Managing Cyber and Information Risks in Supply Chains: insights from an Exploratory Analysis

Claudia Colicchia

University of Hull, Hull University Business School, Logistics Institute

Cottingham Road, Hull, UK, HU6 7RX

e-mail: c.colicchia@hull.ac.uk; Tel. +44 (0)1482 347550

Alessandro Creazza

University of Hull, Hull University Business School, Logistics Institute

Cottingham Road, Hull, UK, HU6 7RX

e-mail: a.creazza@hull.ac.uk; Tel. +44 (0)1482 347586

David Menachof

Florida Atlantic University, Information Technology and Operations Management, College of Business

777 Glades Road, Boca Raton, FL 33431

e-mail: dmenachof@fau.edu

Managing Cyber and Information Risks in Supply Chains: Insights from an Exploratory Analysis

Abstract

Purpose: The increasing level of connectivity is transforming supply chains, and it creates new opportunities but also new risks in the cyber space. Hence, cyber supply chain risk management (CSCRM) is emerging as a new management construct. The purpose of this paper is to explore how companies approach the management of cyber and information risks in their supply chain, what initiatives they adopt to this aim, and to what extent along the supply chain. The ultimate aim is to help organizations in understanding and improving the CSCRM process and cyber resilience in their supply chains.

Design/methodology/approach: This research relied on a qualitative approach based on a comparative case study analysis involving five large multinational companies with headquarters, or branches, in the UK.

Findings: Results highlight the importance for CSCRM to shift the viewpoint from the traditional focus on companies' internal information technology infrastructure, able to "firewall themselves" only, to the whole supply chain with a cross-functional approach; initiatives for CSCRM are mainly adopted to "respond" and "recover" without a well-rounded approach to supply chain resilience for a long-term capacity to adapt to changes according to an evolutionary approach. Initiatives are adopted at a firm/dyadic level, and a network perspective is missing.

Research limitations/implications: This paper extends the current theory on cyber and information risks in supply chains, as a combination of supply chain risk management and resilience, and information risk management. It provides an analysis and classification of cyber and information risks, sources of risks and initiatives to managing them according to a supply chain perspective, along with an investigation of their adoption across the supply chain. It also studies how the concept of resilience has been deployed in the CSCRM process by companies. By laying the empirical foundations of the subject, our study stimulates further research on the challenges and drivers of initiatives and coordination mechanisms for CSCRM at a supply chain network level.

Practical implications: Results invite companies to break the "silos" of their activities in CSCRM, embracing the whole supply chain network for better resilience. The adoption of information technology security initiatives should be combined with organizational ones and extended beyond the dyad. Where applicable, initiatives should be bi-directional to involve supply chain partners, remove the typical isolation in the CSCRM process, and leverage the value of information. Decisions on investments in CSCRM should involve also supply chain managers according to a holistic approach.

Originality/value: A supply chain perspective in the existing scientific contributions is missing in the management of cyber and information risk. This is one of the first empirical studies dealing with this interdisciplinary subject, focusing on risks that are now very high in the companies' agenda, but still overlooked. It contributes to theory on information risk since it addresses cyber and information risks in massively connected supply chains through a holistic approach that includes technology, people and processes at an extended level that goes beyond the dyad.

Keywords: Supply chain risk management, Cyber risk, Information risk, Cyber security, Supply chain management, Supply chain resilience

Article classification: research paper

Introduction

Over the last decades the expansion and importance of supply chain management has paralleled the growing ability of technology to exploit the benefits of information sharing for reducing costs, and concurrently improving customer satisfaction across business operations (Linton *et al.*, 2014). Supply chains are increasingly operating in a massively connected global environment, where connectivity and integration happens among people, processes and devices through information and communication technologies (ICT) (Vanpoucke *et al.*, 2017).

ICT tools and systems such as the Internet, electronic communication protocols (e.g. electronic data interchange – EDI), mobile and cloud computing and paradigms such as the Internet of Things (IoT – referring to sensors, machines and people connected in dynamic network infrastructures) have the potential to completely change the way operations planning, monitoring and execution are carried out (Ben-Daya *et al.*, 2017). The connectivity of supply chains and the digitalization of processes have led to the emergence of the so-called "cyber supply chain", defined as "a supply chain enhanced by cyber-based technologies to establish an effective value chain" (Kim and Im, 2014). The end-to-end flow of data provides visibility at all levels of the supply chain, for better process coordination, efficiency and effectiveness (Caridi *et al.*, 2014).

