deal-breaker if a prospective supplier does not have them (e.g., a single sign-on).

The importance of processes and people has also been stressed: *"I'm less interested in the presence of controls than in the presence of an operating security function that selects controls that work."* (P21). Regarding Processes, focal organizations are looking for the presence of the information security role, whether suppliers adhere to any risk management framework, have privacy policies and documented processes, such as incident response and business continuity plans and how they would notify their partner about an incident or changes. P12 stressed that *"most incidents in vendors are not related to malicious activity; it's a failure of technology that occurs from an error. Then continuity becomes very important."*

Regarding *People*, organizations look at suppliers' attitudes towards protecting information, security awareness programs for their employees, and whether they perform vetting of employees involved in cyber security management. Interviewees raised a concern that most companies fail to check their employees and provide security awareness programs only for

their IT staff. In some cases, focal organizations check suppliers' employees' and senior management's background to verify their security qualifications and trustworthiness.

Regulatory requirements and industry standards are other critical factors determining supplier security posture. *"Many of our key suppliers are also captured by the critical infrastructure legislation. That creates a great deal of certainty. They need to produce a very detailed critical infrastructure management plan."* (P6). If a supplier is subject to privacy laws and the payment card industry standards and is from the critical industry, the regulation provides a sense of security to a focal organization.

Our respondents also acquire information about *past incidents* but have contrasting opinions about whether past incidents indicate future incidents or the lesser likelihood of another incident because a supplier has learnt the lesson (unless it had multiple breaches).

The *complexity of a supplier's supply chain* is another cyber risk posture characteristic, challenging to assess and manage. Only one of our interviewees mentioned having engaged in the investigation beyond Tier 1 suppliers: "*I found that behind that third party provider, there are 12 other companies who manage the data of this company across New Zealand, the US, Australia, and the Netherlands. It is not a supply chain; it is a multi-layer business network; one company provides infrastructure, other companies provide solutions, third companies provide hardware, and fourth companies try to manage it."* (P10). Other interviewees indicated that while they are aware of their suppliers' subcontractors, they do not assess their cyber security. Only if it comes to an incident, meaning that a subcontractor breaches the focal organization's security requirements, the latter might request an on-site visit of the subcontractor. However, some vendor risk management platforms provide the basic risk scores of suppliers' subcontractors, limited to the risks related to their outward-looking technology.

Foreign *ownership/operations/influence* are also a risk as countries have varying laws and regulations regarding data privacy, surveillance, and information control. Some governments may impose strict regulations requiring companies to provide access to their data or compel them to store it within the country's borders.

The supplier's *targeting factor* depends primarily on its industry (e.g., critical infrastructure, financial, ICT) and whether it is a government SC. *The business characteristics* of suppliers, such as financial health, size, age, and market share, were also suggested as important as if they are financially vulnerable and unstable, they can become vulnerable to a cyberattack. Lastly, organizations assess the *supplier's reputation* and customers' and partners' references.

4.1.5 Assurance

Whether organizations require any assurance concerning the information provided depends on the supplier's criticality. "It depends on the perceived risk how many assurance activities make sense or are economically viable. If there's no personal information involved, well, I'll treat that differently than when half a million personal information records are at risk. I'm gonna have stronger assurance built into the contract for the second one and might not need any for the first one." (P21). Only for critical suppliers, the interviewees require audit reports, pen tests, and/or cyber security certifications. However, not much detail might be disclosed to prospective customers: "In pen test reports, they will only give you the cover page which addresses any risks that were identified and how they were mitigated" (P30). Also, the ISO 27001 certification is a one pager that provides the focal organization only with proof that a prospective supplier meets the standard without any details. Only the SOC 2 report by the

American Institute of Certified Public Accountants offers a detailed and comprehensive assessment of the effectiveness of controls. However, reports older than a year are already considered outdated. Some organizations even have to verify that audits have been conducted by certified auditors.

However, in most cases, organizations do not rely on validation, especially for SMEs and non-critical suppliers. They count on the supplier's transparency and willingness to share information and evaluate the information's credibility via partners' references. Most respondents stressed the importance of trust. However, several respondents shared that they caught a supplier lying about their cybersecurity certification: "I actually searched the ISO 27001 database of certificates to see if I could find this certificate (of a supplier), and I couldn't. There is a lot of trust in that process, and there have been times when I've wanted to clarify their response to something, and they had said, oh, that was a mistake" (P11).

4.1.6 Determining supplier cyber risk level

The diverse information from the extensive questionnaire and a due diligence report is rather difficult to synthesize in an overall supplier's risk level. Organizations juxtapose the information acquired from the supplier with that from public sources and threat intelligence for consistency. Ideally and in line with ISO 27005, organizations would first evaluate a supplier's criticality to adopt the proper scope and depth of the assessment process. Criticality is associated with the *impact* of a cyber incident related to a supplier. In the second step, the organization would evaluate the *likelihood* of a supplier having a cyber incident based on its assessed risk posture. However, in practice, most organizations do not separately assess the impact and the likelihood but come up with an overall supplier's risk level, which is determined as a subjective summary of numerous pieces of information, often qualitative and defined on a high, medium, and low scale. *"How critical a certain supplier is a matter of the management subjective judgment in relation to which controls are missing and what is the relationship with a particular supplier" (P19).*

Just one organization stated that it derives the risk level in a formulaic manner (taking a simple non-weighted average of the assessed characteristics). Organizations that use vendor management platforms receive quantitative risk scores, yet there is limited explainability about how the scores are calculated.

Based on the assessed cyber risk level, the assessors (security experts) suggest to decision-makers (executive managers) whether to accept a particular supplier. If the risk level is low, then a supplier is offered a contract specifying detailed cyber security requirements by the focal organizations. However, if the assessment indicates a medium risk level, most organizations do not outright reject a supplier but use the information as a snapshot of the supplier's (missing) controls. They engage with a supplier to discuss further how to uplift its security posture. If the cyber risk level score indicates high risk, the assessors suggest rejecting the supplier to the management. However, they might not always be listened to.

