Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era

Alessandro Creazza
School of Industrial Engineering, LIUC University, Castellanza, Italy
Claudia Colicchia
Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy
Salvatore Spiezia
Ibm Italy, Segrate, Italy, and
Fabrizio Dallari
School of Industrial Engineering, LIUC University, Castellanza, Italy

Abstract

Purpose – The purpose of this paper is to explore the perceptions of supply chain managers regarding the elements that make up cyber supply chain risk management (CSCRM) and the related level of alignment, to understand how organizations can deploy a CSCRM strategy that goes beyond the technical, internal functioning of single companies and moves beyond the dyad, to create a better alignment that can ultimately lead to improved cyber supply chain resilience.

Design/methodology/approach – An exploratory survey in the fast-moving consumer goods (FMCG) industry involving over 100 organizations in Italy was conducted. Results were analysed through one-way analysis of variance, to appraise the differences in the perceptions of the various actors of the FMCG supply chain (Manufacturers, Logistics Service Providers, Retailers).

Findings – While a certain degree of alignment of the perceptions across the FMCG supply chain exists, the study found that Logistics Service Providers can play a crucial role as orchestrators of the CSCRM process towards a more "supply chain-oriented" response to cyber threats and risk events. The research also highlights the necessity to see people as key elements for improving cyber resilience in the supply chain.

Research limitations/implications – Through a vertical analysis of a supply chain, the study extends the existing theory on CSCRM, which contains isolated case studies. It also contributes to extending the current theory with the proposal of the paradigm of Logistics Service Providers as orchestrators of the CSCRM process. The study combines different classifications of CSCRM initiatives and embraces theories external to the supply chain literature.

Practical implications – Through the empirical analysis, this study helps practitioners in streamlining the design of cyber security strategies and actions that span across the supply chain for better alignment. This could mean more coordination of efforts and more targeted/accurate investments in CSCRM initiatives. The study invites practitioners to ponder the perceived relevance of the human factor as a source of risk and the perceived importance of countermeasures aimed at mitigating risk events stemming from that source.

Originality/value – By focusing on an entire supply chain, this is one of the first studies on CSCRM that goes beyond the dyad. Its originality also lies in its use of the investigations of perceptions along the supply chain as pillars for the alignment of CSCRM strategies and mitigation initiatives. This original perspective allows for discovering the role of Logistics Service Providers in driving the alignment of the efforts towards better outcomes of the CSCRM process.

Keywords Information systems, Resilience, Surveys, Supply-chain management, Risk management, Cyber risk, Information risk, Cyber security

Paper type Research paper

1. Introduction

Digital transformation has been in place for years and supply chains have not been exempted from it. Supply chains operate in an increasingly connected environment, based on the collaboration of people, processes and devices. The digitalization of processes, which leads to increasing the exchange of data and information along the supply chain, helped by a massive connectivity level, has led to the rise of the "cyber supply chain, a supply chain enhanced by cyber-based technologies to establish an effective value chain" (Kim and Im, 2014).

The current issue and full text archive of this journal is available on Emerald Insight at: **https://www.emerald.com/insight/1359-8546.htm**

Supply Chain Management: An International Journal
27/1 (2022) 30–53
Emerald Publishing Limited [ISSN 1359-8546]
[DOI 10.1108/SCM-02-2020-0073]

Received 19 February 2020
Revised 6 October 2020
13 January 2021
Accepted 15 January 2021

Although greater sharing of information and greater availability of data are positive elements (Colicchia *et al.*, 2019), they conceal risks that cannot be overlooked. Warren and Hutchinson (2000) noticed for the first time that this is a supply chain issue. Supply chains are frequent targets because a weak link in an integrated system can grant hackers access to every company's data. In these cases, attacks are carried out on the third-party business, which is deemed to have the weakest internal security measures in place. After a single member's security protocols are proven to be weak, this weakness is spread to every partner in the supply chain (Momoh, 2016).

Cyber and information risks in supply chains are becoming more and more evident due to the attacks that have resonated globally. A notorious example is the cyber-attack at the Port of Antwerp in Belgium, which took place for over two years, starting in 2011. A trafficking group hid drugs amidst legitimate cargo. They used hackers to infiltrate computer networks in several companies operating at the port. In this way, they had access to sensitive data, such as the location and destination of containers, allowing them to send in corrupted drivers to steal the illegal load before the genuine owner could arrive (Bateman, 2013). More recent examples include the WannaCry attack in 2017, carried out through ransomware that hit several companies, including the car manufacturer Renault, the UK National Health Service, the Russian Interior Ministry and the express courier FedEx. The most interesting victim of this attack from a supply chain perspective was FedEx, which saw the entire TNT Express division inactive for weeks. Due to the blocking of all computers, the company was no longer able to exchange information or access data stored internally. Therefore, it was no longer able to ship cargoes. The companies that relied on this organization for the delivery of their products found themselves in an unexpected difficulty and had to find alternative solutions to reduce inconvenience to their customers in the form of missed deliveries and delays. After an initial estimate made in September 2017, the impact was deemed to cost up to $300m (Bloomberg.com, 2017).

The growth of these cyber-related issues is shaping the agenda of the top managers of companies around the globe; cyber risks and related attacks on information and data in the supply chain are seen as the top threats of the near future and the years to come (BCI, 2019). This has led the European Union to react with the introduction of the General Data Protection Regulation (GDPR), which has been in force since May 2018 and requires that worldwide organizations adopt security countermeasures. However, it seems that companies tend to adopt security measures, especially of information technology (IT) nature, that are mostly aimed at "firewalling themselves", but not their supply chain (Colicchia *et al.*, 2019). It also seems that cyber risks are dealt with from a technical perspective (Gaudenzi and Siciliano, 2017) within individual organizations (Biener *et al.*, 2015).

In this landscape, a relatively large amount of scientific and practitioners' contributions focused on the countermeasures that can be adopted by an organization in terms of IT security and cyber resilience in the supply chain (Eling and Wirfs, 2019). These contributions mainly examine the strengths and weaknesses of cyber risk and security initiatives, especially the ones that deal with the IT domain. Consequently, it appears that the industrial and scientific communities are concentrated on trying to make sense of "what can be done" to deal with cyber and information risks in the supply chain, particularly at the IT security level within the boundaries of the single organizations, without focusing first on the elements constituting a supply chain security strategy. Developing a fully integrated strategic approach to cyber risk is fundamental to supply chains and to think about how to address cyber risk at the end of the strategic process is simply too late in a cyber supply chain management process (Pandey *et al.*, 2020). These elements also constitute the pillars for creating alignment in the supply chain regarding what kind of policies, actions and initiatives should be undertaken to secure the entire supply chain, rather than protecting only single organizations, which by themselves can become individual points of failure in cyberspace. Alignment, in fact, is essential to steering a supply chain towards the same objective by ultimately heading in the same direction with all partners (Gattorna and Jones, 1998). This concept applies to risk management as well and it is essential for achieving a better level of resilience through the cyber supply chain risk management (CSCRM) process (Colicchia *et al.*, 2019). To achieve alignment in the CSCRM process, consensus on objectives should be reached among the players operating in the supply chain to integrate the design of shared security strategies (Radanliev *et al.*, 2020) and perceptions related to the security needs are to be understood. In fact, perception plays a paramount role in shaping the policies and actions undertaken by organizations when cyber and information risks are considered (Gaudenzi and Siciliano, 2017). Besides, it can also affect the evaluation of risks by the players operating in a supply chain and, consequently, influence the level of investment in CSCRM measures. In fact, companies work in asymmetric environments, where not all the organizations involved in a supply chain make the same decisions (Ezhei and Tork Ladani, 2018). Asymmetric environments generate externalities that can affect the level of investment in cyber security, potentially leading to underinvestment or overinvestment and contributing to investment inefficiency in the supply chain (Li and Xu, 2020). Externalities are thus connected to potential misalignments in how cyber security is approached by the different organizations operating in the supply chain. Consequently, aligning perceptions and related actions in a supply chain can lead to the achievement of the so-called cyber supply chain balanced resilience (Colicchia *et al.*, 2019), to minimize the investment inefficiency and lead to better resilience of the overall supply chain.

Notwithstanding the relevance of the concepts described above, the existing literature seems to have given more attention to technical aspects (data, application and networks) of single enterprises rather than to organizational aspects of the CSCRM process across the supply chain, including human elements (Ghadge *et al.*, 2020). Moreover, the literature appears to be scattered and covers an extensive range of topics and fields, without a holistic view that enables those coordination mechanisms that allow supply chain partners to adopt an end-to-end approach beyond the dyad (Colicchia *et al.*, 2019). There is a narrow focus on the supply chain perspective, and specifically on cyber risks and countermeasures related to inbound and outbound supply chain contexts (Pandey *et al.*, 2020). Although the literature

acknowledges the need to address the highlighted research concerns, recent contributions have focused on the exploration of cyber risks and initiatives in the supply chain in small samples of companies working in different supply chains, without examining the factors leading to adopting those initiatives (Colicchia *et al.*, 2019). Also, previous literature did not extend this type of investigation to global players in different supply chains (Pandey *et al.*, 2020) or carried out vertical studies. Existing research present reviews on the constituents of cyber supply chain risk, identifying the main elements and trends, but without an empirical investigation (Ghadge *et al.*, 2020); or studies the mechanisms of externalities in cyber security and how to tackle them through opportune mechanisms but do not explore how these externalities are generated in the supply chain (Li and Xu, 2020); or again focuses on the data management level only, by devising a new approach for cognitive data analytics to create stronger resilience (Radanliev *et al.*, 2020). To the best of the authors' knowledge, the current literature is scant of explorations of perceptions across the supply chain about the fundamental elements of CSCRM and connected level of alignment, and equally a vertical study focused on CSCRM along a supply chain does not yet exist. Moreover, empirical data on CSCRM along a whole supply chain are not available.

Given this background, our paper aims at investigating the perceptions of companies about CSCRM and the related level of alignment across a supply chain. The goal is to help organizations operating in a supply chain to understand how they can deploy a cyber security strategy that goes beyond the technical side, the internal side of single companies and beyond the dyad, to create a better alignment that can ultimately lead to better cyber supply chain resilience.

We aim to achieve the objective of our research by providing an answer to the following research questions:

RQ1. How relevant are the elements of CSCRM perceived by companies in a supply chain?

RQ2. How aligned are the perceptions about CSCRM of companies in a supply chain?

To answer the research questions of the study, we perform a vertical analysis of a specific supply chain, following suggestions from the literature, which calls for this kind of investigation (Colicchia *et al.*, 2019).

Given its importance in terms of amounts of goods moved, the information generated and data exchanged along its supply chain, we examine the fast-moving consumer goods (FMCG) sector. We conduct an exploratory survey that studies the perceptions of supply chain managers regarding the elements of CSCRM. The managers surveyed operate in the three main stages of a generic FMCG supply chain, i.e. Manufacturers, Logistics Service Providers and Retailers. This allows for exploring the perceptions along the supply chain and for generating insights for the achievement of a more aligned CSCRM process that moves towards better resilience and cyber supply chain balanced resilience.

The remainder of the paper is organized as follows: Section 2 presents an overview of the literature on CSCRM and highlights some research gaps; Section 3 presents the research methodology adopted in this work; Section 4 describes the results from the empirical investigation carried out; Section 5 discusses the findings of the analysis; Section 6 presents the conclusion.

2. Theoretical background

To support the achievement of the objective of the present study, a literature review on the concept of CSCRM has been carried out. This has been done to unveil, understand and isolate the principal elements of CSCRM, which will be the object of the present investigation. To better support the analysis of perceptions of cyber and information risk by managers, specific literature focused on this theme has also been scrutinized.

CSCRM, according to Boyson (2014), is a construct that includes "the strategy and initiatives focusing on the assessment and mitigation of cyber and information risks across the end-to-end operations of a supply chain". Compared to the usual approach to information risk management, CSCRM implies that a more holistic approach is adopted to combine processes, people and technology to take into account a "relationship dimension" (Spekman and Davis, 2004). The relationship dimension is aimed at allowing for a superior level of integration among supply chain partners. Integration should allow for going beyond the dyad to overcome the limitations of a focus on single points of the interface along the supply chain. The purpose of CSCRM is to extend control on cyber risks across the end-to-end supply chain in a fashion that enables a continuously adaptive capacity. According to the theory on CSCRM, a holistic approach is expected to lead to better cyber resilience. More in general, supply chain resilience can be achieved through the identification of a suitable fit between the riskiness of a company's supply chain and the related level of preparedness to manage risks. This "right fit" is then applied to the decisions to make appropriate investments in supply chain risk management initiatives that could cope with the identified level of risk. Pettit *et al.* (2013) define this fit as "balanced resilience". According to Gualandris and Kalchschmidt (2015), the concept of balanced resilience represents:

> the match between the level of riskiness of a certain supply chain configuration and the related amount of investment in the supply chain risk management process, appropriate to adequately confront that level of riskiness and to continuously adapt to changes

Colicchia *et al.* (2019) extend the concept of balanced resilience to cyber risks and, as a result, they propose the concept of "cyber supply chain balanced resilience". To achieve cyber supply chain balanced resilience, the fit between the level of cyber risk in the supply chain and the consequent actions and initiatives to be undertaken needs to be grounded on the evaluation of the level of riskiness and the needs for protection along the entire supply chain and not only in the focal company. Hence, it appears that the set of perceptions that decision makers hold constitutes the basis of that fit leading to enhanced balanced resilience.