Unfortunately, for every good use of an innovation, there is someone looking to take advantage of its vulnerabilities. Warren and Hutchinson (1990) flagged cyber and information risks as supply chain related issues. As an example, a cyber-attack took place over a two year period beginning in 2011 at the port of Antwerp in Belgium, where a Dutch-based trafficking group hid cocaine and heroin among legitimate cargoes. The organised crime group allegedly used hackers based in Belgium to infiltrate computer networks in companies operating in the port of Antwerp. This allowed hackers to access secure data giving them the location and security details of containers, meaning the traffickers could send in lorry drivers to steal the cargo before the legitimate owner arrived (Bateman, 2013).

Besides representing threats for the society coming from an activity within the supply chain, these cyber-attacks have considerable implications for organizations too. In fact, as an additional example, in summer 2017 a major international shipping line had a high-profile cyber-attack. In addition to having an estimated cost for the company's operations up to $300 million, this attack had serious repercussions on the operations of their clients, who found their shipments stranded on uncontrollable and inaccessible vessels. Interestingly, these clients claimed that they had ICT security measures in place to "firewall themselves", but clearly not their supply chain (Williams, 2017).

All of this shows that in today's environment of massive connectivity of supply chains, relying on ICT and technical security solutions to "firewall organizations" is not sufficient, differently from what it could have expected. In fact, threats and attacks could involve partners upstream and downstream in the supply chain and have negative impacts on the focal company, even if "perfectly" protected against cyber-attacks.

This constitutes an interesting and thought-provoking fact that invites one to reflect on the necessity for organizations to go beyond the technical level to confront cyber risks, and to adopt a different approach that allows for deeply embracing the interconnected nature of supply chains. As a response, cyber supply chain risk management (CSCRM) is emerging as a new "management construct resulting from the fusion of approaches, methods, and practices from the fields of cyber security, information risk management, and supply chain management" (Boyson, 2014). This construct requires a cross functional approach combining appropriate capabilities, technical expertise and human factors across the supply chain to avoid and confront disruptions coming from the massive connectivity of today's systems' operations (Bartol, 2014).

In the current theory on the management of cyber and information risks a true supply chain perspective is missing. Traditionally, the literature has focussed on cyber and information risks from a technical and security perspective (Gaudenzi and Siciliano, 2017), within individual organizations (Biener *et al.*, 2015). Several literature contributions highlight the need for a more holistic approach to deal with cyber and information risks for organizations from a management perspective (e.g. Soomro *et al.*, 2016).

Hence, studies on the end-to-end interactions among supply chain players operating in a more open and integrated world need to be undertaken to unveil current issues that firms have to cope with in terms of the level of cyber risk in relation to overall supply chain risk (Linton *et al.*, 2014). Moreover, a substantial dearth of empirical evidence is highlighted in the current body of knowledge. Empirically proven best practices need to be shared for developing managerial approaches and tools for empowering organizations in the management of cyber and information risks in their supply chains (Boyson, 2014). New ways for strategically managing cyber risk could lead to enhanced cyber resilience as a result, by leveraging those principles essential for building a resilient supply chain (Ribeiro and Barbosa-Povoa, 2018).

Given this background, this study aims at pushing the boundaries of supply chain research and practice, by extending the existing theory on cyber and information risks in supply chains, as a combination of SCRM and resilience, and information risk management. This area, as explained above, is currently underdeveloped and in need of further exploration, especially in terms of extending supply chain knowledge beyond a dyadic perspective.

Hence, we present the results of an empirical investigation on cyber and information risks in supply chains. This work is based on multiple case studies of companies operating in connected supply chains where the cyber space links players beyond tier 1. The specific purpose of this paper is to explore how companies approach the management of cyber and information risks in their supply chain, what initiatives they currently adopt to this aim, and to what extent along the supply chain. For the purpose of this study, we investigate the CSCRM process of companies; we stretch our view beyond the dyad and tier 1 to understand the mechanisms of these phenomena and how far an end-to-end approach is adopted with players upstream and downstream in their supply chain. By collecting empirical evidence,

it also aims at offering organizations insights to understanding and enhancing the management of cyber and information risks in their supply chains for better resilience. Simultaneously, it allows embracing the challenges posed by rapidly changing technologies that directly affect supply chain management.