4.2 Monitoring after Onboarding

4.2.1 Uplifting a supplier's security posture

Often, when a supplier is important to an organization on business grounds but does not have all the security requirements in place, focal organizations engage in uplifting a supplier's cyber security posture. Also, focal organizations have more tolerance if suppliers are not involved in critical processes. They tend to onboard such a supplier but impose requirements

to implement missing controls in the master agreement with a specific timeline and a roadmap. They also provide support such as joint vulnerability assessment. *"If someone is poorly assessed, it affects the overall risk assessment. If they are below our risk acceptance, they are contacted and looked at to see if there are any minor deficiencies, given a deadline for correction, and move on with the process"* (P20).

Assisting suppliers in safeguarding the focal organization's information can be mutually beneficial, as the expenses associated with remediation after a breach and the potential lack of resilience would likely surpass the costs of aiding a supplier in addressing any shortcomings. The focal organization and suppliers might also find it advantageous to collaborate on investments in staff training (Davis, 2015; Vanajakumari et al., 2021).

4.2.2 Monitoring methods and frequency

Organizations should continuously or periodically monitor their suppliers' security posture to overcome the relatively static nature of risk assessment and ensure suppliers remain in line with their security requirements (Davis, 2015). Monitoring can be periodic (annual, biannual or triannual), at the renewal of the contract, or based on a trigger, depending on the supplier's criticality and the method of monitoring.

Our findings suggest a significant variation in the maturity of monitoring. For critical suppliers, organizations periodically check compliance with the contract, conduct face-to-face meetings, or require audit reports or pen tests. For non-critical suppliers, performance review and security requirements are mostly checked only at the renewal of the contract. The largest organisations are only just starting to invoke the right to audit. Only the most mature organizations monitor critical suppliers continuously by integrating threat intelligence with the focal organization's Security Information and Event Management System (SIEM). Intrusive methods require direct contact with the supplier's network and include network vulnerability scanning, log reviews, and prediction of cyber threats by machine learning methods (Keskin et al., 2021; Al-Ansari & Asubait, 2022). *"So, we have threat management for our organization, we use the platform [name of the platform], and we wanna use the same kind of technology to keep an eye out for alerts when a hack happens in one of our vendors"* (P33). The costs and the level of expertise associated with conducting these assessments are considerable.

Interestingly, nobody (but German banks) monitors the leading cloud providers because of the power imbalance between cloud providers such as Microsoft, AWS, and Google vs. focal organizations. However, the Chief IT auditor of a German bank explained that the bank, in a consortium with other banks, conducts on-site audits of these systemically important cloud providers as this is required by German prudential regulation. *"We are not competitors, and you also gain more power in the team. It includes the biggest German banks, the biggest insurance companies, and also, I think, the biggest Italian banks."* (P13). Other organizations mostly rely on public information and certifications about the largest cloud providers[3].

We came across some organizations that have a solid risk assessment process before onboarding but do not monitor a supplier after onboarding. *"We're typically relying a lot more on the assessment than the actual contractual obligations at the moment. No follow-up of vendors later. We are developing a new policy here for vendors having protected data."* (P14). In contrast, other

[3] The EU DORA regulation stipulates that such providers will be monitored by the financial regulator itself because of their systemic importance.

organizations have integrated their existing suppliers on their vulnerability scanning platform and conduct continuous monitoring but do not have a mature risk assessment process for suppliers before onboarding.

The greatest challenge is ensuring that a supplier deletes the data as agreed and monitoring the deletion after the contract is terminated, especially in jurisdictions without regulations as strict as GDPR: *"We are an organization highly dependent on third party providers. The first thing is really about getting breached by third parties, and the second risk, in my view, is about the fact that they keep our data for longer than we have agreed to beforehand. It's difficult to keep that overview unless you actually go to their organization and do an internal test whether they still have our data"* (P33).

4.3 Contextual Factors

The best way to understand how the process of supplier risk assessment is applied in organizations is by considering its maturity. Boyson (2014) defines the maturity of C-SCRM as *emergent,* that is, where no systematic risk assessment activities and no risk monitoring or digital forensics and reporting capacity take place, *diligent,* when organizations engage in selected risk assessment activities across the enterprise but have a limited capacity of risk monitoring, and *proficient* for extensive supply chain-wide risk assessment activities involving suppliers and customers and extensive capacity of monitoring. While we do not intend to classify our 18 organizations into specific maturity levels based on interviews, we have observed significant variation in the maturity of supplier cyber risk assessments along these levels – that is, which steps of the assessment they apply and how thorough they are. The variation is influenced by several contextual factors - characteristics of the focal organization.

One of our participating organizations stands out, and that is the German bank. The two contextual factors that differentiate the German bank from all other participating organizations are a combination of *size* and *regulation*, specifically, German prudential banking regulation. *"We are doing on-site audits for all material partners. We do not rely on reports. I read the report before I start to understand the partner, but I also take my own sample testing, and I want to have a look at the whole documentation by myself and normally on-site."* (P13).

Both factors have implications for an organization's risk culture and appetite (Gale *et al.*, 2022; Monev, 2021), which in turn affect financial resources dedicated to C-SCRM and the attraction of talent. Larger organizations have a larger and more complex SC and are more exposed to cyber risk from the SC. Correspondingly, they have a broader scope of assessment and assess more than just critical suppliers. In the financial industry, classification of suppliers, risk assessment and monitoring are subject to prudential oversight (e.g., EBA Guidelines on outsourcing arrangements, 2019). The EBA guidelines, for example, require a manager managing outsourced arrangements to be in a senior management position, which significantly elevates the importance of this area and allocated resources. Furthermore, the EU prudential requirements for the financial industry are considerably increasing (DORA, 2023[4]), and the affected participants stressed that they are already upscaling their capabilities to become compliant.

[4] DORA requires more validation checks, and stipulates the Lead overseer over the critical ICT service providers being one of the three EU financial authorities.