Having a good understanding of risk is essential to supporting managers in making the right decisions and adopting appropriate security measures (Volpentesta *et al.*, 2011). However, the ability of humans to make objective estimations about risk and events that might happen in the future, basing their judgement on what happened in the past, is

limited (Bernstein, 1996). This becomes of particular relevance if we take into account the two dimensions composing the concept of risk, i.e. probability and impact on business (March and Shapira, 1987). The existing literature has attempted to support decision makers in the assessment of the two dimensions of risk, by providing semi-subjective guidelines to assist in the definition of the "values" of probability and impact in the context of risk. Hallikas *et al.* (2004) proposed an impact assessment scale that spans from "no impact" when the consequences of a risk event are "insignificant in terms of the whole company" to "catastrophic impact" when the consequences of a risk event are able to "discontinue business". Similarly, they also proposed a probability assessment scale that spans from "very unlikely" in the presence of a "very rare event" to "very probable" in the presence of an "event that recurs frequently". These semi-subjective estimates have been combined in risk assessment matrixes to support decision makers in a structured and replicable way (Wieland, 2013). However, still much is left to individuals' viewpoints in relation to the organization in which they work and the sector in which their company operates. These limitations also apply to the case of attempts to quantitatively estimate the impacts of a multitude of (though partially connected) drivers of risk, particularly "when there is no way to rely on a real baseline" (Alter and Sherer, 2004). As a consequence, even though decisions and initiatives related to information security are supposed to be based on structured techniques and methods to assess cyber and information risk assessment, these decisions and initiatives seem to be the result of the perception security managers have of information risk, i.e. a personal estimation of the likelihood that a certain type of incident may happen and how they think this affects information systems in terms of the magnitude of its effects (Volpentesta *et al.*, 2011). Individuals are inclined to rely on their perception of risks, that is, on their confidence about the existence of certain sources of risk and their own belief that certain incidents and negative impacts will manifest themselves.

If risk perception seems to be a subjective measure that affects the set of decisions taken by decision makers in terms of risk mitigation actions, subjectivity might be of paramount importance when the effect of decisions taken in a certain stage of a chain of supply spans across multiple stages (Gaudenzi and Siciliano, 2017). Having different perceptions potentially leads to misalignment in the supply chain, which causes a decrease in the overall supply chain performance (Gattorna and Jones, 1998); this concept also applies to risk management, when different approaches or decisions about initiatives are taken for managing (cyber) risks in the supply chain by different players in different stages, with negative effects on the overall level of resilience (Colicchia *et al.*, 2019). In other words, alignment of perceptions along the supply chain could lead to the undertaking of CSCRM actions that veer towards the attainment of improved resilience and cyber supply chain balanced resilience. This idea is closely connected to the principles of the protection motivation theory (Rogers, 1983), which deals with predicting an individual's intention to engage in protective actions based on his/her appraisal of the threats and of his/her capability to cope with those threats (Anderson and Agarwal, 2010).

According to this view, it is essential to take into account the elements to be appraised in terms of threats and in terms of actions to cope with risk because, as previously discussed, they constitute the foundations and backbone of any security policy. Alignment among the players of the supply chain regarding the various elements that make up the CSCRM process, in this sense, could help in conducting consistent appraisals across the supply chain. In the least, it could provide a broader view of the threats that can span the various stages of the chain of supply. In this way, measures could be taken that adequately cope with those threats at a supply chain level. The elements composing the CSCRM process to be appraised in terms of perceptions of the players operating in the supply chain have been examined and classified by the existing literature and they have been condensed into a set of constituents. More specifically, scientific contributions such as Ghadge *et al.* (2020) and Colicchia *et al.* (2019) propose the following set of elements: cyber risks in supply chains, sources of risks, responsibility and ownership of the CSCRM process, information exchanged in the supply chain and countermeasures and initiatives to manage cyber risks in the supply chain.

Table 1 presents a list of the main contributions on the investigated topic that have been analysed and classified, according to the abovementioned elements of the CSCRM process, through the concept-based structure proposed by Webster and Watson (2002). Overall, no contributions focus on all the CSCRM elements in an integrated way, which is fundamental to support the development of an effective and fully strategic approach to CSCRM (Pandey *et al.*, 2020). Among the elements, much of the focus for research still appears to be on cyber risks, sources of cyber risks and measures to tackle them. Previous contributions mainly present conceptual frameworks without empirical data (Boyson, 2014; Radanliev *et al.*, 2020), investigations with illustrative cases or on companies working in different supply chains (Urciuoli and Hintsa, 2017; Pandey *et al.*, 2020) or modelling efforts on specific issues or risk events (Deane *et al.*, 2009; Li and Xu, 2020). The only contributions on the evaluation of perceptions within the investigated field focus either on the effect of incident awareness on information security policies (Volpentesta *et al.*, 2011) or on perceptions of risks and IT interventions (Gaudenzi and Siciliano, 2017) – but without embracing cyber risks according to a supply chain perspective. Also, previous contributions predominantly focus on the technical aspects of single organizations. The nexus between technical aspects and organizational ones, in terms of perceptions, responsibility, type of information shared and countermeasures directed at the backbone of supply chains, i.e. employees, along with empirical data on a whole supply chain is critical to adopt an end-to-end approach that goes beyond the dyad (Smith *et al.*, 2007; Ghadge *et al.*, 2020). Given that the overview of the literature confirms the absence of contributions able to address this nexus, we developed our research building on the contributions included in Table 1.

The elements composing the CSCRM process are defined and classified according to different taxonomies and categories as reported below. In our endeavour, we will take into consideration a combination of the various approaches that merge the different viewpoints to provide a holistic view of the CSCRM process.

Table 1 Overview of the main literature contributions on CSCRM

	Cyber risks in supply chains	Sources of cyber risks	Responsibility and ownership of the CSCRM process	Information exchanged in the supply chain	Initiatives and countermeasures to manage cyber risks	Methodology	Focus of the analysis
Bandyopadhyay *et al.* (2010)					✓	Quantitative	Investments in cyber security
Bartol (2014)	✓				✓	Conceptual	Cyber security standards, processes, tools and techniques
Boone (2017)			✓		✓	Conceptual	Cyber security in the organizations
Boyson (2014)		✓			✓	Conceptual	Definition of the concept of CSCRM
Charitoudi and Blyth (2014)	✓	✓			✓	Qualitative	Estimation of the impacts of cyber attacks
Colicchia *et al.* (2019)	✓	✓	✓		✓	Qualitative	CSCRM initiatives and actions in the supply chain
Deane *et al.* (2009)	✓					Quantitative	Quantification of IT security risks in the supply chain
Eling and Wirfs (2019)	✓	✓				Quantitative	Assessment of cyber risks and related costs
Ezhei and Tork Ladani (2018)	✓	✓				Quantitative	Impact of interconnectivity on security investments
Faisal *et al.* (2007)	✓	✓				Quantitative	Assessment of information risks
Gaudenzi and Siciliano (2017)	✓					Qualitative	Evaluation of perceptions on cyber risks
Ghadge *et al.* (2020)	✓	✓			✓	Conceptual	Review on CSCRM
Gordon and Ford (2006)	✓					Qualitative	Classification of cyber crime
Järveläinen (2013)	✓				✓	Quantitative	Continuity management in information systems
Jones and Horowitz (2012)					✓	Qualitative	Definition of system-aware cyber security architecture
Keegan (2014)					✓	Conceptual	Insurance policies on information and data
Khursheed *et al.* (2016)		✓	✓		✓	Conceptual	Job profiles for cyber security
Kim and Im (2014)					✓	Conceptual	Issues of cyber supply chain security in Korea
Lee and Whang (2000)				✓		Conceptual	Information shared in a supply chain
Li and Xu (2020)	✓				✓	Quantitative	Impact of interconnectivity on security investments
Linton *et al.* (2014)	✓					Conceptual	Introduction to the concept of cyber supply chain security
Lotfi *et al.* (2013)				✓		Conceptual	Information shared in a supply chain
Luiijf *et al.* (2013)	✓	✓			✓	Qualitative	National cyber security strategies
Mukhopadhyay *et al.* (2013)	✓				✓	Quantitative	Decision models for cyber risk insurance
Pandey *et al.* (2020)	✓	✓			✓	Qualitative	Cyber risks in the global supply chain

(*continued*)

Table 1

	Cyber risks in supply chains	Sources of cyber risks	Responsibility and ownership of the CSCRM process	Information exchanged in the supply chain	Initiatives and countermeasures to manage cyber risks	Methodology	Focus of the analysis
Radanliev *et al.* (2020)	✓				✓	Conceptual	Cognitive data analytics for stronger resilience in the cyber space
Secci and Murugesan (2014)		✓			✓	Conceptual	Cloud resiliency and IT operational resilience measures
Sharma and Routroy (2016)		✓				Quantitative	Models of information risk
Sindhuja (2014)					✓	Quantitative	Impact of information security initiatives on supply chain performance
Sindhuja and Kunnathur (2015)		✓			✓	Conceptual	Review on information security management
Smith *et al.* (2007)	✓	✓				Quantitative	Trade-off between collaboration and cyber security
Spekman and Davis (2004)	✓					Conceptual	Risks across the extended enterprise
Stephens and Valverde (2013)	✓	✓			✓	Qualitative	Cyber security, threat models, security policies for e-procurement
Tao *et al.* (2016)	✓				✓	Quantitative	Information sharing and disruptions in a supply chain
Tran *et al.* (2016)	✓	✓			✓	Qualitative	Supply chain managers perceptions of risks related to information sharing
Trombley (2015)		✓			✓	Qualitative	Information risk management
Urciuoli and Hintsa (2017)	✓	✓	✓			Qualitative	Security threats in supply chains
Volpentesta *et al.* (2011)	✓				✓	Quantitative	Effects of incident security awareness on information risk perception
Warren and Hutchinson (2000)	✓				✓	Conceptual	Cyber-attacks to supply chains and some seminal countermeasures
Windelberg (2016)	✓				✓	Conceptual	Objectives for managing cyber supply chain risk
Xue *et al.* (2013)	✓	✓			✓	Quantitative	Supply chain digitization and IT governance
Zuo and Hu (2009)	✓	✓				Conceptual	Trust-based information risk management in a supply chain

2.1 Cyber risks in supply chains

While generally, the existing literature contains a number of classifications for supply chain risks (Jüttner *et al.*, 2003; Manuj and Mentzer, 2008; Ho *et al.*, 2015), very few taxonomies exist for classifying cyber risks in supply chains. Faisal *et al.* (2007) presented a seminal paper identifying different information risks that can have an impact on the supply chain. Gordon and Ford (2006) propose two categories of risks: Type 1 cyber risks include incidents of phishing and theft or manipulation of data or services; Type 2 covers cyberstalking and harassment, stock market manipulation, blackmailing and corporate espionage. National Cyber Security Centre, UK (2016) distinguish cyber-attacks into un-targeted and targeted attacks. Ghadge *et al.* (2020) propose a holistic classification of risk events that takes into account risks coming from external environments, internal activities and physical breakdowns, while Colicchia *et al.* (2019) emphasize the dimension of confidentiality, privacy and information integrity across different layers of the supply chain. Building on previous literature on specific cyber and information risk items, a combination of the various taxonomies will be adopted. The following cyber risks will be taken into account, which we derived from Colicchia *et al.* (2019) as a backbone, together with the main sources of literature that informed the development of their taxonomy: enterprise resource planning (ERP) system malfunction (Colicchia *et al.*, 2019), the crash of company's website (Tran *et al.*, 2016), lack of network connectivity (Faisal *et al.*, 2007), malware (Deane *et al.*, 2009), a data breach (Boyson, 2014), damage of records (Zuo and Hu, 2009) and theft of credentials (Zuo and Hu, 2009). As previously mentioned, the traditional literature on supply chain risk management has proposed several ways to "assess" risks and these are mainly based on the assessment of the two dimensions of probability and impact on business (Hallikas *et al.*, 2004). However, it seems that the concurrent assessment of the actual occurrence of these risks as a further dimension is not contemplated – notwithstanding the statements by Volpentesta *et al.* (2011). They affirm that how risk incidents are experienced and reported affects the perception of the risks themselves.

2.2 Sources of cyber risks

Likewise, very few classifications of the sources of cyber risks that exist in the literature. Colicchia *et al.* (2019) propose a taxonomy that takes into account the internal/external dimension of the sources and the maliciousness/non-intentionality of the actions of those sources of risk (Table 2). Ghadge *et al.* (2020) posits the points of penetration (i.e. the weak points of the supply chain network where risks are most likely to penetrate (Smith *et al.*, 2007), subdividing them into human points of penetration (employees) and physical points of penetration (physical objects such as buildings, machines and other surroundings) and technical points of penetration (IT-related assets including systems, software, personnel and equipment). These are classified by Colicchia *et al.* (2019) as external and internal technical problems. External technical problems, for example, relate to power cuts or loss of connectivity due to the failure of the energy provider or the internet service provider. In contrast, internal technical problems relate to the failure of the company's power and connectivity infrastructure, including their power and IT assets and systems.

2.3 Responsibility and ownership of the cyber supply chain risk management process

Another element characterizing CSCRM is the ownership of the risk management process (Jüttner *et al.*, 2003; Ribeiro and Barbosa-Povoa, 2018), which is essential to drive coordination among supply chain members to manage risk and enhance resilience through both proactive and reactive measures (Wieland and Wallenburg, 2013). Likewise, it is also essential that the whole organization is engaged in the CSCRM process, with strong commitment from the top and with the removal of the silo approach in the management of the process (Boone, 2017). This could be empowered through the introduction of specific job profiles in the organization working in the area of cyber security (Khursheed *et al.*, 2016). The main departments potentially owning and collaborating in the CSCRM process have been proposed by Colicchia *et al.* (2019) and they are represented by top management, IT, operations, supply chain/logistics, finance, risk management, legal, human resources.