The contribution of the present study is important to the advancement of both theory and practice on the investigated topic, in that it furthers our understanding by presenting a combination of the various disciplines and by offering novel and unique insights thanks to the collection of field evidence. Our original findings complement the existing theory by offering new knowledge on the approaches to cyber and information risk management by companies; they also enrich practice by informing the industry on the end-to-end interactions among supply chain players when cyber and information risk management initiatives are considered. This lays the foundations to stimulate further research too.

The remainder of this paper is organized as follows. The following section presents the theoretical background of the study, while the adopted research methodology is described subsequently. The findings of the empirical investigation are then reported and discussed. Final remarks, implications and directions for future research conclude this paper.

Theoretical background

Consistently with the objectives of this research, we present a theoretical background focused on the areas investigated in this work: supply chain risk management and resilience, information risk management, and CSCRM (including cyber and information risk in supply chains and related sources, and initiatives to manage this kind of risk). We conclude this section with the research gaps arising from our literature review.

Supply chain risk management and resilience

Few areas of management interest have risen to prominence in recent years as rapidly as supply chain risk management (SCRM), due to the turbulence of the business environment, volatile and variable consumer demands, along with actions by competitors (Christopher and Holweg, 2011). A definition of supply chain risk is “the variation in the distribution of possible supply chain outcomes, their likelihoods, and their subjective values” (Jüttner *et al.*, 2003). This definition points at the dimensions of risk, i.e. probability of occurrence and impact on business, originally proposed by the traditional risk management literature (March and Shapira, 1987). According to Tang (2006), supply chain risks can be classified into “disruption” and “operational”. Disruption risks are related to natural and man-made disaster, while operational risks are connected to the uncertainty of supply and demand processes and price. Operational risks were further classified by Prasanna Venkatesan and Kumanan (2012), and include risks such as quality risk, capacity risk, supply and demand risk, exchange rate risk, and information flow risk.

The main aim of SCRM is to protect businesses from adverse events, through a process that is composed of four main phases, represented by risk identification, risk assessment, risk mitigation and risk monitoring (Ho *et al.*, 2015). The first phase entails the identification of the risks and related sources; the second phase implies the assessment of the probability of occurrence of risky events and their impact on business; the third phase includes the design, selection and implementation of strategies and tools to manage and mitigate the negative effects of potential risks; the fourth phase requires the implementation of abnormality diagnosis models and other metrics and measures to early detect potential signals of risk and act upon them.

Besides arranging the SCRM process internally to the organization (by setting appropriate ownership/level of centralization of decisions), a coordinated approach among supply chain members is deemed as essential to manage supply chain risk and enhance supply chain resilience (Colicchia and Strozzi, 2012; Chowdhury and Quaddus, 2016; Ribeiro and Barbosa-Povoa, 2018). This coordinated approach should encompass both proactive and reactive measures to achieve resilience, which respectively refer to the concepts of robustness and agility (Wieland and Wallenburg, 2013).

Various definitions of supply chain resilience have been proposed and revolve around the idea of restoring the state of operations (Ribeiro and Barbosa-Povoa, 2018). In this respect, Davoudi (2012) discusses three views on resilience: engineering resilience as the ability of a system to return to an equilibrium or steady-state after a disturbance; ecological resilience which instead proposes the existence of multiple equilibria, and the possibility of systems to enter alternative stability domains; and evolutionary resilience, which moves away from the concept of equilibrium and affirms that systems might change over time with or without an external disturbance. In this sense, Davoudi (2012) proposes resilience as the capacity to adapt to all types of changes in a continuous way, since today's world is seen as a chaotic and uncertain environment.

Given this view of the world, supply chain resilience is composed of a set of adaptive responses in a multi-stage approach. If according to Ribeiro and Barbosa-Povoa (2018) these responses are triggered by potential risky events, Davoudi (2012) specifies that responses are generated by the continuous tensions deriving from changes in complex and uncertain systems, which require a continuously adaptive response. This approach should embrace different phases: prepare, respond, recover and maintain, where "maintain" also means a long-term adaptive capacity. Hence, the concept of supply chain resilience needs to combine proactive and anticipating actions with plans and planned steps to respond to incidents and maintain not only a steady-state solution after the recovery from a disruption, but a continuously adaptive approach to changes in today's complex and uncertain systems (Davoudi, 2012; Hohenstein *et al.*, 2015; Ribeiro and Barbosa-Povoa, 2018).