However, in the case of the German bank, the crucial determinant of its proficiency is the *pooling of resources* within the industry. Given the complexity of SC, the nature of various risks from suppliers (not just cyber but also, for example, geopolitical and ESG risks) and the sheer size of cloud providers, pooling resources seems to be the most effective way to share not only costs of expensive risk assessment but also expertise and information. *"We audit Google, Microsoft and AWS every year in a team from Europe with financial institutions and insurance companies, because they are under the same regulator, and we are visiting the big three American companies together. It's normally a lot of fun. It's 20 auditors."* (P13)

Regulation (e.g., Security of Critical Infrastructure 2018 in Australia, the Network and Information System Directive 2022 in the EU) has also resulted in a typically higher maturity of the critical infrastructure, such as IT, transport, energy, and healthcare, compared to other non-critical industries. While security is a top priority in the provision of critical services, in other industries, some interviewees acknowledged that cyber security is not the decisive factor in the selection of a supplier, but the price of a service or a product, even if such a cheaper supplier is more likely to pose a higher cyber risk. This is especially problematic in the public sector, where even if an organization belongs to critical infrastructure (in this study, a public hospital), it is subject to public tender legislation, which emphasizes the price and quality of service/product above other supplier selection criteria.

While each contextual factor has an independent effect on the process, their interaction may boost (size and regulation) or downplay (critical infrastructure subject to public procurement legislation) the maturity of the process. Regulated and large organizations dedicate more resources to *IT governance*, characterized by strong top leadership support, clearly defined responsibilities, high hierarchical position of IT and security roles, and experienced and knowledgeable security staff in charge of C-SCRM. Their agency leads to the continuous development of risk assessment and monitoring methods. One such good example of cyber security experts' agency is a national approach to safer technologies in schools and pooling of resources in primary and secondary education in Australia, where hundreds of state and territory schools rely on a common third-party risk management program completed by prospective vendors once and for all. This minimizes the duplication of work on both sides. Merely participating in this program and completing the questionnaires provides security enhancement opportunities for both schools and vendors. For schools, it includes agreeing on a common set of privacy criteria and managing resources efficiently. Vendors want to 'look good' as it opens up the market (P32).

In many organizations, security roles have only recently been set up, and the supplier cyber risk process has yet to be fully established. The demand for experts exceeds the supply. Organizations are also affected by significant fluctuations of experts, which can, on the one hand, have a positive effect via the mimicry of best practices but also a negative impact because of less-than-perfect transfer of knowledge.

Lastly, *efficiency* (the cost-benefit analysis) is the ultimate determinant of the maturity of the assessment process. Our findings indicate that while the security experts are familiar with best practices and cyber security standards, the challenge is to comply with them due to constrained resources. A massive retail organization may have 10,000 suppliers subject to assessment and monitoring, requiring mammoth resources. Allocation of resources to this area is proportionate to the perception of cyber risk exposure and the benefits of managing cyber risk. If cyber incidents from the SC have never been experienced and are perceived as

highly uncertain and out of control, the benefits of allocating resources may also seem somewhat uncertain. In multi-billion dollar organizations, there are usually not more than one to three persons involved in assessments. Although our interviewees demonstrated awareness of risks and how to manage them, they also expressed frustration with the extensive scope and risks' uncontrollability.

4.4 Effectiveness of the Assessment Process in Identifying Risky Suppliers

In this section, we present the survey findings. Before presenting the findings about the effectiveness of the process in identifying risky suppliers, we triangulate the interview findings with those from the survey. We tested whether supplier criticality dictates the scope of the assessment process with the correlation analysis between criticality and the number of controls assessing supplier characteristics related to Technology, People, Processes and General information (see Table 3). We find that if a supplier is critical to the focal organization's operations, a significantly higher number of supplier controls is assessed related to Technology and Processes (but not to People and General information). However, we did not find support that suppliers with access to sensitive data are more scrutinized, partly perhaps because of the correlation between the involvement of a supplier in critical processes and their access to sensitive information.

	Data sensitivity a supplier has access to	Criticality of processes a supplier is involved in
Data sensitivity a supplier has access to	1	.391**
Criticality of processes a supplier is involved in	.391**	1
Number of supplier's controls assessed (Total)	0.177	.360**
N of supplier's technology controls assessed	0.143	.364**
N of supplier's processes controls assessed	0.206	.326*
N of supplier's people controls assessed	0.099	0.251
N of supplier's general information categories assessed	-0.124	0.047

Note: ** $p < 0.01$ (2-tailed), * $p < 0.05$ level (2-tailed).

Table 3: Correlations between supplier's criticality and the scope of risk assessment (the number of assessed controls)

Regarding the contextual factors, we do not find the *size* of the focal organization to be associated with the assessment scope. Concerning *IT governance*, if an organization has a cyber expert who assesses supplier cyber risk, then this is associated with a broader scope of assessment of supplier's processes. However, we do not find the scope to differ for other areas. Interestingly, we find that those organizations that use some sort of vendor management software assess fewer controls for Technology and People but not for Processes and General information. It might be that these platforms monitor other controls than those assessed in our questionnaire (they focus on outward-looking websites). Among *industries*, organizations from the Financial and ICT industries were found to assess a significantly larger number of controls in all areas except for Processes (Table 4). The size of our sample and the nature of the variables did not allow us to assess a causality model and interactions among the contextual variables; however, the results, by and large, support the interview findings, except for size.