2.4 Information exchanged in the supply chain

CSCRM deals with the exchange of data and information along the supply chain; consequently, it is essential to understand what categories of information are exchanged in cyberspace and what level of criticality/riskiness/need to protection is perceived in relation to them. A few scientific contributions present classifications of the categories of information exchanged in the supply chain. Building on Lee and Whang (2000) and on Lotfi *et al.* (2013), we take into account the following categories of information: inventory level, sales data and forecasts, invoices, discounts and promotional plans, order status (delivery tracking information), production plans, performance metrics (including costs and capacity) and product information (master data).

2.5 Initiatives and countermeasures to manage cyber risks

The existing literature provides some classification of the initiatives and countermeasures to mitigate cyber and information risks in supply chains. These classifications propose an examination of possible CSCRM actions in terms of scope and in terms of time-phasing. Building on previous literature, Colicchia *et al.* (2019) suggest a taxonomy that includes organizational initiatives, training and internal awareness, compliance and external awareness, event management, IT security tools and IT operational resilience initiatives. In doing this, they emphasize the presence of supply chain-oriented actions and actions internal to the single organizations. In their work, they found that organizations tend to focus more on the internal and IT technical side. Likewise, moving from an examination of previous studies, Ghadge *et al.* (2020) overcome a conventional proactive and reactive risk mitigation classification and propose a time-phased classification of mitigation measures. Building on Jones and Horowitz (2012), they differentiate among three phases of a cyber-attack: pre-, trans- and post-attack. Pre-attack countermeasures include actions at the technical level and those directed at or carried out by human factors. Trans-attack measures include data consistency checks and task forces, while post-attack measures include forensics, incident

Table 2 Main sources of cyber risks

	Malicious		Non-intentional	
Internal	Current employees	Eling and Wirfs (2019) **Faisal *et al.* (2007)** **Sindhuja and Kunnathur (2015), Urciuoli and Hintsa (2017); Pandey *et al.* (2020), Boyson (2014); Trombley (2015)**	Current employees	Eling and Wirfs (2019) Faisal *et al.* (2007) Sindhuja and Kunnathur (2015), Urciuoli and Hintsa (2017); Pandey *et al.* (2020), Boyson (2014); Trombley (2015)
	Former employees	Eling and Wirfs (2019) **Faisal *et al.* (2007)** **Sindhuja and Kunnathur (2015), Urciuoli and Hintsa (2017); Pandey *et al.* (2020), Boyson (2014); Trombley (2015)**	Former employees	Eling and Wirfs (2019) Faisal *et al.* (2007) Sindhuja and Kunnathur (2015), Urciuoli and Hintsa (2017); Pandey *et al.* (2020), Boyson (2014); Trombley (2015)
			Technical problems	Bandyopadhyay *et al.* (2010), Smith *et al.* (2007); Secci and Murugesan (2014)
External	Suppliers/ contractors	Li and Xu (2020), Ezhei and Tork Ladani (2018); Boyson (2014)	Suppliers/contractors	Li and Xu (2020), Boyson (2014)
	Customers **Competitors**	Ezhei and Tork Ladani (2018), Boyson (2014) Faisal *et al.* (2007); Ezhei and Tork Ladani (2018), Boyson (2014)	Customers Natural disasters	Boyson (2014) Charitoudi and Blyth (2014) **Faisal *et al.* (2007)** **Tran *et al.* (2016)** **Urciuoli and Hintsa (2017), Boyson (2014)**
	Hackers/ Hacktivists	Deane *et al.* (2009) **Ezhei and Tork Ladani (2018)** **Faisal *et al.* (2007)** **Khursheed *et al.* (2016)** **Sindhuja and Kunnathur (2015), Ezhei and Tork Ladani (2018); Pandey *et al.* (2020), Luiijf *et al.* (2013)**	Technical problems	Bandyopadhyay *et al.* (2010), Secci and Murugesan (2014)

Source: adapted from Colicchia *et al.*, 2019 and main related references

documentation, insurance and recovery and backup procedures. Ghadge *et al.* (2020) found that the literature on the pre-attack phase is abundant, with several examples of implementation of actions by companies, while trans- and post-attack measures are less addressed by the scientific community and less adopted by organizations. However, they also claim that trans- and post-attack measures are needed to foster proactive mitigation of cyber risks and reactive mitigation strategies. In general, the literature seems to be aligned on suggesting a varied set of actions that should be available to use to cover different attacks and different risk environments in a dynamic way. The literature indicates the importance of having integration and collaboration when investments in CSCRM actions are undertaken by the various players operating in a supply chain (Bandyopadhyay *et al.*, 2010).

In our research endeavour, we will adopt a combination of the taxonomies and classification approaches proposed by Ghadge *et al.* (2020) and Colicchia *et al.* (2019) (see Table 3, which also includes the main sources of knowledge related to each initiative that informed the development of the adopted taxonomies).

3. Methodology

Given the objective and the research questions of the present study and the identified research gaps, we decided to develop a quantitative study through a survey built upon the existing exploratory research on CSCRM. This approach based on exploratory research is consistent with several studies published in the literature that deal with supply chain contexts (Croom, 2005) or cutting-edge supply chain issues (Van Hoek, 2019).

As previously mentioned, the existing literature calls for further analysis of the management of CSCRM to collect empirical data, especially concerning vertical studies that concentrate on and examine a specific supply chain or sector (Colicchia *et al.*, 2019). This would allow for overcoming the limitations of dyadic studies and to better understand the specific mechanisms of a certain supply chain. In addition, differences among industries make it sensible to concentrate on a particular industry at a time (Thun and Hoenig, 2011). For these reasons, in this study, we focus on a specific sector, specifically the FMCG industry in Italy. We decided to study this industry because it relies heavily on information sharing and is one of the main contributors to the gross domestic product of all countries. Also, the retail sector is among the top three in which cybercrime is spreading more rapidly. This sector shows a growing trend in IT violations, exceeded only by the health care industry (Clusit, 2017). The FMCG sector has considerably raised the attention of consumers and policymakers because it is vital for providing essential products at high quality and low cost (Bourlakis and Weightman, 2004).

Table 3 Types of initiatives to mitigate cyber risks

Initiatives	Type of initiative		References
Employ a chief information security officer (CISO) or data protection officer (DPO)	Internal organizational initiatives	Pre-attack	Khursheed *et al.* (2016), Boyson (2014)
Conduct personnel background checks	Internal organizational initiatives	Pre-attack	Kim and Im (2014), Stephens and Valverde (2013)
Presence of an information security strategy	Internal organizational initiatives	Pre-attack	Sindhuja (2014), Xue *et al.* (2013); Bartol (2014)
Specific data and information insurance	Internal organizational initiatives	Post-attack	Boyson (2014), Keegan (2014); Mukhopadhyay *et al.* (2013)
Employee security awareness training programme (cyber hygiene)	Training and internal awareness	Pre-attack	Boyson (2014), Sindhuja and Kunnathur (2015); Stephens and Valverde (2013), Tran *et al.* (2016); Xue *et al.* (2013), Windelberg (2016)
Secure data access and control measures	Internal data management	Pre-attack	Sindhuja and Kunnathur (2015), Pandey *et al.* (2020); Windelberg (2016), Trombley (2015)
Accurate record of personnel handling sensitive data	Internal data management	Pre- and trans-attack	Pandey *et al.* (2020), Windelberg (2016)
IPS, data and URL filtering (antivirus and antispam)	Internal IT security and resilience tools	Pre-attack	Charitoudi and Blyth (2014)
Multiple data backup	Internal IT security and resilience tools	Pre-attack	Sindhuja (2014), Secci and Murugesan (2014)
Geographical distributed datacentres	Internal IT security and resilience tools	Pre-attack	Sindhuja (2014), Secci and Murugesan (2014)
Require suppliers and customers to comply with the privacy and security policies	Compliance and external awareness	Pre-attack	Boyson (2014), Sindhuja and Kunnathur (2015); Sindhuja (2014), Tran *et al.* (2016); Bandyopadhyay *et al.* (2010), Li and Xu (2020); Pandey *et al.* (2020)
Conduct supply chain partners security audits	Compliance and external awareness	Pre-attack	Boyson (2014), Stephens and Valverde (2013)
Communication procedures with involved supply chain partners	External event management	Trans- and post-attack	Boyson (2014), Kim and Im (2014); Radanliev *et al.* (2020), Sindhuja (2014); Li and Xu (2020), Tran *et al.* (2016); Tao *et al.*, 2016; Scholten and Schilder, 2015; Järveläinen (2013)
Business continuity and disaster recovery plans	External event management	Trans- and post-attack	Tao *et al.*, 2016; Järveläinen (2013)

Note: URL = Uniform resource locator
Source: Adapted from Ghadge *et al.*, 2020 and Colicchia *et al.*, 2019 and related references

Increased competition creates considerable pressure on FMCG retailers to reduce costs and improve service levels at the same time (Fernie and Sparks, 2014). This is particularly challenging in the FMCG context because in the past few years consumers have expressed a clear demand for a higher service level, which has inevitably led to more frequent deliveries and smaller delivery batches, with resulting fragmentation of logistics flows (Fernie and Sparks, 2014). In turn, this has led to a dramatic growth of the quantity of data exchanged in cyber space and to an increase in the number of cyber violations. The Italian FMCG sector represents an appropriate context to be investigated given its international relevance. The Italian FMCG industry is placed among the top four markets in Europe for logistics flows and generated turnover, and it is one of the fastest-growing sectors across Europe, after Spain in 2016 (Nielsen, 2016). It is characterized by a level of fragmentation higher than other European markets, such as France, the UK, Spain and Germany (Fornari *et al.*, 2013). In this sector, it is possible to isolate a few major retailers that hold the majority of market shares, as seen in other principal European markets (source: Nielsen, 2019). Similarly to what has happened across Europe, over the past few decades the Italian FMCG supply chain has gone through a deep transformation, leading to the adoption of the principles of efficient consumer response (ECR) and IT technologies, such as electronic data interchange systems, along with tools for exchanging data and information over the internet.

We built our sample for our research according to the principles proposed by Punch (1998) when conducting an exploratory study. Firstly, we wanted to access as many organizations as possible in a reasonable timescale. Consistent with the scope and aim of our research, the names of the target organizations were retrieved from the database of the most important FMCG trade association in Italy, i.e. Indicod-ECR GS1 Italy (available at: https://gs1it.org/) and from the database of the most important trade association for logistics in Italy, i.e. Assologistica (available at: www.assologistica.it – focusing on those logistics providers operating in the FMCG sector). The questionnaire was distributed to 524 companies, with the following representation: 321 manufacturers, 134 logistics service providers and 69 retailers. Secondly, the authors' aim was

not to make substantial claims in the first instance about the generalizability of the sample, as suggested by Croom (2005).

Managers in charge of supply chain management or logistics are chosen as potential respondents for this survey as they are expected to be the most appropriate professionals that can provide a supply chain perspective to the analysis and to overcome the traditional silo approach that IT departments have in the management of cyber and information risks in the supply chain. Consequently, their perception is deemed to be very significant to this aim. Similar to Tsai *et al.* (2008) and Golgeci and Ponomarov (2013), we selected participants in such a way so that they can offer global insights and comprehensive perception. A minimum working experience of five years in the industry at the middle to senior management level was consequently included as a further respondent selection criterion as we thought that having already experienced the supply chain mechanisms and challenges of the sector would provide a better level of understanding and a more pertinent perception of risks.

After contacting the organizations included in the sample database, 112 full questionnaires were returned and this constitutes the database of the final sample analysed, representing 21.4% of the overall target population. According to exploratory studies, such as the one presented by Croom (2005), this response rate provides a sufficiently significant sample to draw some insights about the study's representativeness.

Consistently with the adopted research methodology, we designed our data collection instrument in the form of a survey questionnaire. The questionnaire was developed with the aim to allow the collection of data able to provide an answer to the research questions of the study. As the research questions aim to investigate the elements composing the managerial construct of CSCRM and the related perceptions of supply chain managers, we decided to rely on the outcomes of the literature review as building blocks for the survey questionnaire. In particular, we referred to the work by Ghadge *et al.* (2020) and main related literature contributions for exploring the constituents of the "sources of cyber risk" element and the constituents of the "measures to manage cyber risk" element. This work was complemented by the taxonomies presented by Colicchia *et al.* (2019) and main related literature contributions, which were used also for exploring the constituents of the "ownership of the CSCRM process" element along with the constituents of the "cyber and information risks" element (in terms of probability and impact of risks – which we further complemented by newly developing a set of items to ascertain the occurrence of those risks). Finally, we relied on the work by Lee and Whang (2000) and Lotfi *et al.* (2013) for deriving the constituents of the "categories of information shared in the supply chain" element. Appendix reports the questions composing our data collection instruments along with the linked theoretical underpinnings. The resulting questionnaire consisted of six different sections, which asked for information regarding the demographics of the respondents and related companies (to generate the groups of respondents composing the FMCG supply chain and empower the evaluations of the alignment of their perceptions), as well as the key elements of CSCRM previously described in the literature review (i.e. cyber risks, sources of risks, ownership of the CSCRM process, information exchanged in the supply chain, measures to manage cyber risks). The questions were measured by five-point Likert scales, ranging from "very relevant" to "not relevant", from "low impact" to "very high impact" (according to the assessment scale presented by Hallikas *et al.*, 2004) or from "very low probability" to "very high probability" (according to the assessment scale presented by Hallikas *et al.*, 2004). In this way, we ensured that the data collection instrument was capable of providing an answer to the research questions, i.e. assessing the perception of importance about the elements of CSCRM and evaluating the alignment of the recorded perceptions, based on the scores assigned by the respondents. The questionnaire was pre-tested in panel sessions with a sample of 10 senior academics and 13 industry professionals. The industry professionals were represented by supply chain managers and IT managers and Chief Information Officers, to ascertain that the "IT side" of the questions was also sufficiently precise and compliant with the technicalities. The panel members provided valuable comments and feedback that were incorporated into the final version of the survey questionnaire. It is worthwhile underlining that none of the panel members (industry professionals or academics) took part in the actual survey. We also conducted a pilot study before administering the questionnaire to the entire sample. The pilot study aimed to cross-verify the content, architecture and nature of the questions and enhance its validity (Mitchell, 1996). The pilot study was carried out through the administration of the questionnaire to 10 organizations. The collected responses and related data are not included in this paper as the pilot phase was undertaken with the aim to refine and validate the research instrument rather than to collect field evidence.