The literature discusses enablers and barriers to supply chain resilience. The main identified enablers are: flexibility, supply chain visibility, collaboration/coordination among supply chain partners by means of communicative and cooperative relationships (Wieland and Wallenburg, 2013), joint relationship efforts (Scholten and Schilder, 2015; Ali *et al.*, 2017). Whilst, the main identified barriers

are: misalignment of objectives within and among the partnering firms, along with lack of visibility, collaboration and trust (Ali *et al.*, 2017), which are affected by the presence of behavioural uncertainty among people in the supply chain (Dubei *et al.*, 2017).

To achieve resilience in supply chains, it is necessary to identify the right fit between a company's level of risk in the supply chain and its preparedness in risk management. This can be seen also from the perspective of investments in supply chain risk management initiatives. In this regard, Pettit *et al.* (2013), and Gualandris and Kalchschmidt (2015) introduce the concept of "balanced resilience". This concept represents the right fit between the level of riskiness of a certain supply chain configuration and the related amount of investment in the SCRM process, appropriate to adequately confront that level of riskiness and to continuously adapt to changes. Ambulkar *et al.* (2015) discuss the implications for resources' configuration in firms when contexts of high disruption impact or low disruption impact are concerned.

The literature reveals that it might not be possible to implement resilience driven actions in an isolated form. In fact, in connected and complex supply chain networks with several tiers that create dependency, resilience strategies should be devised together with supply chain partners and rely on knowledge created and shared across the supply chain (Ribeiro and Barbosa-Povoa, 2018). This should be aimed at building that long-term adaptive capacity that makes the whole supply chain more resilient to the continuous changes and inner tensions of today's complex systems according to an evolutionary view (Davoudi, 2012). This would also allow embracing the concept of risk propagation at a network level (Han and Shin, 2016). In other words, risks can migrate across the supply network, and for this reason it is necessary to adopt a holistic approach to resilience because of the strong interconnectedness of players along the supply chain (Tukamuhabwa *et al.*, 2017).

Information risk management

Information is an element widely acknowledged as a competitive advantage source for organizations (Daugherty *et al.*, 2006). It can give power and insight (Trombley, 2015), and it allows for integration and coordination in the supply chain when data are shared in a controlled way (Wang *et al.*, 2008; Boulesnane and Bouzidi, 2013). Seminal works defined information as "the substance from which the managerial decisions are made" (Forrester, 1962). Managing information in a proper way is a challenging task for organizations, due to increased volume, speed of transmission and growing variety of types of information and data. Moreover, threats to information are rising and similarly concerns about how to manage these risks (Trombley, 2015).

"Information risk" can be defined as "the probability of loss arising because of incorrect, incomplete, or illegal access to information" (Faisal *et al.*, 2007) that can undermine its security. Information risk is in fact tightly connected to the concept of information security (Trombley, 2015). Numerous frameworks for managing risks to information and technology resources have been proposed in the academic and technical literature: the ISO standards on risk management (ISO 31000, ISO 31010) and

information security management (ISO 27000); the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (Yeo *et al.*, 2014); the NIST standards for risk management and information security (Bartol, 2014). Alongside, a considerable body of knowledge has focused on the management of information risks and related security issues for organizations.

However, from an overall analysis of the extant literature, it appears that research on information risk and security has been dominated by technical aspects (Karlsson *et al.*, 2016), and information security management was treated as a technical issue (Singh *et al.*, 2013). Hence, the majority of the attention was given to technological solutions (Soomro *et al.*, 2016). Some contributions studied the return on investments on security technology and initiatives, such as intrusion detection systems and anti-virus protection, as well as technologies used to protect the confidentiality and integrity of data (Yeo *et al.*, 2014). These include cryptography solutions and secure multi-party computation, which has the aim to create methods for parties to ensure a secure collaboration and process information while keeping identities private (Prabhakaran and Sahai, 2013). Hao and Cai (2011) proposed a cloud model to provide "a confidential and verifiable environment for each sensitive application". Generic technical solutions also exist, such as access controls solutions (Chen *et al.*, 2007; Santos-Pereira *et al.*, 2013) and virus propagation models (Yuan *et al.*, 2009).