	Cyber expert who assesses supplier cyber risk	N	Mean	Std. Dev	SE Mean	Vendor management software	N	Mean	Std. Dev	SE Mean	Fin/ ICT sector	N	Mean	Std. Dev	SE Mean
Supplier's characteristics Total (N of controls =29)	Yes	37	25.5	5.00	0.82	Yes	31	24.3**	6.13	1.10	Yes	17	27.1**	3.02	0.73
	No	13	23.4	5.95	1.65	No	21	26.6**	2.93	0.64	No	36	24.1**	5.71	0.95
Supplier's Technology	Yes	37	11.3	3.64	0.60	Yes	31	10.5**	4.49	0.81	Yes	17	12.4**	1.97	0.48
(N of controls =13)	No	13	10.2	4.26	1.18	No	21	12.2**	1.70	0.37	No	36	10.5**	4.20	0.70
Supplier's Processes	Yes	37	2.9**	1.40	0.23	Yes	31	2.6**	0.56	0.10	Yes	17	3.2	1.29	0.31
(N of controls=4)	No	13	2**	1.68	0.47	No	21	2.8**	0.40	0.09	No	36	2.5	1.56	0.26
Supplier's People	Yes	37	2.7	0.52	0.09	Yes	31	2.6	1.59	0.29	Yes	17	2.8*	0.39	0.10
(N of controls=3)	No	13	2.6	0.51	0.14	No	21	2.9	1.39	0.30	No	36	2.6*	0.55	0.09
Supplier's General information	Yes	37	8.6	0.76	0.12	Yes	31	8.6	0.56	0.10	Yes	17	8.8*	0.44	0.11
(N of controls=9)	No	13	8.6	0.65	0.18	No	21	8.7	0.80	0.17	No	36	8.5*	0.85	0.14

Note: We used Analysis of Variance (ANOVA) to analyze whether the fact that an organization employs a specific expert for assessments of supplier cyber risk, uses vendor management software, and is from the financial or ICT sector, affects the number of controls assessed (the scope of the assessment). The number of controls in the brackets for each area indicates the maximum number of controls considered in this study for that specific area, and bolded Means with asterisks indicate which areas significantly differ between the two groups. ** $p < 0.01$ (2-tailed), * $p < 0.05$ level (2-tailed).

Table 4: ANOVA analysis of the scope of assessment

To analyze whether the risk assessment process can effectively identify risky suppliers we compared the assessed quality of controls between the suppliers that suffered a cyber incident and those that didn't. The analysis is presented in Tables 5 and 6. On eight out of 13 Technology controls, suppliers without an incident scored significantly better than suppliers with an incident. This supports the interview findings that the assessment of Technology is the most important area for understanding supplier cyber security posture and that weaknesses can be identified in a thorough assessment process.

Suppliers who haven't experienced an incident were also better assessed on management attitudes towards protecting information (People), transparency and reputation (General information). In contrast to the interview findings, Process controls were not significantly different. The descriptive statistics indicate that processes were perceived as well-established also for suppliers that had an incident. The survey also showed threat intelligence is paramount, as red flags were provided significantly more often for suppliers that suffered an incident than for those who did not (24% vs 3.6%). Another noteworthy finding is that in our more detailed analysis (for brevity, not tabulated), those suppliers that the focal organization classified as less critical reported a cyber incident more frequently than those that were classified as more critical, but there was no difference in the number of incidents between suppliers that had access to sensitive data and those that do not. This suggests that contrary to current practices, organizations might need to pay more attention to suppliers that are classified as less critical, as they might be a weak point of access. Overall, the findings from the survey suggest that the process of supplier cyber risk assessment can be effective in identifying risky suppliers.

Supplier controls	Incident	N	Mean	Std. Deviation	Std. Error Mean
Technology (1 Min - 4 Max)					
Commitment to secure-by-design practices	Yes	21	2.48	.981	.214
	No	24	2.88	1.116	.228
Use of secure coding practices	Yes	21	2.29*	1.007	.220
	No	24	2.71*	1.042	.213
Delivery of secure-by-default products and services	Yes	20	2.30	1.031	.231
	No	24	2.54	1.215	.248
Commitment to maintaining the security of their products and services	Yes	22	2.50	1.012	.216
	No	25	2.76	1.052	.210
Vulnerability disclosure policy	Yes	18	2.28	1.179	.278
	No	25	2.72	1.173	.235
Protected third-party access	Yes	18	2.22*	1.114	.263
	No	25	2.76*	1.091	.218
Use of encryption and cryptography	Yes	22	2.18**	1.053	.224
	No	25	3.08**	.954	.191
Updated and patched software and servers	Yes	21	2.33**	1.017	.222
	No	25	3.04**	1.060	.212
Strong password systems supported with MFA	Yes	20	2.35*	1.226	.274
	No	26	2.85*	1.084	.213
Secure configuration of tools and firewalls	Yes	21	2.24**	1.091	.238
	No	26	2.88**	.993	.195
Detection systems	Yes	21	2.29*	1.056	.230
	No	26	2.81*	1.167	.229
Physical security controls	Yes	22	2.41*	1.221	.260
	No	25	2.88*	1.092	.218
People (1 Min - 5 Max)					

How thoroughly does your chosen supplier perform employee background checks for those involved in cyber risk management	Yes	24	3.13	.900	.184
	No	28	3.07	1.152	.218
How would you rate your chosen supplier's management attitudes towards the protection of information	Yes	25	2.56**	1.325	.265
	No	28	3.18**	1.188	.225
General information (1 Min - 5 Max)					
How complex is your supplier's supply chain?	Yes	25	3.00	1.041	.208
	No	28	2.79	1.134	.214
How likely is your selected supplier subject to foreign ownership, operations or control?	Yes	25	2.72	1.242	.248
	No	28	2.75	1.266	.239
How attractive is your chosen supplier as a target for cyber incidents?	Yes	25	3.60	1.000	.200
	No	28	3.57	1.103	.208
What is your chosen supplier's financial health?	Yes	25	3.96	.978	.196
	No	28	4.25	.967	.183
What is your chosen supplier's market share?	Yes	25	3.00	.816	.163
	No	28	3.04	.922	.174
What is your chosen supplier's age? (1 Min – 4 Max)	Yes	23	2.87*	.344	.072
	No	26	2.65*	.562	.110
What is your chosen supplier's size? (1 Min – 4 Max)	Yes	22	2.64*	.727	.155
	No	27	2.33*	.832	.160
How would you assess your chosen supplier customers' references and reputation?	Yes	24	3.46*	1.062	.217
	No	27	3.85*	.949	.183
How would you assess the quality of information and transparency of your chosen supplier with regard to its cyber security risk management?	Yes	25	2.56**	1.083	.217
	No	28	3.46**	.838	.158
What kind of assurance does your chosen supplier provide with regard to its cyber security (e.g. penetration tests, assurance conducted by a third party, audit reports)?	Yes	18	3.33	1.283	.302
	No	23	3.78	1.242	.259