Given the objective of this study, which intends to examine the perceptions of supply chain managers operating in the FMCG supply chain, we decided to rely on a data analysis tool that allows for investigating differences among groups of data (Bourlakis *et al.*, 2014). For this reason, we decided to analyse the responses to our survey questionnaire through a one-way analysis of variance (ANOVA), carried out with the precise aim to assess the differences in the responses obtained from the various categories of respondents in the FMCG supply chain, as indicated above (Manufacturers, Logistics Service Providers and Retailers). ANOVA is a well-established statistical method which complies with our research requirements and that has been adopted in many scientific contributions focused on the analysis of supply chains (Greer and Ford, 2009 and Lai *et al.*, 2004). This method implies that a set of tests are performed on the variance of a population and the variability of results is scrutinized with reference to differences between groups (Dobroszek, 2020). The one-way ANOVA served to compare averages in groups and it was used to test the relevance of variations in the perceptions about CSCRM of the surveyed supply chain managers. As it is customary in similar studies (Zhu *et al.*, 2007; Bourlakis *et al.*, 2014), we adopted a p-value equal to 0.05 as a threshold for discriminating the statistical significance of differences in the responses among the groups of respondents in our survey (Manufacturers, Logistics Service Providers and Retailers). For each item composing our measurement scale (i.e. our questionnaire), we studied the mean value and the standard deviation value of the responses, subdivided in the three groups of supply chain players of the

FMCG sector. We performed the ANOVA test to derive the F-statistics value, which, with a significance level of 5%, was compared to the value of F-crit. If the F-statistics value was higher than the F-crit value and the *p*-value was lower than 5%, then the null hypothesis (i.e. data from all groups are characterized by the same stochastic distribution) was rejected and significant differences among the groups of respondents were detected. Otherwise, no significant difference in the perception of supply chain managers was recorded. Based on the outcomes of the ANOVA tests, carried out for each item of the survey questionnaire, considerations on the level of alignment of perceptions about CSCRM across the FMCG supply chains were drawn, discussed and interpreted.

4. Results from the survey study

In the present section, the results of the survey study on the selected sample of companies operating in the FMCG supply chain in Italy are shown. The items analysed regard the main components of the CSCRM process, as outlined in the literature review.

4.1 Profile of the respondents' sample

Out of 112 participants in the survey, 64 are manufacturers, 31 logistics service providers and 17 retailers. The composition of the final sample of participants reflects the composition of the FMCG sector in Italy very well, where there is a concentration around few players in the retail stage compared to the manufacturing stage (source: Nielsen, 2019).

4.2 Perception of the risk events

We first studied the perception of the respondents regarding risk events. In Table 4, we report the mean, standard deviation and F-statistics values of the responses in relation to the probability, impact and occurrence of the events.

The mean and standard deviation values, along with the F-statistics results, show a certain alignment of the perception of the risk events across the FMCG supply chain. In fact, the mean values of the surveyed items show similar results across the groups (see, for example, the score of the probability of the item "crash of website", which is equal to 1.67, 1.61 and 1.71, respectively, for Manufacturers, Logistics Service Providers and Retailers). In general, the value of F-statistics is below the threshold of the critical value for almost all the items and this confirms the substantial alignment of the entire sample.

More in details, it emerges that impact shows higher values of perception compared to probability. In terms of occurrence, it seems that the whole FMCG supply chain has experienced the same risk events, as the same categories of risk events have been unanimously perceived in the same way by the groups of respondents as shown in the table, i.e. similar mean values across the groups and low values of the F-statistics.

There is an almost unanimous consensus around the two events considered to be the most dangerous ones (i.e. ERP malfunction and lack of connectivity – with the highest mean scores across the groups of respondents). These risk events seem to be the ones that also have occurred most recently (with mean scores of ERP malfunction equal to 3.07, 2.90 and 2.87, respectively, for Manufacturers, Logistics Service Providers and Retailers; and mean values of lack of connectivity equal to 3.44, 3.27 and 3.46, respectively, for Manufacturers, Logistics Service Providers and Retailers). Malware has been judged to be a high risk, especially by retailers, who assigned higher scores to probability (mean value = 2.24), impact (mean value = 3.88) and occurrence (mean value = 2.87) of this event compared to the scores assigned by the other groups. This is most probably due to the fact that they have occurred relatively recently and because retailers are possibly more likely to be the target of these attacks from external sources, given their direct presence in the consumer market. The only divergence in the perception of the risk events shown by the F-statistics regard data breach in terms of impact, which seems to be perceived as a real threat by the upstream stages of the supply chain, with a decreasing perception as we move down the chain (3.34, 3.19 and 2.47, respectively, for Manufacturers, Logistics Service Providers and Retailers). The same trend can be highlighted for the occurrence of this risk event, even if with smaller differences among the values of the sample (1.62, 1.33 and 1.25, respectively, for Manufacturers, Logistics Service Providers and Retailers).

The previous observation leads one to suppose that there is a potential relationship among the studied variables (i.e. probability and impact against occurrence). To isolate potential trends and behaviours, we built a bubble diagram analysis (Figure 1). The Bubble diagram reports the mean values of the three variables for each assessed risk event: impact (vertical axis), probability (horizontal axis) and occurrence (bubble diameter, i.e. the larger the bubble diameter, the more recently the risk event has occurred).

The bubble diagrams show that the occurrence affects the perception of the level of riskiness of the evaluated events, especially in terms of impact. While the mean values of probability are aligned around medium-low values, impact values vary significantly and increase consistently with the occurrence of the events, i.e. larger bubbles (those events with high occurrence) are positioned in the upper side of the charts (the one corresponding to high impact values) and *vice versa*. In other words, it appears that for those events that have actually and recently occurred, companies are well-aware of the impact of incidents. On the contrary, for those events that have not happened, companies perceive a smaller impact, which may occur because companies cannot assess what effects those events could have. It is reasonable to think that if companies had been aware of the actual consequences deriving from an incident (and measured them), these risk events would have been assigned higher impact scores. By looking at the FMCG supply chain, it seems that this tendency is stronger as we move down the chain, with Retailers showing a clear difference between the cluster of events that have occurred (with greater impact values) and the cluster of events that have seldom or never occurred (with smaller impact values).

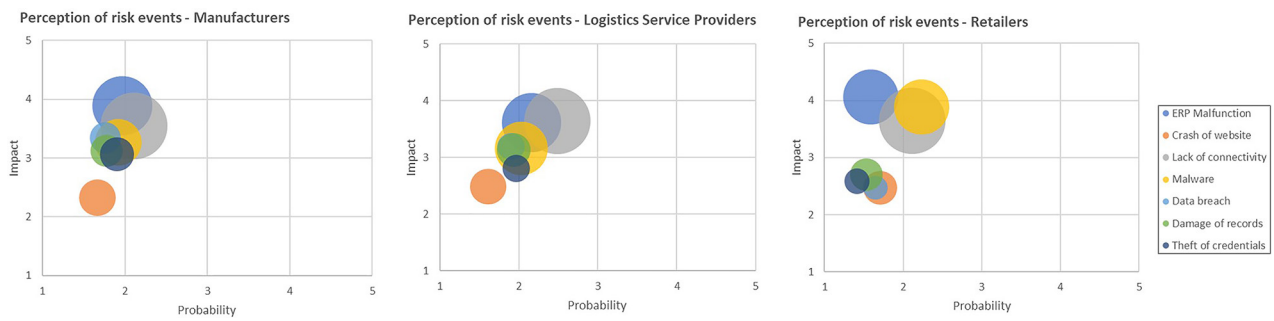
Another interesting insight emerges from an overall comparison of the charts. It appears that Manufacturers are more centred around the mean values of probability and Retailers are biased towards a lower score given to the probability and impact of risk events that have not occurred. Logistics Service Providers seem to have a broader view that spans across the different values assigned to the probability and impact of the various risk events more uniformly and

Table 4 Perception of risk events in terms of probability and impact and occurrence of incidents

	Manufacturers		Logistics service providers		Retailers		ANOVA
	Mean	St. dev.	Mean	St. dev.	Mean	St. dev.	*F*-statistics
Probability							
ERP malfunction	1.97	1.06	2.16	1.00	1.59	0.87	1.70
Crash of website	1.67	0.74	1.61	0.80	1.71	0.92	0.07
Lack of connectivity	2.11	0.92	2.48	0.96	2.12	0.93	1.98
Malware	1.92	0.92	2.03	0.80	2.24	1.03	1.01
Data breach	1.76	0.96	1.90	0.94	1.65	0.93	0.48
Damage of records	1.78	0.87	1.94	1.09	1.53	0.72	1.08
Theft of credentials	1.90	1.12	1.97	0.98	1.41	0.80	1.68
Impact							
ERP malfunction	3.89	1.16	3.61	1.38	4.06	1.14	0.86
Crash of website	2.33	1.37	2.48	1.39	2.47	1.46	0.16
Lack of connectivity	3.55	1.38	3.65	1.14	3.65	1.22	0.08
Malware	3.27	1.24	3.16	1.13	3.88	0.99	2.29
Data breach	3.34	1.21	3.19	1.38	2.47	1.42	3.08*
Damage of records	3.13	1.16	3.13	1.34	2.71	1.26	0.85
Theft of credentials	3.06	1.33	2.81	1.35	2.59	1.33	1.00
Occurrence							
ERP malfunction	3.07	1.37	2.90	1.56	2.87	1.52	0.21
Crash of website	1.88	1.07	1.77	1.01	1.76	0.77	0.15
Lack of connectivity	3.44	1.09	3.27	1.36	3.46	1.29	0.24
Malware	2.42	1.20	2.62	1.26	2.87	1.38	0.94
Data breach	1.62	0.94	1.33	0.31	1.25	0.21	2.68
Damage of records	1.66	1.02	1.65	0.99	1.69	0.98	0.01
Theft of credentials	1.74	1.08	1.37	0.38	1.32	0.30	2.79

Note: $^{*}p < 0.05$

Figure 1 Bubble chart linking the perception of the risk events (probability and impact) to the occurrence of incidents



consistently. It appears that their perception is a sort of compromise between the two different approaches shown by Manufacturers and Retailers.

4.3 Perception of the sources of risk

Table 5 shows the perception related to the sources of risk, subdivided according to the three different categories of actors in the FMCG supply chain. The mean, related standard deviation and F-statistics values are reported.

Also, as far as the sources of risks are concerned, the values of F-statistics show a certain degree of alignment of perceptions across the FMCG supply chain: these values are below the threshold of F-crit for almost all the items and this confirms the substantial alignment of the entire sample.