Research also discussed the fact that technology alone is unable to provide enough solutions to address organisational information security concerns and needs (Singh *et al.*, 2013). Consequently literature has started to focus on a balanced approach of technical, human and organizational factors (Soomro *et al.*, 2016). Examples of this category of initiatives include: internal audit processes (Yeo *et al.*, 2014); information security policies (Siponen *et al.*, 2014); policies to countermeasure information asymmetry among different departments within an organization (Kumar *et al.*, 2008); compliance training schemes to create information security awareness and drive the behaviour of employees (Parsons *et al.*, 2014).

Nevertheless, from the reviewed literature it appears that information risk management efforts are generally focussed within the boundaries of the organization or, on a much lesser scale, on inter-organizational dyadic connections between companies (Karlsson *et al.*, 2016). Hence, the literature advocates for a more holistic approach to information risk management (Soomro *et al.*, 2016).

The new management construct of cyber supply chain risk management

Building on Boysons's (2014) definition, CSCRM 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 (Boyson, 2014). Differently from a traditional approach to information risk management, CSCRM entails a holistic approach that combines processes, people and technology to embrace a "relationship dimension" (Spekman and Davis, 2004). This is intended to enable a high level of integration that extends to supply chain partners beyond the dyad or single points of interface between supply chain partners.

The aim of CSCRM is to gain control within the boundaries of the focal company and on inter-organizational dyadic connections between companies, but most importantly, building upon this, to gain control at an end-to-end supply chain level that allows for a continuously adaptive capacity. This holistic approach should lead to better resilience related to cyber and information risk according to an evolutionary view.

The challenge is that the process of CSCRM has to deal with increasing complexity of supply chains. This is linked to the number of suppliers in an organization's supply base (horizontal complexity), to the number of tiers in that supply chain (vertical complexity), and to the geographical spread of a company and/or supply base (spatial complexity) (Bode and Wagner, 2015). To add to this growing supply chain complexity, market behaviours, configurations and often non-transparent supply chain partners' identities in the cyber space are constantly changing (Bartol, 2014; Linton *et al.*, 2014).

Risky events can happen also in stages of the supply chain distant from the focal company and have a knock-down effect on the entire supply chain (Williams, 2017). Hence, the extended holistic approach through CSCRM is deemed as essential to confront the mentioned challenges towards enhanced cyber resilience.

According to the abovementioned concept of balanced resilience, the CSCRM process needs to take into account the level of supply chain risk contingent to different contexts and sectors. This should be something similar to what happens when different supply chain configurations are explored and devised to fit with the characteristics of products and related demand (Fisher, 1997; Fine, 2000). In this way it would be possible to achieve the so-called "strategic fit" (Wagner *et al.*, 2012). In a similar fashion, the proneness of the supply chain to cyber risks in terms of probability and impact needs to be taken into account when planning appropriate investments to confront these risks to achieve balanced resilience. This would entail also the adoption of performance measurement systems for turbulence and risk management to facilitate the achievement of enhanced resilience for organizations (Bühler *et al.*, 2016).

Cyber and information risk in supply chains

According to Zuo and Hu (2009), the main information risks in a supply chain include: risk to information confidentiality, which relates to the potential loss of control over sensitive information/data across the supply chain; risk to information privacy, which relates to the potential misuse of data out of the principal purpose of releasing data by the data owner; risk to information integrity, which relates to the potential corruption and damaging of data/information stored in IT systems across the supply chain network.

The cyber supply chain offers numerous levels of targets for breach and corruption. This can result in customers, suppliers and employees records compromised (WEF, 2014; BCI, 2015), breach and disclosure of sensitive data on processes, products, data flows, governance and operations (Boyson, 2014). Literature also discusses the risk of theft of intellectual property and counterfeits aimed at

gaining financial advantage over the focal company/supply chain (WEF, 2014; Stevenson and Busby, 2015). Another risk debated in the literature is represented by the problems connected to the IT systems such as the crash of websites and the failure of companies' IT networks, leading to the unavailability of critical services (BCI, 2015).