Note: Variance analysis of supplier's controls based on the notification that a supplier had an incident in the past 12 months (those suppliers are in the Incident Yes group, and those without an incident are in the Incident No group). * $p < 0.1$, ** $p < 0.05$ (two-tailed)

Table 5: Variance analysis of supplier's controls based on received notification that a supplier had an incident in the past 12 months

Supplier controls (Yes/No questions)	Incident	Frequency	Chi-square
Technology			
Vulnerability and penetration testing performed	Yes	52.4%	
	No	60.0%	0.241
Processes			
Documented incident response plan	Yes	75.0%	
	No	94.1%	2.343
Documented business continuity plan	Yes	82.4%	
	No	83.3%	0.006
Information security role in place	Yes	88.2%	
	No	85.0%	0.082
Security policies, frameworks, and documents	Yes	100.0%	
	No	86.4%	2.511
People			

Security awareness program for employees	Yes	93.8%	
	No	85.7%	0.608
General			
Red flags by threat intelligence	Yes	24%**	
	No	3.6%**	4.8

Note: We used the cross-tabulation analysis and chi-square estimator to assess whether the frequency of controls in suppliers without an incident significantly differs (Incident No group) from those in suppliers who suffered an incident (Incident Yes group). ** $p < 0.05$ (two-tailed)

Table 6: Cross-tabulation analysis of supplier's characteristics based on received notification that a supplier had an incident in the past 12 months

5 Discussion

5.1 Theoretical Contributions

Cyber security management studies are generally based on variance theories that suggest a determinate relationship between cause and effect; that is, more controls invariably lead to smaller cyber risks whereby the risks can be measured (Baskerville, 2005). However, given the high unpredictability and uncontrollability of supplier cyber risks and challenges of its measurement, in formulating the process theory of supplier cyber risk, we rely on a different logical structure – that of life-cycle process theories, which propose that the outcome (in our case, the mitigation of supplier cyber risk) is contingent on a *sequence of steps* rather than on an expected relationship between the controls and the risk (Mohr, 1982; Markus & Robey, 1988, van de Ven & Poole, 1995; Baskerville, 2005). Hence, if some steps in the process are missed, a risky supplier will not be identified. The process theories, however, do not suggest that the outcome is guaranteed: it might happen under certain conditions but not necessarily (Markus & Robey, 1988; p. 591). We identify the elements (steps) of the process of supplier cyber risk assessment and their sequential logic and study how one phase influences the next (Figure 1). Our quantitative findings support that the appropriate elements of the process were derived during the qualitative analysis and that assessing these elements would likely help an organization identify a risky supplier.

In addition to identifying the sequential steps of the process, the teleological process theory adds the perspective that resource limitations and organizational environment constrain organizations in what can be accomplished (van de Ven & Poole, 1995). We considered this perspective when analyzing how contextual factors affect the maturity of the process. Adapting the process's scope and depth to supplier *criticality* demonstrates that organizations optimize their resources by following a *risk-based principle*, which focuses on identifying and mitigating the most pertinent risks first (Lin & Saebeler, 2019; Pollmeier et al. 2022). For example, organizations with massive numbers of suppliers can only focus on critical suppliers, leaving many non-critical ones unassessed and non-monitored. "*You can have hundreds of questionnaires, and you do not have resources to analyze those questionnaires; they are in Excel or Word documents. The first party reads it at a point in time, and then it gets it stored, but then it is never looked at again.*" (P18). The *adaptability* of the process (to constraint resources) is a fundamental principle of teleological process theory (van de Ven & Poole, 1995; Bekmeier-Feuerhahn, 2009). We find that organizations that are more exposed to cyber risk and are larger have more resources and expand their assessment beyond just critical suppliers. They automate the process after a supplier is onboarded, invest more resources in ensuring that supplier

information remains accurate and that a supplier maintains its security posture even after onboarding.

Compared to the findings of prior research (e.g., Gaudenzi & Siciliano, 2018; Colicchia *et al.*, 2019; Boyens *et al.*, 2020) who found that the majority of C-SCRM initiatives are primarily associated with the IT domain (technology) and that organizations are prioritizing protection measures over cyber risk assessment, we found that in the recent years, this process has rapidly progressed. Still, most interviewees concur that their supplier risk assessment and monitoring process is a 'work in progress'. While prior studies interpret the assessment of the suppliers' IT domain (technology) as early stages of maturity, we observe that most organizations have expanded beyond merely assessing this area. However, we also find that technology remains the most critical characteristic of the supplier's risk posture. A significant share of organizations is only at the low maturity of the described process – many have just started to assess the cyber risk of suppliers in the selection process but are struggling to catch up with monitoring hundreds or thousands of existing suppliers.

Some organizations rely on reduced assessment due to resource constraints, while in others, the assessment is lax as the assessment outcome is not decisive for the decision to onboard a supplier due to the lack of management support, which considers other factors more important. In sum, organizations repetitively review their achievable goals and strive to advance and modify their assessment processes in accordance with teleological process theory (van de Ven & Poole, 1995).

By proposing a process theory of supplier cyber risk assessment, this study makes a theoretical contribution to the existing research on C-SCRM by utilizing a perspective that hasn't been researched in previous studies that focused predominantly on normative guidance, technical solutions, or described practices in selected case studies. The fundamental theoretical contribution is the integration of life-cycle and teleological process theories in the context of C-SCRM. Dictated by constrained resources, this integration is achieved by focusing on suppliers' criticality and applying sequential steps in a risk-based manner.