However, it appears that Retailers have a generally weaker perception of the sources of cyber and information risks in their supply chain showing lower mean values compared to the other groups in all categories of surveyed items (e.g. Malicious – Former suppliers with values equal to 2.41, 2.37 and 2.12, respectively, for Manufacturers, Logistics Service Providers and Retailers; Non-intentional – Former employees with values equal to 2.30, 2.37 and 1.71, respectively, for Manufacturers, Logistics Service Providers and Retailers). It is interesting to note that in all categories, Hackers are seen as the most dangerous source of risk,

Table 5 Perception of the sources of risk

	Sources of risk	Manufacturers		Logistics service providers		Retailers		ANOVA
		Mean	St. dev.	Mean	St. dev.	Mean	St. dev.	*F*-statistics
Malicious	Current employees	2.48	1.40	2.77	1.38	2.65	1.37	0.36
	Former employees	2.86	1.46	2.93	1.39	2.47	1.18	0.43
	Suppliers	2.27	1.18	2.37	1.22	2.35	1.00	0.07
	Former suppliers	2.41	1.29	2.37	1.38	2.12	1.11	0.26
	Customers	2.06	1.11	2.37	1.35	1.82	1.07	0.92
	Industrial espionage	2.94	1.52	2.97	1.45	3.00	1.54	0.04
	Hackers/Hacktivists	3.41	1.42	3.63	1.35	3.41	1.46	0.12
Non-intentional	Current employees	3.10	1.40	2.80	1.61	2.82	1.55	0.55
	Former employees	2.30	1.38	2.37	1.30	1.71	1.21	1.27
	Suppliers	2.81	1.29	2.37	1.13	2.00	1.17	3.13*
	Customers	2.52	1.42	2.33	1.24	1.59	1.06	2.95
	Natural disasters	2.37	1.27	2.60	1.25	2.53	1.37	0.30
	Internal technical problems	2.84	1.30	3.07	1.26	2.59	1.18	0.47
	External technical problems	2.89	1.35	3.07	1.14	2.94	1.09	0.11

Note: $^{*}p < 0.05$

ranking first in all groups of respondents with mean values of 3.41, 3.63 and 3.41, respectively, for Manufacturers, Logistics Service Providers and Retailers. According to Manufacturers, current employees are the main unintentional source of risk (mean value = 3.10), followed by industrial espionage (mean value = 2.94) and external technical Problems (mean value = 2.89). In contrast, malicious attacks from former employees are seen as the fifth most important source of risk (mean value = 2.86). A similar perception is also shown by Logistics Service Providers, with internal and external technical problems as other main sources (mean values = 3.07 for both sources of risk), followed by industrial espionage (mean value = 2.97) and malicious attacks from former employees (mean value = 2.93). Retailers, too, show a very similar perception compared to that of Manufacturers, with industrial espionage (mean value = 3.00), external technical problems (mean value = 2.94) and unintentional and intentional actions by current employees (mean value = 2.82 and mean value = 2.65, respectively) as main sources. It seems that, besides terrorism, the "human factor" and the "enemy within" are common threats to all categories of organizations in the FMCG supply chain, along with malicious actions coming from unfair competition. The role of the human factor as a source of risk in the supply chain appears to be quite significant, especially for manufacturers, who also see suppliers and customers as potential non-intentional sources of risk (with mean values equal to 2.81 and 2.52, respectively), probably due to intellectual property violation incidents. This perception fades as we move down the chain from Manufacturers to Logistics Service Providers to Retailers and is underlined by a high value of the F-statistics that shows a certain divergence in the perception of the different players (i.e. non-intentional – suppliers F-statistics is above the threshold of the critical value). Natural events are perceived as less threatening by the sample. It is interesting to note that Logistics Service Providers seem to perceive technical reasons as one of the main causes of risks for their business continuity, as explained above, and this shows fairly well their interest in securing their cyber supply chain from the technical side, across the boundaries of their organization and beyond the dyad.

4.4 Involvement of the organization's departments in cyber and information risk management

As far as the involvement of the various departments in the CSCRM process is regarded (Table 6), it appears that the IT department is the most involved one, across all categories of players in the FMCG supply chain (with mean values equal to 4.46, 4.37 and 4.82, respectively, for Manufacturers, Logistics Service Providers and Retailers). Top management and the risk management department are also felt to be important in the CSCRM process and this applies to all categories of actors of the supply chain.

As far as the supply chain department is concerned, respondents across the FMCG sector are quite aligned in stating the importance of the involvement of such department (mean values equal to 3.14, 2.90 and 3.00, respectively, for Manufacturers, Logistics Service Providers and Retailers with a low value of the F-statistics). However, it is not seen as a leading function and, equally as it is not seen as one of the top three areas to manage CSCRM, except for Manufacturers. They place the supply chain department in the third position, while Logistics Service Providers place it in fifth and Retailers in fourth. This could lead to miscommunications across organizations in the sharing of plans and policies across the supply chain, given the different levels of involvement perceived in relation to the various departments. Given the top scores received, it emerges that the CSCRM process is still the domain of the IT department everywhere.

What is surprising about these responses is the very low score allocated to the human resources (mean values equal to 2.43, 2.60, 1.94, respectively, for Manufacturers, Logistics Service Providers and Retailers) and the Legal Department (mean values equal to 2.71, 2.87, 2.53, respectively, for Manufacturers, Logistics Service Providers and Retailers). Taking into account also the importance of the "human factor" as one of the key sources of cyber risk (see above) and the enforcement of the GDPR, it is now necessary for all departments to be able to manage data and information appropriately. Human resources and legal departments should be able to comply with this, in particular because their staff often manages a great deal of sensitive information.

Table 6 Perception of the involvement of various business departments

Departments	Manufacturers		Logistics service providers		Retailers		ANOVA
	Mean	St. dev.	Mean	St. dev.	Mean	St. dev.	*F*-statistics
Top management	3.05	1.35	3.40	1.35	3.06	1.52	0.43
IT department	4.46	1.01	4.37	1.13	4.82	0.53	1.52
Operations	2.98	1.08	2.83	1.49	2.65	1.54	0.44
Supply chain/logistics	3.14	1.19	2.90	1.30	3.00	1.46	0.50
Finance	2.83	1.30	3.13	1.31	3.06	1.43	0.50
Risk management	3.25	1.60	3.10	1.56	2.94	1.52	0.27
Legal department	2.71	1.54	2.87	1.36	2.53	1.37	0.15
Human resources	2.43	1.25	2.60	1.19	1.94	1.25	1.18

4.5 Perception of the criticality of the information shared across the supply chain

This section analyses how important it is to protect each category of information according to each player across the FMCG supply chain (Table 7).

It is interesting to note that the level of importance given to the protection of the various categories of information exchanged in the FMCG supply chain varies quite significantly across the different stages and is related to the core activities of each player. As one would expect, Manufacturers seem more concentrated on the master data (mean value = 3.22) and invoicing side (mean value = 3.41), along with data about their sales (mean value = 3.17). Retailers seem focused on the discounts and promotional data (mean value = 3.18) along with inventory (mean value = 3.00), as these represent one of the main levers to their competitive advantage. Logistics Service Providers seem to be mainly focused on transport data (mean value = 3.48) and present a balanced profile in terms of importance given to the exchanged data of both the upstream and downstream sides of the supply chain, with generally high scores assigned to the various items. The high F-statistics values that are above the threshold of the critical value show that the great relevance of master data (F-statistics value = 4.75) and transport rates (F-statistics value = 9.90), assigned, respectively, by Manufacturers and Logistics Service Providers, is not confirmed by the other players of the supply chain. On the other hand, the high importance assigned by Retailers to discounts and promotional plans is associated to the lowest value of F-statistics (value = 0.04), which means that the other players in the supply chain also agree on the level of sensitivity of these data to protect. Low mean values are assigned to those data customarily shared across a supply chain (e.g. delivery tracking, with mean values equal to 2.11, 2.58 and 2.29, respectively, for Manufacturers, Logistics Service Providers and Retailers).

4.6 Perception of the countermeasures and actions for mitigating cyber risks

Table 8 shows the level of perception regarding the initiatives and countermeasures for managing cyber risks in the supply chain, subdivided according to the different categories of players.

It emerges that the IT technical side is still dominant in every stage of the FMCG supply chain (as shown by the high scores assigned by the groups of respondents to those initiatives falling into the internal IT security and resilience tools, e.g. intrusion prevention systems (IPS) with mean values equal to 4.75, 4.83 and 4.67, respectively, for Manufacturers, Logistics Service Providers and Retailers). However, as highlighted by the values of the F-statistics, there is no unanimous consensus regarding some technical measures, such as multiple data backup (F-statistics value = 4.32) and geographically distributed datacentres (F-statistics value = 9.38). These initiatives are perceived as very important by Logistics Service Providers (mean values = 4.75 in both cases), consistently with the strong perception of technical problems' riskiness, whose business continuity is strongly dependent on the availability and accessibility of data.

At the organizational level, considerable importance is given to the presence of an information security strategy that should drive the design and implementation of initiatives for CSCRM (mean values equal to 4.50, 4.50 and 4.67, respectively, for Manufacturers, Logistics Service Providers and Retailers). On the other hand, those initiatives that regard the so-called

Table 7 Perception of the criticality of various categories of information shared across the FMCG supply chain

Information categories	Manufacturers		Logistics service providers		Retailers		ANOVA
	Mean	St. dev.	Mean	St. dev.	Mean	St. dev.	*F*-statistics
Master data	3.22	1.23	3.00	1.26	2.18	1.24	4.75*
Sales data and forecasts	3.17	1.18	3.00	1.32	2.65	1.32	1.24
Invoices	3.41	1.14	3.26	1.24	2.82	1.59	1.49
Discounts and promotional plans	3.08	1.35	3.06	1.59	3.18	1.59	0.04
Inventory	2.45	1.17	2.87	1.36	3.00	1.70	1.77
Production plans	2.50	1.23	2.55	1.36	2.18	1.13	0.54
Delivery tracking	2.11	1.10	2.58	1.39	2.29	1.61	1.45
Transport rates and logistics costs	2.52	1.14	3.48	1.52	1.94	1.09	9.90*

Note: $^{*}p < 0.05$

Table 8 Perception of the initiatives and countermeasures to mitigate cyber risks

Initiatives	Type of initiative		Manufacturers Mean	Manufacturers St. dev.	Logistics service providers Mean	Logistics service providers St. dev.	Retailers Mean	Retailers St. dev.	ANOVA *F*-statistics
Employ a CISO or DPO	Internal organizational initiatives	Pre-attack	3.14	1.46	3.40	1.35	3.18	1.47	0.18
Conduct personnel background checks	Internal organizational initiatives	Pre-attack	2.62	1.28	2.93	1.14	2.76	1.35	0.47
Presence of an information security strategy	Internal organizational initiatives	Pre-attack	4.50	0.80	4.50	0.84	4.67	0.58	0.06
Specific data and information insurance	Internal organizational initiatives	Post-attack	3.33	1.63	4.00	0.82	4.00	1.00	1.19
Employee security awareness training programme (cyber hygiene)	Training and internal awareness	Pre-attack	3.48	1.19	3.73	1.14	3.29	1.49	0.37
Secure data access and control measures	Internal data management	Pre-attack	3.67	1.23	3.50	0.55	2.00	1.73	2.53
Accurate record of personnel handling sensitive data	Internal data management	Pre- and trans-attack	3.58	1.16	3.83	0.41	3.00	1.73	0.58
IPS, data and URL filtering (antivirus and antispam)	Internal IT security and resilience tools	Pre-attack	4.75	0.62	4.83	0.41	4.67	0.58	0.09
Multiple data backup	Internal IT security and resilience tools	Pre-attack	4.16	0.75	4.75	0.61	3.33	0.58	4.32*
Geographical distributed data centres	Internal IT security and resilience tools	Pre-attack	3.67	1.21	4.75	0.52	2.00	0.42	9.38*
Require suppliers and customers to comply with the privacy and security policies	Compliance and external awareness	Pre-attack	3.43	1.25	3.77	1.19	3.65	1.00	0.61
Conduct supply chain partners security audits	Compliance and external awareness	Pre-attack	3.35	1.31	3.57	1.22	3.47	1.33	0.19
Communication procedures with involved supply chain partners	External event management	Trans- and post-attack	3.67	0.89	4.17	0.75	3.00	1.73	1.43
Business continuity and disaster recovery plans	External event management	Trans- and post-attack	4.67	0.52	4.75	0.80	4.33	0.58	1.19

Note: $^{*}p < 0.05$

"human factor" are perceived as less critical, with no significant differences among Manufacturers, Logistics Service Providers and Retailers. There is less importance given to initiatives such as controls on employees (mean values equal to 2.62, 2.93 and 2.76, respectively, for Manufacturers, Logistics Service Providers and Retailers), notwithstanding a great deal of danger allocated to the human factor as a source of risk events.

It is interesting to note that in relation to those initiatives that regard the supply chain side (such as the adoption of security policies along the supply chain, the conduction of audits, the adoption of communication procedures with suppliers and customers in case of incidents and business continuity actions) the sample is almost entirely aligned in recognizing the importance of such countermeasures, with high scores assigned to these measures (e.g. business continuity and disaster recovery plan with mean values equal to 4.67, 4.75, 4.33, respectively, for Manufacturers, Logistics Service Providers and Retailers). This applies to all-time phases for the mitigation of cyber risks (i.e. pre-, trans-, and post-attack). However, it seems that Logistics Service Providers perceive as even more urgent the opportunity to adopt these initiatives that span across the supply chain. Logistics Service Providers have assigned all items falling in the categories of compliance and external awareness and external event management higher scores compared to the values assigned by the other groups of respondents (e.g. communication procedures with mean value equal to 4.17 for Logistics Service Providers compared to mean values equal to 3.67 and 3.00 for Manufacturers and Retailers, respectively). Logistics Service Providers appear to be more inclined to look beyond the boundaries of their organization and to search for measures that can support the CSCRM process along the upstream and downstream supply chain and beyond the dyad.

Overall, it appears that Retailers show a weaker perception of the importance of the various initiatives, with lower mean values assigned to almost all items in all categories compared to the other groups of respondents.

5. Discussion

An overview of our survey results allows for generating interesting insights on the main dimensions of the analysis carried out, as shown in Table 8, which reports in an aggregated fashion the results of the survey and qualitatively classifies them to elaborate and interpret the outcomes of the analysis.

First of all, by looking at the perceived relevance of the different elements composing CSCRM across the whole sample, it appears that our respondents confirm the significance of the investigated topic (i.e. no element has been assigned an overall low value of relevance). It is interesting to note that among the elements, high relevance is assigned to initiatives and countermeasures and medium-high relevance to the involved business departments, impacts of risk events and information shared: this shows that respondents think that taking actions towards CSCRM is essential to secure the information shared across the supply chain and that this should involve the business departments within the organization to confront the effects that risk events can have on business operations. In terms of alignment of perceptions, also, in this case, an overall medium-high level of alignment is confirmed by the responses across the whole sample and for all the CSCRM elements. However, the only elements that show a medium level of alignment are related to information shared and to initiatives and countermeasures. This suggests that, notwithstanding the strong perception of the sample about these elements in terms of relevance, some items are perceived differently by the groups of respondents (i.e. Manufacturers, Logistics Service Providers and Retailers).