Basing on the previous literature, we propose a classification of the sources of cyber and information risks in the supply chain (see Table 1), built on two dimensions: the location of the source of risk in the supply chain (i.e. internal to the focal company or external to it) and the nature of the source of risk (i.e. malicious attacks or natural and non-intentional actions). The necessity to distinguish between internal and external sources of risk is essential given that internal sources of risks are progressively gaining importance: fraud by employees is common and difficult to detect, stop or prevent (Boyson, 2014). Both current and former employees can represent a threat to organizations. Distinguishing between current and former employees stresses the different level of control on these sources, because it is usually more difficult to track the actions of former employees who might still have retention of relevant data/information but who operate externally to the company (PwC, 2014). While in several occasions employees deliberately act against the interests of their own employers, some cases are related to non-intentional actions that include forwarding of infected messages, sharing of passwords or account details, replying to phishing messages, retrieving and storing data on portable and uncontrolled devices (PwC, 2014). Employees are progressively becoming the vehicle for malicious attacks: this happens through the so-called "social engineering" techniques, which involve tricking human beings into breaking companies' common security procedures and divulgating confidential information (Happ *et al.*, 2016). Recent research points at phishing and social engineering as the top source of cyber disruption (BCI, 2016).

Externally, the sources of cyber and information risks lie in the various tiers of the supply chain (Boyson, 2014), in most cases beyond the Tier 1 and affect the entire network (BCI, 2015): current and former suppliers/contractors, customers and competitors contribute to expose the supply chain to cyber and information risks through both malicious and non-intentional attacks. These mainly include actions related to the sharing and transmission of information and data across multiple stages of the supply chain, which are not always happening through secure communication channels/methods (Barkataki and Zeineddine, 2015). Likewise, the points of interface among supply chain partners are vulnerable to cyber-attacks, especially when they concentrate large international flows of products and related information: for example seaports are particularly exposed to advanced persistent threats (APT) by criminal activities due to the increased use of mobile devices (Rushmere, 2015) and data transmission (Yang and Wei, 2013). Also foreign nation states, domestic intelligence services/espionage and hacker/hactivists represent a source of risk coming from malicious attacks, through actions connected to broader societal implications (Luiijf *et al.*, 2013).

Among the natural and non-intentional sources of cyber and information risks, literature includes factors such as power outages and technical problems to the IT infrastructure. These can be both

internal and external to the focal company, causing failures that compromise the operations and the flow of information across multiple tiers (Intel Security, 2014). Finally, natural disasters are also mentioned as external and non-intentional sources of risk (Boyson, 2014).

Existing literature stresses the importance of investigating the perceptions of these new threats to the value creation in companies, as explained by the work of Gaudenzi and Siciliano (2017), who showed that there is very little awareness of what these risks are and to what kind of sources they are linked. This calls for further investigations on this underexplored theme.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Table 1. Sources of cyber and information risks in the supply chain

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Initiatives to manage cyber and information risk in supply chains

In order to understand the tools and instruments available to companies for implementing a CSCRM process, we present a review of the initiatives to managing cyber and information risks in the supply chain. The current literature has explored the development and implementation of security safeguards and initiatives for addressing the described concerns. The reviewed initiatives were aggregated to create homogeneous clusters and in doing this, we identified a link that connects them with the sources of risk they aim at counteracting.

Security safeguards and initiatives include:

- *Organizational initiatives:* these initiatives have as a first focal point the alignment of the information security strategy with the overarching strategy and specific needs of the business (Bartol, 2014). Standards and protocols have been developed to improve the mentioned strategic alignment and to provide regulatory guidelines, e.g. ISO27000 and NIST SP 800-161 (Bartol, 2014; Keegan, 2014). This could also lead to the establishment of a chief information security officer position in companies (Boyson, 2014) and to the introduction of security entrance barriers such as personnel background checks (Kim and Im, 2014). Also, cyber insurance products have been proposed to specifically tackle cyber threats (Mukhopadhyay *et al.*, 2013), even if their adoption is still in its infancy (BCI, 2015). This is confirmed by the work of Biener *et al.* (2015), who stress the fact that the cyber risk insurance market lags behind the expectations of companies. This is also due to the internal perceptions related to the capability of the existing insurance products to protect organizations from highly interrelated losses, lack of data, and severe information asymmetries. These problems

hinder the development of a sustainable cyber insurance market. Given their broad focus, this group of initiatives has a pervasive effect and are aimed at counteracting all sources of risks.