5.2 Practical Contributions

From our findings, significant practical implications arise. First, the most important concern is the lack of resources dedicated to supplier cyber risk assessment. Pooling resources with other organizations using the same suppliers for cyber risk assessments and other operational and strategic risk assessments in the SC (e.g., ESG) would be one way to optimize the available resources. Another solution could be using vendor management platforms (Keskin et al., 2021) and automation tools for monitoring onboarded suppliers. However, vendor management platforms should not operate as a black box – the scores need to be understood and aligned with other cyber risks related assessments if they are to affect business decisions. Third, in most of the interviewed organizations, despite reliance on various methods and tools, translating a supplier's information into risk score is a *subjective* expert judgment. The objectivity of assessments could improve if organizations started building a database of suppliers' characteristics that would enable benchmarking and validation of the assessment methods by analyzing *ex-post* whether suppliers assessed with a higher/lower risk score were actually more/less risky.

Fourth, the likelihood of a supplier suffering a cyber incident and the likelihood that this incident would affect the focal organization are not perfectly correlated. The latter depends on

the failure of other controls in the focal organization and what processes a supplier is involved in. This calls for better integration of supplier cyber risk assessment with the overall cyber risk assessment process in the focal organization in the light of ISO/IEC 27005 or NIST Special Publication 800-30 (Monev, 2021). Our model in Figure 1 illustrates how different steps in the supplier cyber risk assessment process can be integrated with the steps laid out in ISO/IEC 27005 or NIST SP 800-30 for organizational cyber risk assessment – risk assessment (identification, analysis, evaluation), risk mitigation and monitoring.

Fifth, currently, international cybersecurity certifications are not fit for purpose for SMEs, and the assessments are tailored towards the ICT technology providers. To get visibility across the entire SC, as suggested by one of our interviewees (P15), organizations could consider making suppliers accountable for their cyber security by getting self-attestation and acquiring a multi-tiered cybersecurity certification. Instead of each organization assessing the risk, providing SMEs with the standards they can attest to would shift the accountability for cyber security to suppliers. Currently, self-attestation services are only just developing. If such optimizations do not occur, a threat exists that the regulated industries subject to stringent assessment requirements will not be able to engage small and micro suppliers, who are unable to adhere to ever-increasing requirements. Such an approach would provide better protection to a focal organization which could adopt a policy that all suppliers in its SC need some sort of certification, be it ISO for the critical suppliers or anything else at some minimum level (P15: *"black, brown and white belts, in the parlance of karate"*). Sixth, outsourcing cyber risk assessment would be another move towards optimizing resources and increasing the effectiveness of assessments.

5.3 Limitations

Our findings are subject to some limitations: despite investing a great effort in attracting participants to the survey, we ended up with only 53 usable observations – some being excluded due to non-suitability. This has severely limited our analyses and the generalizability of the results. Because of the niche expertise needed to participate in the study and the young phenomenon under investigation, the participants who were prepared to participate might have come from more mature organizations, and this relates to both survey and interview participants who were mostly from large, regulated, and resourceful organizations or consultants. The findings can thus not be generalized: while our participants already acknowledged the early stage of the development of the process, the findings might, in fact, show a better picture than it is on average. However, despite the limitations in data collection, we followed rigorous research methods to analyze the findings.

6 Conclusion

C-SCRM and supplier cyber risk assessment offer ample opportunities for future research. Qualitative and quantitative analyses could further examine the process and its determinants for the optimal development of cyber risk assessment given the context of an organization. A couple of ideas for future research are to validate the process framework and its contextual variables on a large sample, to further explore the role of Processes and People characteristics, how they could be defined and measured to better differentiate between risky and less risky suppliers; to assess a predictive model of a supplier cyber risk; or to study the role and importance of supplier cyber risk assessment in the overall supplier assessment.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review, 5*(5), 5–14. doi.org/10.22215/timreview/861

Akinrolabu, O., Nurse, J., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security, 87.* doi.org/10.1016/j.cose.2019.101600

Al-Ansari, A. O., & Alsubait, T. M. (2022). Predicting cyber threats using machine learning for improving cyber supply chain security. In *2022 National Computing Colleges Conference (NCCC)* (pp. 123–130). IEEE. doi.org/10.1109/NCCC57165.2022.10067692

Alkhadra, R., Abuzaid, J., AlShammari, M., & Mohammad, N. (2021). SolarWinds Hack: In-depth analysis and countermeasures. In *2021 International Conference on Computing, Networking and Communications (ICCCNT)*. IEEE. doi.org/10.1109/ICCCNT51525.2021.9579611

Angst, C., Block, E., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893–916. doi.org/10.25300/MISQ/2017/41.3.10

Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: Impact of network vulnerability and supply chain integration on incentives to invest. *Information Technology & Management, 11*(1), 7–23. doi.org/10.1007/s10799-010-0066-1

Bartol, N. (2014). Cyber supply chain security practices DNA: Filling in the puzzle using a diverse set of disciplines. *Technovation, 34*(7), 354–361. doi.org/10.1016/j.technovation.2014.01.005

Baskerville, R. (2005). Information warfare: A comparative framework for business information security. *Journal of Information System Security, 1*(1), 23–50.

Benaroch, M. (2021). Third-party induced cyber incidents—Much ado about nothing? *Journal of Cybersecurity, 7*(1). doi.org/10.1093/cybsec/tyab020

Benthall, S. (2017). Assessing software supply chain risk using public data. In *2017 IEEE 28th Annual Software Technology Conference (STC)* (pp. 1–5). IEEE. doi.org/10.1109/STC.2017.8234461

Bekmeier-Feuerhahn, S. (2009). Mechanisms of teleological change. *Management Revue, 20*(2), 126–137.