More in details, as far as the perceptions of risk events are concerned, it appears that impacts on business are seen as more relevant than probability, which confirms the empirical evidence discussed by Colicchia *et al.* (2019). Even though all categories of players in the FMCG supply chain reported a similar occurrence of the different investigated risk events and related incidents, it seems that Logistics Service Providers have a broader perception of the risk events compared to Manufacturers and Retailers. Their focus spans in a way that appears to combine Manufacturers' and Retailers' attitudes towards risk – see also Figure 1, where the bubbles in the Logistics Service Providers' chart are spread across the area from left to right. In contrast, the charts of Manufacturers and Retailers show more concentrated bubbles. The concurrent examination of the perception of the impact of the risk events along with their probability and the actual occurrence of those events also raises the important concern related to the effect of incident awareness on the perception of risk, something that has been widely discussed in the literature. For example, Volpentesta *et al.* (2011) discuss the positive impact for organizations of incident reporting to generate widespread awareness in their employees, which can affect perceptions and, in turn, drive more coordinated actions in terms of information security policies and strategies. Our analysis seems to confirm the link between occurrence and perception, as it appears that those risks with higher occurrence are perceived more vividly compared to other risk with lower values of occurrence and this might be due also to the way incidents are reported within single organizations but also across the supply chain. It seems that little awareness leads to underestimating the importance of risk events (and the other way around). This leads to inferring that there should be a clear policy regarding incident reporting and management to build a correct level of awareness on cyber threats and risk events in organizations, which is consistent with the findings of Volpentesta *et al.* (2011). Other authors refer to this as "shared knowledge" or "mutually created knowledge" (Tao *et al.*, 2016; Scholten and Schilder, 2015), and this "knowledge" becomes more and more effective in building resilience when widely shared not only across the departments of the single organizations but along the whole chain of supply (Radanliev *et al.*, 2020).

As far as the sources of risk are concerned, it is interesting to note that the so-called "human factor" is seen as one of the predominant threats to cyber security in supply chains and this is in line with previous literature (Ghadge *et al.*, 2020). Surprisingly, if looked at concurrently with the perception of the other elements of CSCRM that regard human resources within the business operations, as it will be discussed in the following paragraphs, departments and initiatives related to human resources are perceived as less important compared to other items of the same categories. It appears that all groups of players of the FMCG supply chain give smaller importance to those countermeasures aimed at dealing with the human factor as a source of risk and this is something that seems contradictory and which companies should address, as suggested by the existing literature (Smith *et al.*, 2007; Boyson, 2014; Windelberg, 2016). It also seems that Logistics Service Providers are more concerned about technical problems that could undermine the continuity of their business operations – a fear that is consistent with their role as a critical link in the FMCG supply chain between Manufacturers and Retailers.

As far as the ownership of the CSCRM process is concerned, it appears that, from an overall perspective, the medium-high scores assigned to the majority of the business departments indicate that respondents recognize the importance of involving different business departments in the CSCRM process, in line with the literature (Trombley, 2015; Boone, 2017). Existing studies suggest that CSCRM should be organization-wide and not "silo-focused". However, our results show that the IT department emerges as the owner of the process according to all categories of players. This is something that one could expect, but it looks in contrast with the literature that suggests that cyber security should be led from the top (Boone, 2017). A striking finding is that the human resources department is at the bottom of the list and this again shows a contradiction in terms of approach to the "human factor" in the CSCRM process: if this is perceived as one of the most critical sources of risk, then the department dealing with human resources should be involved much more in the CSCRM process and the perception of its relevance should be stronger. Likewise, the supply chain department is not perceived as one of the top departments that should own or lead the CSCRM process for driving a supply chain view into the CSCRM process – so that the other involved departments could benefit from a perspective that goes beyond the boundaries of the organization and desirably beyond the dyad or Tier 1.

The concurrent view of the perception of the level of criticality of the different categories of information shared across a supply chain shows a certain degree of awareness that

protecting the whole range of information shared across the supply chain is critical, as demonstrated by the scores assigned by our respondents (Tables 7 and 9). This seems in contrast with the existing literature, which posits that information leakages are not perceived as a security risk by organizations (Tran *et al.*, 2016). As it emerges from Table 7, while all the respondents recognize the relevance of some information (e.g. invoices), it seems that different groups of respondents focus on different categories of information shared, and in particular, on those types of information that are more specific and critical for their stage of the supply chain and the continuity of their business operations: Manufacturers focus on sales, invoices and master data; Logistics Service Providers put transport data in the first place, but they also give a balanced level of weight to the majority of the information exchanged; Retailers, instead, seem to focus more on the downstream side of the supply chain and related exchanged data, including discounts and promotional plans and inventory. So, once more, it appears that Logistics Service Providers can play a role as a bridge connecting the views of Manufacturers and Retailers. This is in line with previous literature, which affirms that Logistics Service Providers are in the middle of relationships among the partners of a supply chain and they can foster collaboration across the supply chain (Zacharia *et al.*, 2011; Sanchez Rodrigues *et al.*, 2015). However, this view has not been applied to the context of supply chain risk management or CSCRM yet. Furthermore, our results suggest that the role of Logistics Service Providers can be critical not only for promoting collaboration but also for driving alignment for a consistent approach to CSCRM across the supply chain – eventually contributing to coordinated investments in information security in a networked environment (Bandyopadhyay *et al.*, 2010; Li and Xu, 2020).

As far as the countermeasures to mitigating cyber risks are concerned, Table 9 reports an overall high level of relevance assigned to the set of initiatives but a medium level of alignment of the respondents' perceptions related to them. Also, in this case, the collected evidence seems to indicate that, while there is an overall awareness of the importance of taking actions to tackle cyber risks, Retailers have a generally weaker perception about the countermeasures (Table 8). This is probably due to their position in the supply chain: the literature affirms that a large number of players in the upstream side of their supply chain makes it complicated to implement measures other than internal actions on the internal IT and organizational sides (Colicchia *et al.*, 2019). Instead, it emerges that Logistics Service Providers perceive protection initiatives as potential tools to drive supply chain actions given the level of importance allocated to those initiatives that go beyond the boundaries of the single organizations. This constitutes interesting evidence as the literature has found that organizations are usually more concentrated on those actions that instead seldom go beyond the focal firm or the dyad in the best case (Colicchia *et al.*, 2019). Perceiving those initiatives as very important shows a significant level of awareness by Logistics Service Providers about the necessity to go beyond the traditional view of risk management as a "business-related" process rather than as a "supply chain" issue. If we analyse the countermeasures according to the taxonomy presented by Ghadge *et al.* (2020), which distinguishes among pre-, trans- and post-attack countermeasures, it appears that the level of importance given to the different initiatives does not depend on the time phase of the actions themselves. Our respondents have allocated considerable relevance to pre-attack but also trans- and post-attack measures, assigning high scores to the perception of their importance. On the contrary, the literature shows little focus on the trans-, and especially the post-attack, actions, while a better balance of proactive and reactive approaches to CSCRM would be opportune (Ghadge *et al.*, 2020). Eventually, this could also lead to better resilience in terms of preparedness and the ability to respond and maintain (Ribeiro and Barbosa-Povoa, 2018). Looking at the categories of actors in the FMCG supply chain, but taking for granted the importance allocated to those actions that fall in the category of IT technical initiatives, it seems that Logistics Service Providers are even more inclined towards a balance of proactive and reactive measures compared to Manufacturers and Retailers, especially as far as business continuity and event management actions are concerned. This leads to inferring that Logistics Service Providers could play an important role in the FMCG supply chain in promoting the adoption of initiatives for a proactive and reactive approach to CSCRM across the supply chain.

As discussed, it seems that, overall, a certain level of alignment of the perception about the elements composing the CSCRM process among the various actors of the FMCG supply chain exists, especially as far as the "classical" technical issues and actions are concerned. All the actors, in fact, seem to allocate a high level of importance to those elements. Instead, a certain misalignment seems to exist when the data exchanged in a supply chain is regarded. In this case, it appears that Manufacturers and Retailers are more focused on their domain rather than on the supply chain. On the contrary, it seems that Logistics Service Providers can overcome this limitation and have a broader perception of the risks, sources of risks and criticality of information and data exchanged that span across the different stages of the supply chain. This is also reflected in their attitude towards the various initiatives and countermeasures. While the technical area is still regarded as important, it seems that Logistics Service Providers emphasize the importance of external initiatives and initiatives that can balance proactive and reactive approaches to CSCRM. Consequently, it seems that the Logistics Service Providers could be promoters of a stronger supply chain approach to CSCRM in the FMCG industry. They could further improve the level of awareness of cyber risks across the whole chain (Volpentesta *et al.*, 2011; Linton *et al.*, 2014), with the creation of a common basis of shared knowledge that could also help in evaluating the level of riskiness of the supply chain (Colicchia *et al.*, 2019). In fact, according to the literature, it is important to have a coordinated approach to information sharing and information security across the supply chain, otherwise, the benefits of collaboration will be outweighed by the detrimental effect of misalignment in the protection initiatives (Bandyopadhyay *et al.*, 2010). As coordination can be challenging across the supply chain, a pivotal role would help drive alignment, coordination and integration for cyber resilience. The Logistics Service Providers could be the pivot of this process, leading to joint decisions and better coordination in the investments to be made in terms of cyber security, according to the literature (Li and Xu, 2020). This is also in

Table 9 Overview of the outcomes of the survey towards a cyber resilient supply chain

Elements of CSCRM	Perceived relevance	Alignment of perceptions	Highlights	How to build a cyber resilient supply chain	Main related literature
Cyber risks – probability	Medium-low	Medium-high	•Values of impact generally higher than probability	•Raise more awareness in terms of incidence occurrence to align perceptions (e.g. incident reporting policies)	Volpentesta *et al.* (2011); Scholten and Schilder (2015); Tao *et al.* (2016), Radanliev *et al.* (2020)
Cyber risks – impact	Medium-high	Medium-high	•Logistics Service Providers have a broader perception of the risk events		
Cyber risks – occurrence	Medium	Medium-high	•Higher occurrence values seem to influence the perception of impact values		
Sources of risk	Medium	High	•Stronger perception by Logistics Service Providers, playing a key role for the continuity of the entire supply chain •The "human factor" is perceived as one of the main threats	•Give more emphasis to those actions aimed at dealing with the "human factor" (e.g. protecting organizations from unintentional and malicious actions of employees)	Smith *et al.* (2007), Boyson (2014); Windelberg (2016), Ghadge *et al.* (2020)
Business departments	Medium-high	High	•The importance of involving different business departments is recognized •IT department seen as the most involved department by far, followed by top management •Supply chain/logistics dept are not seen as top departments •Human resources dept is not perceived as important to be involved	•Involve the HR dept to manage the "Human Factor" and the SC dept to drive a SC view into the CSCRM process	Trombley (2015), Boone (2017)
Information shared	Medium-high	Medium	•The relevance of some types of information is shared among all the participants (i.e. invoices) •Different groups of respondents focus on those types of information more related and critical to their business operations •Logistics service providers show a broader perception of the relevance of different types of shared information	•Leverage LSPs to combine the views of SC players on the types of information to protect and secure in the SC	Bandyopadhyay *et al.* (2010), Tran *et al.* (2016); Li and Xu (2020)
Initiatives and countermeasures	High	Medium	•Retailers show weaker perception, while Logistics Service Providers have a stronger perception of initiatives going beyond the boundaries of the single organization •Considerable relevance has been allocated to initiatives during the different phases of an incident (pre-attack, trans- and post-attack measures) •Notwithstanding the relevance assigned to the human factor, measures to tackle the "insider threat" (e.g. personnel background checks) are less perceived compared to other initiatives (e.g. IT security tools)	•Empower LSPs to act as a bringing link in the SC to drive risk appraisals across the chain and devise consistent security policies and investments (cyber supply chain balanced resilience)	Gualandris and Kalchschmidt (2015), Colicchia *et al.* (2019)

Notes: HR = Human resources; SC = supply chain; LSP = logistics service provider

line with the role of Logistics Service Providers in fostering collaboration across the supply chain, which has been recognized by previous research on supply chain collaboration initiatives (Zacharia *et al.*, 2011; Sanchez Rodrigues *et al.*, 2015). This pivotal role in driving alignment across the supply chain would allow for conducting appraisals to devise consistent security policies and CSCRM measures towards achieving the cyber supply chain balanced resilience (Gualandris and Kalchschmidt, 2015; Colicchia *et al.*, 2019).

6. Conclusions

In the present paper, we conducted an empirical analysis focused on the perception of supply chain managers working in the FMCG supply chain about the items composing the CSCRM process. This analysis aimed to shed light on the level of alignment of perception regarding CSCRM to understand what kind of policies, actions and initiatives should be undertaken to secure the entire supply chain, rather than just the single organizations. In doing this, we carried out an exploratory survey in the Italian FMCG supply chain.

As mentioned in the discussion of our findings, the outcomes of the survey allow understanding the perceptions of supply chain managers about the elements of CSCRM and the numerical results highlight those elements being perceived as the most important/relevant. In this way, we succeeded in providing an answer to *RQ1* (How relevant are the elements of CSCRM perceived by companies in a supply chain?). In doing this, we have segmented our analysis based on the groups of respondents identified in the FMCG supply chain (i.e. Manufacturers, Logistics Service Providers and Retailers) and this has permitted us to evaluate the level of alignment of the perceptions of supply chain managers across the board. In this way, an answer to *RQ2* (How aligned are the perceptions about CSCRM of companies in a supply chain?) was provided.