- *Training and internal awareness:* training and awareness programmes for employees are essential for good "cyber hygiene". O'Connell (2012) define it as the process of "educating everyone legitimately relying on the Internet on good network usage practices". These initiatives are critical to educate and up-skill the human capital in companies to enhance resilience and prevent, detect and respond to internal threats in supply chains (Boyson, 2014). In fact, it is necessary to strengthen staff awareness in order to help directors and top management in driving choices regarding security investment and supplier selection to better security (BCI, 2016). Likewise, employees need to be aware of the potential implications of their choices mainly in terms of usage of security tools, especially when performance and security trade-offs are involved (Intel Security, 2014). Training and awareness programmes are aimed at hunting trust assumptions and ineptitude when unpalatable courses of action might be necessary to ensure a higher degree of security in processes and operations (Windelberg, 2016). This is connected to the perceptions of employees regarding motivations internal to the company or related to their personal beliefs environment. Also motivations external to the company (coming from the wider environment) can trigger compliant or non-compliant behaviours towards cyber security (Bulgurcu *et al.*, 2010). Along these lines, the study by Ifinedo (2012) showed that factors such as self-efficacy, attitude toward compliance, subjective norms, response efficacy and perceived vulnerability positively influence behavioural compliance intentions of employees. Procedures for protecting intellectual property are also seen as critical in the literature (Stevenson and Busby, 2015), including safe and controlled sharing of data and information across multiple tiers of the supply chain (WEF, 2014). This group of initiatives are especially aimed at counteracting the sources of risk coming from people working within the company, i.e. current employees.
- *Compliance and external awareness:* being that today's supply chains are strongly interlinked and massively connected, it is necessary that supply chain partners are made sufficiently aware of the threats and risks coming from the cyber space to increase the resilience of inter-entity business processes to cyber disruptions (Tran *et al.*, 2016). This could happen through appropriate supply chain coordination mechanisms as suggested by the literature (Pilbeam *et al.*, 2012; Herrera and Janczewsky, 2015). Supply chain coordination can be achieved through: alignment, intended as the development of a collective strategy among supply chain partners, along with a common culture and shared norms and processes (Hanf and Dautzenberg, 2006; Pradabwong *et al.*, 2017); synchronization, intended as a tool enabling effective information-sharing among supply chain partners and supporting decision making especially during disruption responses (Soni *et al.*, 2014; Singh *et al.*, 2018); shared knowledge, i.e. sharing of experiences among supply chain partners after disruptions are overcome with the aim to

create post-incident reports accessible to all supply chain partners (Tao *et al.*, 2016). This is also referred to as mutually-created knowledge (Scholten and Schilder, 2015). In the context of this study, this is translated into a set of specific initiatives. It is important for companies to: (i) require customers and suppliers/contractors to comply with their privacy and security policies, by adhering to security protocols and guidelines (Eurich *et al.*, 2010) to achieve alignment; (ii) conduct supply chain partner security audits (BCI, 2015) and qualification/operational checks (Boyson, 2014) to ensure that the third party has the ability to safeguard and share the information and is protecting the data (PwC, 2014), according to the principle of synchronization; (iii) establish collaborative agreements with supply chain partners on security (Kim and Im, 2014) to create an end-to-end IT integration including supply chain policies, processes and people (Boyson, 2014) to reinforce synchronization and to improve "threat intelligence" (PwC, 2014) through shared knowledge. Given their focus, this group of initiatives are especially aimed at counteracting the sources of risk coming from partners in the supply chain, i.e. suppliers and customers.