Bode, C., & Wagner, S. M. (2015). Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. *Journal of Operations Management, 36,* 215–228. doi.org/10.1016/j.jom.2014.12.004

Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2021). Key practices in cyber supply chain risk management: Observations from industry. *National Institute of Standards and Technology.* doi.org/10.6028/NIST.IR.8276

Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2020). *Case studies in cyber supply chain risk management: Summary of findings and recommendations.* National Institute of

Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2021). Cybersecurity supply chain risk management practices for systems and organizations. *National Institute of Standards and Technology.* doi.org/10.6028/NIST.CSWP.02042020-1

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review,* 5(4), 28–34. doi.org/10.22215/timreview/888

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation, 34*(7), 342–353. doi.org/10.1016/j.technovation.2014.02.001

Boyson, S., Corsi, T., & Paraskevas, J. (2022). Defending digital supply chains: Evidence from a decade-long research program. *Technovation, 118.* doi.org/10.1016/j.technovation.2021.102380

Boyson, S., Corsi, T., & Rossman, H. (2009). *Building a cyber supply chain assurance reference model.* Science Applications International Corporation (SAIC).

Boyson, S., Corsi, T., Rossman, H., & Dorin, M. (2011). Assessing SCRM capabilities and perspectives of the IT vendor community: Toward a cyber supply chain code of practice. *University of Maryland Robert H. Smith School of Business and National Institute of Standards and Technology.*

Caldwell, T. (2015). Securing small businesses – The weakest link in a supply chain? *Computer Fraud & Security*, *2015*(9), 5–10. doi.org/10.1016/S1361-3723(15)30083-X

Chakravarthy, B. S./Lorange, P. (1991): Managing the strategy process. Englewood Cliffs.

Chowdhury, N. H., Adam, M. T., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour & Information Technology*, *38*(12), 1290–1308. doi.org/10.1080/0144929X.2019.1583769

Colicchia, C., Creazza, A., & Menachof, D. A. (2018). Managing cyber and information risks in supply chains: Insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2), 215–240. doi.org/10.1108/SCM-09-2017-0289

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *13*(1), 3–21. doi.org/10.1007/BF00988593

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2021). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, *27*(1), 30–53. doi.org/10.1108/SCM-02-2020-0073

Crosignani, M., Macchiavelli, M., & Silva, A. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432–448. doi.org/10.1016/j.jfineco.2022.12.002

Davis, A. (2015). Building cyber-resilience into supply chains. *Technology Innovation Management Review*, *5*(4), 19–27.

Deane, J., Baker, W., & Rees, L. (2023). Cybersecurity in supply chains: Quantifying risk. *Journal of Computer Information Systems*, *63*(3), 507–521. doi.org/10.1080/08874417.2022.2081882

do Amaral, T. M. S., & Gondim, J. J. C. (2021, November). Integrating Zero Trust in the cyber supply chain security. In *2021 Workshop on communication networks and power systems (WCNPS)* (pp. 1-6). IEEE.

European Banking Authority (EBA). (2019). Guidelines on outsourcing arrangements. Retrieved October 3, 2023, from https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

Gale, M., Bongiovanni, I., & Slapničar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, 121, 102840. doi.org/10.1016/j.cose.2022.102840

Gani, A., Fernando, Y., Lan, S., Lim, M., & Tseng, M. (2023). Interplay between cyber supply chain risk management practices and cybersecurity performance. *Industrial Management & Data Systems*, *123*(3), 843–861. doi.org/10.1108/IMDS-05-2022-0313

Gaudenzi, B., & Siciliano, G. (2017). Just do it: Managing IT and cyber risks to protect the value creation. *Journal of Promotion Management*, *23*(3), 372–385. doi.org/10.1080/10496491.2017.1294875

Gaudenzi, B., & Siciliano, G. (2018). Managing IT and cyber risks in supply chains. In Y. Khojasteh (Ed.), *Supply Chain Risk Management: Advanced Tools, Models, and Developments* (pp. 85–96). Springer. doi.org/10.1007/978-981-10-4106-8_5

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223–240. doi.org/10.1108/SCM-10-2018-0357

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods*, *16*(1), 15–31. doi.org/10.1177/1094428112452151

Giunipero, L., & Eltantawy, R. (2004). Securing the upstream supply chain: A risk management approach. *International Journal of Physical Distribution & Logistics Management*, 34, 698–713. doi.org/10.1108/09600030410567478

Glaser, B., & Strauss, A. (2017). *Discovery of grounded theory: Strategies for qualitative research*. Routledge.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, *30*(3), 611–642. doi.org/10.2307/25148742

Hao, J., & Cai, W. (2011). Trusted Block as a Service: Towards sensitive applications on the cloud. In *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 73–82). IEEE. doi.org/10.1109/TrustCom.2011.13

Healthcare & Public Health Sector Coordinating Councils. (2019, October). *Healthcare industry cybersecurity supply chain risk management guide*. Private Public Partnership. Retrieved from https://healthsectorcouncil.org/hic-scrim-v2/

International Organization for Standardization & International Electrotechnical Commission. (2021). *ISO/IEC 27036-1: Cybersecurity — Supplier relationships Part 1: Overview and concepts*.

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27036-2: Cybersecurity — Supplier relationships Part 2: Requirements*.

International Organization for Standardization & International Electrotechnical Commission. (2023). *ISO/IEC 27036-3: Cybersecurity — Supplier relationships Part 3: Guidelines for information and communication technology supply chain security*.

Iovan, Ş., & Iovan, A. A. (2016). Cloud computing security. Fiability & Durability/Fiabilitate si Durabilitate, (1), 1(Suppl.1), 206-212.

ISACA. (2018). *Control objectives for information and related technologies COBIT 2019*. Retrieved from https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf

Khan O, Estay S. D. (2015). Supply chain cyber-resilience: Creating an agenda for future research. Technology Innovation Management Review. 5,6–12. doi.org/10.22215/timreview/885

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics*, *10*(10), 1168. doi.org/10.3390/electronics10101168

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, 23, 1–13. doi.org/10.1007/s10796-019-09977-z

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review*, *24*(4), 691–710. doi.org/10.5465/amr.1999.2553248

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). Cybersecurity information sharing: A framework for information security management in UK SME supply chains.