The work carried out has theoretical and practical implications.

In terms of theoretical implications, this study provides the scientific community with a vertical analysis of a supply chain, something that extends the existing theory on CSCRM, which only provides analyses of isolated and often disconnected cases and provides empirical data at a supply chain level. Besides going beyond the dyad, it also contributes to extending the current theory with the proposal of a paradigm that highlights the role of Logistics Service Providers as "orchestrators" of the CSCRM process. As a result, our study combines different existing classifications of CSCRM initiatives. It embraces the views of theories outside the traditional supply chain literature, such as the theory on information risk perception, to leverage the fundamental concept of alignment to achieve better cyber resilience. Our research also contributes to the theoretical debate regarding the role of the human factor in the management of risks in general and cyber and information risks, in particular, highlighting the necessity to embrace the perspective of people as critical elements to be leveraged for improving cyber resilience in the supply chain.

In terms of practical implications, our study provides the industrial community with an analysis of empirical data coming from a supply chain where the exchange of information in cyberspace is an essential process for adequately managing a large amount of generated logistics flows. It also provides the community of supply chain professionals with better awareness of the role of Logistics Service Providers in orchestrating the efforts towards the establishment of more "supply chain oriented" CSCRM policies. This could help practitioners streamlining the design of cyber security strategies and actions that could span across the different layers of the supply chain and allow for better alignment, resulting in better resilience and better visibility and more coordination of efforts. This, in turn, could mean more targeted/accurate investments in CSCRM initiatives in line with the concept of cyber supply chain balanced resilience. It also offers the industrial community an assessment of the level of importance given to the various items of the CSCRM process. It consequently unveils some elements of "common thinking" regarding risk management that could be a wake-up call for many organizations to overcome those traditional (and ineffective) approaches based on "firewalling themselves" from the IT technical perspective only. Our study also provides the industrial community with thought-provoking insights on the misalignment between the perceived relevance of the human factor as a source of risk (high) and the perceived importance of countermeasures to mitigate the risk events stemming from that source (low). This invites companies to rethink their approach to the mitigation of risks coming from employees. Finally, it also invites companies to assess their level of awareness about their supply chain's riskiness regarding the relationship between the occurrence of events and the perceived level of risk connected to those events. This could help organizations devise procedures and policies to report incidents and create common and shared knowledge about risks that could help them assess the level of risk in their supply chains more closely, moving beyond the boundaries of their companies.

Our study's main limitation lies in the relatively small sample analysed in our survey, which belongs to one supply chain only (i.e. the FMCG sector). This industry was selected as the object of the present investigation because of its great relevance in terms of economic impact, generated revenues and market size. As explained, it represents a very interesting field of investigation given the amount of shared data in the cyber space – so it constitutes a relevant testbed. Likewise, the Italian FMCG industry was selected because of its role in the European scenario, being the second fastest-growing market in the continent and being Italy one of the countries members of the Group of Seven (G7). Therefore, we believe that our empirical investigation's object provides results that are representative of the phenomenon under study. However, in terms of the generalizability of this research's outcomes, some of the findings are inevitably related to the industry investigated (e.g. the supply chain structure, which affects the architecture of the relationships among the various players operating in the industry). It would be interesting to apply the developed survey to other sectors, such as the pharmaceutical or automotive sectors, where data sensitivity is paramount and the level of complexity is extremely high. Additionally, it would be interesting to broaden the analysis by conducting more focused case studies to delve deeper into the mechanisms that Logistics Service Providers could put in place as "orchestrators" to foster the adoption of a supply chain perspective to CSCRM along the supply chain. It would be interesting to investigate the

motivations leading to certain CSCRM decisions, actions and outcomes. Another development of this study could be represented by comparing the perceptions of supply chain managers and IT managers/chief information officers to evaluate their level of alignment and the related consequences on the decisions made, the consequent actions undertaken and the level of resilience attained. A final direction for future research is represented by the investigation of the adoption of technologies such as Blockchain or distributed ledger systems as tools to mitigate cyber risks. These technologies could improve the CSCRM process outcomes, given their potential ability to secure transactions and data storage/transmission over different layers of the supply chain beyond the boundaries of the focal company.

References

Alter, S. and Sherer, S.A. (2004), "A general but readily adaptable model of information system risk", *Communications of the Association for Information Systems*, Vol. 14, pp. 1-28.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34 No. 3, pp. 613-643.

Bandyopadhyay, T., Jacob, V. and Raghunathan, S. (2010), "Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest", *Information Technology and Management*, Vol. 11 No. 1, pp. 7-23.

Bartol, N. (2014), "Cyber supply chain security practices DNA– filling in the puzzle using a diverse set of disciplines", *Technovation*, Vol. 34 No. 7, pp. 354-361.

Bateman, T. (2013), *Police Warning after Drug Traffickers' Cyber-Attack*, BBC News.

BCI (2019), "Cyber resilience report 2019", available at: www.thebci.org/index.php/obtain-the-cyber-resilience-report-2019

Bernstein, P.L. (1996), *Against the Gods: The Remarkable Story of Risk*, John Wiley, New York, NY.

Biener, C., Eling, M. and Wirfs, J.H. (2015), "Insurability of cyber risk: an empirical analysis", *The Geneva Papers on Risk and Insurance - Issues and Practice*, Vol. 40 No. 1, pp. 131-158.

Bloomberg.com (2017), *FedEx Cuts Profit Forecast on $300 Million Hit from Cyberattack*, available at: Bloomberg.com

Boone, A. (2017), "Cyber-security must be a C-suite priority", *Computer Fraud & Security*, Vol. 2017 No. 2, pp. 13-15.

Bourlakis, M., Maglaras, G., Gallear, D. and Fotopoulos, C. (2014), "Examining sustainability performance in the supply chain: the case of the Greek dairy sector", *Industrial Marketing Management*, Vol. 43 No. 1, pp. 56-66.

Bourlakis, M.A. and Weightman, P.W. (Eds) (2004), *Food Supply Chain Management*, Blackwell Pub.

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

Charitoudi, K. and Blyth, A.J.C. (2014), "An agent-based socio-technical approach to impact assessment for cyber defense", *Information Security Journal: A Global Perspective*, Vol. 23 Nos 4/6, pp. 125-136.

Clusit, (2017) "Clusit report. Clusit", available at: https://clusit.it/rapporto-clusit/

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

Colicchia, C., Creazza, A., Noè, C. and Strozzi, F. (2019), "Information sharing in supply chains: a review of risks and opportunities using the systematic literature network analysis (SLNA)", *Supply Chain Management: An International Journal*, Vol. 24 No. 1, pp. 5-21.

Croom, S.R. (2005), "The impact of e-business on supply chain management: an empirical study of key developments", *International Journal of Operations & Production Management*, Vol. 25 No. 1, pp. 55-73.

Deane, J.K., Ragsdale, C.T., Rakes, T.R. and Rees, L.P. (2009), "Managing supply chain risk and disruption from IT security incidents", *Operations Management Research*, Vol. 2 Nos 1/4, pp. 4-12.

Dobroszek, J. (2020), "Supply chain and logistics controller–two promising professions for supporting transparency in supply chain management", *Supply Chain Management: An International Journal*, Vol. 25 No. 5, pp. 505-519.

Eling, M. and Wirfs, J. (2019), "What are the actual costs of cyber risk events?", *European Journal of Operational Research*, Vol. 272 No. 3, pp. 1109-1119.

Ezhei, M. and Tork Ladani, B. (2018), "Interdependency analysis in security investment against strategic attacks", *Information Systems Frontiers*, Vol. 22 No. 1, pp. 187-201.

Faisal, M.N., Banwet, D.K. and Shankar, R. (2007), "Information risks management in supply chains: an assessment and mitigation framework", *Journal of Enterprise Information Management*, Vol. 20 No. 6, pp. 677-699.

Fernie, J. and Sparks, L. (2014), *Logistics and Retail Management: Emerging Issues and New Challenges in the Retail Supply Chain*, 4th ed., Kogan Page, London.

Fornari, E., Fornari, D., Grandi, S. and Menegatti, M. (2013), "The influence of retailing-mix levers on private label market share: the case of the Italian FMCG market", *Journal of Retailing and Consumer Services*, Vol. 20 No. 6, pp. 617-624.

Gattorna, J. and Jones, T. (Eds) (1998), *Strategic Supply Chain Alignment: best Practice in Supply Chain Management*, Gower Publishing Ltd.

Gaudenzi, B. and Siciliano, G. (2017), "Just do it. Managing IT and cyber risks to protect the value creation", *Journal of Promotion Management*, Vol. 23 No. 3, pp. 1-14.

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

Golgeci, I. and Ponomarov, Y.S. (2013), "Does firm innovativeness enable effective responses to supply chain disruptions? An empirical study", *Supply Chain Management: An International Journal*, Vol. 18 No. 6, pp. 604-617.

Gordon, S. and Ford, R. (2006), "On the definition and classification of cybercrime", *Journal in Computer Virology*, Vol. 2 No. 1, pp. 13-20.

Greer, B.M. and Ford, M.W. (2009), "Managing change in supply chains: a process comparison", *Journal of Business Logistics*, Vol. 30 No. 2, pp. 47-63.

Gualandris, J. and Kalchschmidt, M. (2015), "Supply risk management and competitive advantage: a misfit model", *The International Journal of Logistics Management*, Vol. 26 No. 3, pp. 459-478.

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V.M. and Tuominen, M. (2004), "Risk management processes in supplier networks", *International Journal of Production Economics*, Vol. 90 No. 1, pp. 47-58.

Ho, W., Zheng, T., Yildiz, H. and Talluri, S. (2015), "Supply chain risk management: a literature review", *International Journal of Production Research*, Vol. 53 No. 16, pp. 5031-5069.

Järveläinen, J. (2013), "IT incidents and business impacts: validating a framework for continuity management in information systems", *International Journal of Information Management*, Vol. 33 No. 3, pp. 583-590.

Jones, R.A. and Horowitz, B. (2012), "A system-aware cyber security architecture", *Systems Engineering*, Vol. 15 No. 2, pp. 225-240.

Jüttner, U., Peck, H. and Christopher, M. (2003), "Supply chain risk management: outlining an agenda for future research", *International Journal of Logistics Research and Applications*, Vol. 6 No. 4, pp. 197-210.

Keegan, C. (2014), "Cyber security in the supply chain: a perspective from the insurance industry", *Technovation*, Vol. 34 No. 7, pp. 380-381.

Khursheed, A., Kumar, M. and Sharma, M. (2016), "Security against cyber-attacks in food industry", *International Journal of Control Theory and Applications*, Vol. 9 No. 17, pp. 8623-8628.

Kim, K.C. and Im, I. (2014), "Research letter: issues of cyber supply chain security in Korea", *Technovation*, Vol. 34 No. 7, pp. 387-388.

Lai, K.H., Ngai, E.W.T. and Cheng, T.C.E. (2004), "An empirical study of supply chain performance in transport logistics", *International Journal of Production Economics*, Vol. 87 No. 3, pp. 321-331.

Lee, H.L. and Whang, S. (2000), "Information sharing in a supply chain", *International Journal of Technology Management*, Vol. 20 Nos 3/4, pp. 373-387.

Li, Y. and Xu, L. (2020), "Cybersecurity investments in a two-echelon supply chain with third-party risk propagation", *International Journal of Production Research*, Vol. 59 No. 4.

Linton, J.D., Boyson, S. and Aje, J. (2014), "The challenge of cyber supply chain security to research and practice – an introduction", *Technovation*, Vol. 34 No. 7, pp. 339-341.

Lotfi, Z., Mukhtar, M., Sahran, S. and Zadeh, A.T. (2013), "Information sharing in supply chain management", *Procedia Technology*, Vol. 11 No. 2, pp. 298-304.

Luiijf, E., Besseling, K. and de Graaf, P. (2013), "Nineteen national cyber security strategies", *International Journal of Critical Infrastructures*, Vol. 9 Nos 1/2, pp. 3-31.

Manuj, I. and Mentzer, J.T. (2008), "Global supply chain risk management strategies", *International Journal of Physical Distribution & Logistics Management*, Vol. 38 No. 3.

March, J.G. and Shapira, Z. (1987), "Managerial perspectives on risk and risk taking", *Management Science*, Vol. 33 No. 11, pp. 1404-1418.

Mitchell, V. (1996), "Assessing the reliability and validity of questionnaires: an empirical example", *Journal of Applied Management Studies*, Vol. 5 No. 2, pp. 199-208.

Momoh, O. (2016), "Supply chain attack", available at: www.investopedia.com/terms/s/supply-chain-attack.asp

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S.K. (2013), "Cyber-risk decision models: to insure IT or not?", *Decision Support Systems*, Vol. 56 No. 1, pp. 11-26.

National Cyber Security Centre, UK (2016), "Common cyber attacks: reducing the impact", available at: www.ncsc.gov.uk/white-papers/common-cyber-attacksreducing-impact (accessed 26 December 2019).

Nielsen (2016), "Nielsen growth reporter Q2 2016", available at: www.nielsen.com/uk/en/press-room/2016/Nielsen-growth-reporter-Q2-2016.html

Nielsen (2019), *Nielsen Growth Reporter Europe*, available at: www.nielsen.com/wp-content/uploads/sites/3/2019/04/2019-02-EU-Growth20Reporter20Q4202018-final.pdf

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

Pettit, T.J., Croxton, K.L. and Fiksel, J. (2013), "Ensuring supply chain resilience: development and implementation of an assessment tool", *Journal of Business Logistics*, Vol. 34 No. 1, pp. 46-76.

Punch, K.F. (1998), *Introduction to Social Research: Quantitative and Qualitative Approaches*, Sage Publications, London.

Radanliev, P., De Roure, D., Page, K., Nurse, J.R., Mantilla Montalvo, R., Santos, O., Maddox, L. and Burnap, P. (2020), "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains", *Cybersecurity*, Vol. 3 No. 1, pp. 1-21.

Ribeiro, J.P. and Barbosa-Povoa, A. (2018), "Supply chain resilience: definitions and quantitative modelling approaches – a literature review", *Computers & Industrial Engineering*, Vol. 115, pp. 109-122.

Rogers, R. (1983), "Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation", In Cacioppo, J. and Petty R. (Eds) *Social Psychophysiology: A Sourcebook*, Guilford Press, New York, NY, pp. 153-176.

Sanchez Rodrigues, V., Harris, I. and Mason, R. (2015), "Horizontal logistics collaboration for enhanced supply chain performance: an international retail perspective", *Supply Chain Management: An International Journal*, Vol. 20 No. 6, pp. 631-647.

Scholten, K. and Schilder, S. (2015), "The role of collaboration in supply chain resilience", *Supply Chain Management: An International Journal*, Vol. 20 No. 4, pp. 471-484.

Secci, S. and Murugesan, S. (2014), "Cloud networks: enhancing performance and resiliency", *Computer*, Vol. 47 No. 10, pp. 82-85.

Sharma, S. and Routroy, S. (2016), "Modelling information risk in supply chain using Bayesian networks", *Journal of Enterprise Information Management*, Vol. 29 No. 2, pp. 238-254.

Sindhuja, P. (2014), "Impact of information security initiatives on supply chain performance an empirical investigation",

Information Management and Computer Security, Vol. 22 No. 5, pp. 450-473.

Sindhuja, P.N. and Kunnathur, A.S. (2015), "Information security in supply chains: a management control perspective", *Information & Computer Security*, Vol. 23 No. 5, pp. 476-496.

Smith, G.E., Watson, K.J., Baker, W.H. and Pokorski Ii, J.A. (2007), "A critical balance: collaboration and security in the IT-enabled supply chain", *International Journal of Production Research*, Vol. 45 No. 11, pp. 2595-2613.

Spekman, R.E. and Davis, E.W. (2004), "Risky business: expanding the discussion on risk and the extended enterprise", *International Journal of Physical Distribution & Logistics Management*, Vol. 34 No. 5, pp. 414-433.

Stephens, J. and Valverde, R. (2013), "Security of e-procurement transactions in supply chain reengineering", *Computer and Information Science*, Vol. 6 No. 3, pp. 1-20.

Tao, Y., Lee, L.H. and Chew, E.P. (2016), "Quantifying the effect of sharing information in a supply chain facing supply disruptions", *Asia-Pacific Journal of Operational Research*, Vol. 33 No. 4, pp. 165-194.

Thun, J.H. and Hoenig, D. (2011), "An empirical analysis of supply chain risk management in the German automotive industry", *International Journal of Production Economics*, Vol. 131 No. 1, pp. 242-249.

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

Trombley, S. (2015), "Managing your information risk", *Computer Fraud & Security*, Vol. 2015 No. 7, pp. 5-9.

Tsai, M., Liao, C. and Han, C. (2008), "Risk perception on logistics outsourcing of retail chains: model development and empirical verification in Taiwan", *Supply Chain Management: An International Journal*, Vol. 13 No. 6, pp. 415-424.

Urciuoli, L. and Hintsa, J. (2017), "Adapting supply chain management strategies to security – an analysis of existing gaps and recommendations for improvement", *International Journal of Logistics Research and Applications*, Vol. 20 No. 3, pp. 276-295.

Van Hoek, R. (2019), "Unblocking the chain–findings from an executive workshop on blockchain in the supply chain", *Supply Chain Management: An International Journal*, Vol. 25 No. 2, doi: 10.1108/SCM-11-2018-0383.

Volpentesta, A.P., Ammirato, S. and Palmieri, R. (2011), "Investigating effects of security incident awareness on information risk perception", *International Journal of Technology Management*, Vol. 54 Nos 2/3, pp. 304-320.

Warren, M. and Hutchinson, W. (2000), "Cyber attacks against supply chain management systems: a short note", *International Journal of Physical Distribution & Logistics Management*, Vol. 30 Nos 7/8, pp. 710-716.

Webster, J. and Watson, R.T. (2002), "Analyzing the past to prepare for the future: writing a literature review", *MIS Quarterly*, Vol. 26 No. 2, pp. 13-23.

Wieland, A. (2013), "Selecting the right supply chain based on risks", *Journal of Manufacturing Technology Management*, Vol. 24 No. 5, pp. 652-668.

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

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

Xue, L., Zhang, C., Ling, H. and Zhao, X. (2013), "Risk mitigation in supply chain digitization: system modularity and information technology governance", *Journal of Management Information Systems*, Vol. 30 No. 1, pp. 325-325.

Zacharia, Z.G., Sanders, N.R. and Nix, N.W. (2011), "The emerging role of the third-party logistics provider (3PL) as an orchestrator", *Journal of Business Logistics*, Vol. 32 No. 1, pp. 40-54.

Zhu, Q., Sarkis, J. and Lai, K.H. (2007), "Initiatives and outcomes of green supply chain management implementation by Chinese manufacturers", *Journal of Environmental Management*, Vol. 85 No. 1, pp. 179-189.

Zuo, Y. and Hu, W.C. (2009), "Trust-based information risk management in a supply chain network", *International Journal of Information Systems and Supply Chain Management*, Vol. 2 No. 3, pp. 19-34.

Further reading

Khan, A., Bakkappa, B., Metri, B.A. and Sahay, B.S. (2009), "Impact of agile supply chains' delivery practices on firms' performance: cluster analysis and validation", *Supply Chain Management: An International Journal*, Vol. 14 No. 1.

Appendix. Section 1 – Company profile and respondent demographics

Survey questionnaire and scale items

Section 1 - Company profile and Respondent demographics

1. Company's role in the FMCG supply chain:
   - Manufacturer
   - Retailer
   - Logistics Service Provider

2. Annual company turnover in year 2018 (in Italy):
   - < 10 M €
   - 10-49 M €
   - 50-100 M €
   - >100 M €

3. Your Job Title/Role: _____

4. Number of years of working experience in the Fast-Moving Consumer Goods sector: _____

5. Number of years of working experience in your role at your current company: _____

Section 2 – Cyber and information risks

1. Please evaluate the following cyber and information risks in your company's supply chain in terms of PROBABILITY (from 1 = very low to 5 = very high) (adapted from Colicchia et al., 2019 and Hallikas *et al*., 2004)
   - ERP Malfunction
   - Crash of website
   - Lack of connectivity
   - Malware
   - Data breach
   - Damage of records
   - Theft of credentials
2. Please evaluate the following cyber and information risks in your company's supply chain in terms of IMPACT on your business (from 1 = very low to 5 = very high) (adapted from Colicchia et al., 2019 and Hallikas *et al*., 2004)
   - ERP malfunction
   - Crash of website
   - Lack of connectivity
   - Malware
   - Data breach
   - Damage of records
   - Theft of credentials
3. Please evaluate the following cyber and information risks in your company's supply chain in terms of OCCURRENCE (1 = never; 2 = more than one year ago; 3 = more than 6 months ago; 4= less than six months ago; 5 = less than one month ago) (newly developed by the authors on the basis of the risk events defined in questions 1 and 2)
   - ERP malfunction
   - Crash of website
   - Lack of connectivity
   - Malware
   - Data breach
   - Damage of records
   - Theft of credentials

Section 3 – Sources of cyber risks

4. Please evaluate the relevance of the following sources of cyber and information risk in your supply chain. Please refer to these items as MALICIOUS. (from 1 = very low to 5 = very high) (adapted from Ghadge *et al*., 2020 and Colicchia *et al*., 2019)
   - Current Employees
   - Former Employees
   - Suppliers
   - Former suppliers
   - Customers
   - Industrial Espionage
   - Hackers/Hacktivists
5. Please evaluate the relevance of the following sources of cyber and information risk in your supply chain. Please refer to these items as NON-INTENTIONAL. (from 1 = very low to 5 = very high) (adapted from Ghadge *et al*., 2020 and Colicchia *et al*., 2019)
   - Current Employees
   - Former Employees
   - Suppliers
   - Customers
   - Natural disasters
   - Internal technical problems
   - External technical problems

(*continued*)

Section 4 – Ownership of the cyber risk management process

6. Please indicate the level of importance of the involvement of the following organisational units in the management of cyber and information risk in your supply chain. (from 1 = very low to 5 = very high) (adapted from Colicchia *et al*., 2019)
   - Top management
   - IT-department
   - Operations
   - Supply chain/logistics
   - Finance
   - Risk management
   - Legal department
   - Human resources

Section 5 – Categories of information exchanged in the supply chain

7. Please indicate the degree of criticality of the following categories of information shared across the FMCG supply chain (from 1 = very low to 5 = very high) (adapted from Lee and Wang (2000) and Lofti *et al*., 2013).
   - Master data
   - Sales data and forecast
   - Invoices
   - Discounts and promotional plans
   - Inventory
   - Production plans
   - Delivery tracking
   - Transport rates and logistics costs

Section 6 – Measures to manage cyber risks in the supply chain

8. Please evaluate the relevance of the following initiatives and countermeasures to mitigate cyber risks. (from 1 = very low to 5 = very high) (adapted from Ghadge *et al*., 2020 and Colicchia *et al*., 2019)
   - Employ a chief information security officer (CISO) or data protection officer (DPO)
   - Conduct personnel background checks
   - Presence of an information security strategy
   - Specific data and information insurance
   - Employee security awareness training programme (cyber hygiene)
   - Secure data access and control measures
   - Accurate record of personnel handling sensitive data
   - Intrusion prevention systems (IPS), data and URL filtering (antivirus and antispam)
   - Multiple data backup
   - Geographical distributed datacentres
   - Require suppliers and customers to comply with the privacy and security policies
   - Conduct supply chain partners security audits
   - Communication procedures with involved supply chain partners
   - Business continuity and disaster recovery plans

About the authors

Alessandro Creazza is an Associate Professor of Logistics and Supply Chain Management at the School of Industrial Engineering of LIUC University (Italy) and a Visiting Fellow in the Faculty of Business, Law and Politics at the University of Hull, UK. He is a fellow of the Higher Education Academy in the UK and a member of the Italian Association of Professors of Industrial Plants Design and Management. Prior to this post, he was a Reader in Logistics and Supply Chain Management at Hull University Business School within the Logistics Institute, where he was Director of UK Recruitment and Partnerships for the Faculty of Business Law and Politics. He specializes in the area of the design and management of international logistics networks and his research interests include: cyber and information risk management, supply chain network design with risk and sustainability considerations (Eco-Resilience), health-care logistics, Logistics 4.0 and Industry 4.0, Circular Economy applied to logistics and supply chain management. He is the author of more than 90 publications at the international and national level.

Claudia Colicchia is an Associate Professor of Logistics and Supply Chain Management at Politecnico di Milano, Italy. She is Visiting Fellow in the Faculty of Business, Law and Politics, University of Hull, UK. She is a Fellow of the Higher Education Academy in the UK and a Member of the Italian

Association of Professors of Industrial Plants Design and Management. She is the author of more than 80 papers at the national and international level. Her research interests include Supply Chain Sustainability, Supply Chain Risk Management, Industry 4.0 and Logistics 4.0 and Citation Network Analysis. Her research has appeared in leading scientific journals, such as *Journal of Supply Chain Management*, *Production Planning and Control*, *Supply Chain Management*: *An International Journal*, *International Journal of Production Research*, *Journal of Cleaner Production* and *Journal of Business Ethics*. She has also received the 2019 Best Paper Award in the Journal of Supply Chain Management. Claudia Colicchia is the corresponding author and can be contacted at: claudia.colicchia@polimi.it

Salvatore Spiezia is a Project Manager at IBM Italy, where is responsible for planning and overseeing projects in the Track & Trace Area to ensure they are completed on time and within budget. He has worked for over two years in the optimization of various production processes, gaining experience with reengineering and transformations of the same. He has also worked at IBM as a SAP consultant, focusing on the reengineering of several processes within companies in the Pharmaceutical sector, developing manufacturing and logistic modules. In 2017, he obtained his MSc in Management and Industrial Engineering at LIUC University, Italy.

Fabrizio Dallari is a Full Professor of Logistics and Supply Chain Management at LIUC University (Italy) and he is also head of the Center for Supply Chain, Operations and Logistics. His current research interests include Operations and Supply Chain Management with a special emphasis on physical distribution network design, transportation systems, materials handling and supply chain planning. His research studies on the FMCG supply chain have been cited widely. He has been researching and teaching in logistics and supply chain for over 20 years and has published extensively in journals, conferences and he wrote 8 books. Fabrizio Dallari has cooperated with many companies, leaders in their respective fields. In 2010, he received the "Logistic Man of the year" award by Assologistica, the Italian logistics professionals' association. He is the owner of the "Logistica" discussion group on Linked-in, with +4.000 followers.