Li, F. (2024, July 24). Microsoft-CrowdStrike outage: How a single software update was able to cause IT chaos across the globe. *The Conversation*. Retrieved from https://theconversation.com/microsoft-crowdstrike-outage-how-a-single-software-update-was-able-to-cause-it-chaos-across-the-globe-235165

Lin, W. C., and Saebeler, D. (2019). Risk-based v. compliance-based utility cybersecurity - A false dichotomy? Energy Law Journal, *40*(2), 243–282.

Linton, J. D., Boyson, S., & Aje, J. (2014). The challenge of cyber supply chain security to research and practice – An introduction. *Technovation*, *34*(7), 339–341. doi.org/10.1016/j.technovation.2014.05.001

Liu, C. W., Huang, P., & Lucas, H. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems*, 37, 758–787. doi.org/10.1080/07421222.2020.1790190

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. *Management Science*, *34*(5), 583–598.

Miller, A. R., & Tucker, C. E. (2011). Encryption and the loss of patient data. *Journal of Policy Analysis and Management*, *30*(3), 534–556. doi.org/10.1002/pam.20590

Mohr, L. B. (1982). *Explaining organizational behavior*. San Francisco, CA: Jossey-Bass.

Monev, V. (2021). The 'self-assessment' method within a mature third-party risk management process in the context of information security. *2021 IEEE XX International Scientific and Technical Conference (InfoTech)*. doi.org/10.1109/InfoTech52438.2021.9548373

National Institute of Standards and Technology. (2020). *SP-800-53r5: Security and privacy controls for information systems and organizations*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Nutt, P. C. (2002). Why decisions fail: Avoiding the blunders and traps that lead to debacles. San Francisco, CA: Berrett-Koehler Publishers.

Pandey, S., Singh, R., Gunasekaran, A., & Kaushik, A. (2020). Cybersecurity risks in globalized supply chains: Conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103–128. doi.org/10.1108/JGOSS-05-2019-0042

Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. Safety Science, 159, 106022. doi.org/10.1016/j.ssci.2022.106022

Ponemon Institute. (2022). *The 2022 Data Risk in the Third-Party Ecosystem Study*. Retrieved from https://ponemonsullivanreport.com/2022/10/the-2022-data-risk-in-the-third-party-ecosystem-study/

Siciliano, G., & Gaudenzi, B. (2018). The role of supply chain resilience on IT and cyber-disruptions. In Lamboglia, R., Cardoni, A., Dameri, R., & Mancini, D. (Eds.), *Reshaping Accounting and Management Control Systems* (pp. 57–69). doi.org/10.1007/978-3-319-62636-9_4

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, *282*(1), 161–171. doi.org/10.1016/j.ejor.2019.09.017

Sindhuja, P. N., & Kunnathur, A. S. (2015). Information security in supply chains: A management control perspective. Information & Computer Security, *23*(5), 476-496. doi.org/10.1108/ICS-07-2014-0050

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, 44, 100548. doi.org/10.1016/j.accinf.2021.100548

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems*, 51, 100642. doi.org/10.1016/j.accinf.2023.100642

Tender, I. (2023). Top 5 security threats from 3rd parties. *Network World*. Retrieved from https://www.networkworld.com/article/2991914/top-5-security-threats-from-3rd-parties.html

The European Union Digital Operational Resilience Act (DORA), Articles 28–30. (2023). Retrieved from https://www.digital-operational-resilience act.com/DORA_Articles_(Proposal).html

The Ponemon Institute. (2022). *The 2022 data risk in the third-party ecosystem study*. Retrieved from https://ponemonsullivanreport.com/2022/10/the-2022-data-risk-in-the-third-party-ecosystem-study/

Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts: Analyzing coverage of supply chain cybersecurity in critical national infrastructure sectorial and cross-sectorial frameworks. *Computers & Security*, 108, 102324. doi.org/10.1016/j.cose.2021.102324

Urciuoli, L., Männistö, T., Hintsa, J., & Khan, T. (2013). Supply chain cybersecurity – Potential threats. *Information & Security: An International Journal*, 29, 51–68. doi.org/10.11610/isij.2904

Urciuoli, L., Mohanty, S., Hintsa, J., & Boekesteijn, E. (2014). The resilience of energy supply chains: A multiple case study approach on oil and gas supply chains to Europe. *Supply Chain Management: An International Journal*, 19. doi.org/10.1108/SCM-09-2012-0307

Vanajakumari, M., Mittal, S., Stoker, G., Clark, U., & Miller, K. (2021). Towards a leader-driven supply chain cybersecurity framework. *Computers & Security*, 14, 42–52.

Van de Ven, A. H., & Poole, M. S. (1995). Explaining development and change in organizations. *Academy of Management Review*, *20*(3), 510–540. doi.org/10.5465/amr.1995.9508080329

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 Information Security Framework for reducing cyberattacks on supply chain management systems. *IFAC-PapersOnLine*, *48*(3), 1846–1852. doi.org/10.1016/j.ifacol.2015.06.355

Wolf, J. (2021). How the NotPetya attack is reshaping cyber insurance. *Brookings*. Retrieved from https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/

Yeo, M., Rolland, E., Ulmer, J., & Patterson, R. (2014). Risk mitigation decisions for IT security. *ACM Transactions on Management Information Systems (TMIS)*, 5. doi.org/10.1145/2576757

Acknowledgement

We thank our reviewers, Editor, and all our interviewees and survey participants for their time. We thank Ryan Ko for providing support in terms of contacts and funding, the organizers of the AusCert conference, and, in particular, Gary Gaskell for promoting our study among the ISACA Brisbane members and at the Auscert Conference 2023 and 2024. We also thank Uroš Žust for promoting our study to the ISACA Slovenia participants and Longxiao Zhang to distribute our survey to participants in China.

This work is a part of the research project entitled "A methodology and framework to assist organizations in managing cyber security requirements of their suppliers" that was supported by the University of Queensland's 2022 Cyber Security Transdisciplinary Research Seed Funding, Grant number: 2022-R1 Ko.

https://doi.org/10.3127/ajis.v29.5323