- *Event management:* this category of measures mainly refers to ways in which organizations can respond to cyber and information risk events. This category contributes to the achievement of supply chain coordination through the so-called situational awareness. Literature defines this concept as "an individually as well as socially cognitive state of understanding 'the big picture' during critical situations" (Sarter and Woods, 1991). It enables mechanisms supporting companies' willingness to share information in order to create trust among supply chain partners (Tao *et al.*, 2016). It also contributes to a "common baseline of the current conditions" available to partners and exchanged among them, so that actions can be undertaken as quickly as possible (Sheffi, 2005). Initiatives include business continuity and disaster recovery plans (BCI, 2016) and incident management processes (WEF, 2014). These measures need to be validated and agreed with supply chain partners. According to the principle of situational awareness, specific initiatives such as communication procedures with involved supply chain partners are essential for improving the timeliness and effectiveness of responses to events and of recovery from incidents (BCI, 2016). These should be coupled also with initiatives that embrace information systems continuity management approaches (Järveläinen, 2013), which can help to identify the dependencies between internal and external systems and supply chain players. Plans, analyses and continuity processes involve supply chain players and not only IT experts, leveraging their perceptions to positively affect the effectiveness of these practices on perceived business impacts (Järveläinen, 2013). These initiatives are focused on the risky events themselves, independently from who/what triggers the risky event, so they can address all sources of risk.
- *Data management:* managing access to data is of vital importance for companies in protecting themselves from cyber risks. The foundation of a secure data management approach is to

build and maintain an accurate record of all the employees accessing and handling data. A critical success factor will be the identification of the suitable/trusted people that could access data. The answer to this question leads to the allocation of access permissions and privileges to different categories of users (Trombley, 2015). Secure data access and control measures complying with the devised information security strategy and fulfilling the specific business requirements, need to be put in place to identify sensitive assets, detect and prevent the leakage of confidential information (Eurich *et al.*, 2010). This group of categories specifically focuses on the handling of data and information by employees, and consequently represents ways in which the behaviours/tasks of current and former employees can be contained.

- *IT security tools:* todays companies' IT systems have a range of security tools to protect from cyber intrusions, spanning from encryption of e-mail messages (Bartol, 2014), intrusion prevention systems (IPS), data loss prevention tools (PwC, 2014), geo-location and geo-fencing controls (firewall and virtual private networks) (Secci and Murugesan, 2014), data and URL filtering (antivirus and antispam) (Intel Security, 2014). Some of these tools feature detection functionalities, which report on malicious codes, unauthorized use or access. Similarly, mobile security strategy and device management are essential to securing a fleet of devices, whether owned by the enterprise or the individual (PwC, 2014). Given their focus, aimed at protecting the supply chain from vulnerabilities and attacks, this group of initiatives counteracts sources of risks including current and former employees and external sources, such as suppliers, customers, competitors, foreign nation states, domestic intelligence services, and hackers/hacktivists.
- *IT operational resilience:* this category of initiatives include actions aimed at ensuring continuity to the IT operations across the supply chain. They revolve around hardware and systems architecture resilience and recovery capabilities. They refer to measures connected to the IT system failure management across the supply chain, through actions such as recovery plan processes, both internal and externally involving supply chain partners (Boyson, 2014; BCI, 2015). They also include measures for improving operational resilience through IT systems and solutions, such as multiple data backup, geographical distributed datacentres, virtual networks/IT infrastructures, uninterruptible power supplies/power banks (Secci and Murugesan, 2014), and cloud systems orchestrators able to isolate a company's network in case of cyber-attack penetration, concurrently offering continuity of operations on a separated cloud network (BCI, 2016). Given their operational resilience and continuity focus, this group of initiatives especially counteract those sources such as technical problems, natural disasters, power outages and external attackers.

From an overall view, the set of initiatives to CSCRM reflect the modern concept of supply chain resilience, which is composed of a set of adaptive responses in a multi-stage approach (Ribeiro and

Barbosa-Povoa, 2018). In fact, the above initiatives include actions aimed at ensuring adequate response to disruptions (e.g. event management), complemented by actions covering all phases of the multi-stage approach discussed in the literature, i.e. prepare, respond, recover and maintain. For example, "Training and internal awareness" initiatives allow for preparing employees and empowering them to manage potential incidents, drive recovery plus maintenance of a robust state and, according to an evolutionary view (Davoudi, 2012), to develop a long-term adaptive capacity to face the continuous changes and inner tensions in today's complex and uncertain environment. Furthermore, this set of initiatives encompasses the need to stretch beyond the boundaries of the focal company and of dyadic relationships to avoid those issues related to isolation highlighted by the literature as impeding elements to building a cyber resilient supply chain.

Research gaps

The review of the existing body of knowledge allowed broadly exploring the uniqueness of the concept of CSCRM and its components, building upon literature on supply chain risk and resilience, and information risk management. It also emerged that information risk management in supply chains is a field which has not been extensively researched, although its importance is well recognized in the supply chain management literature (Sharma and Routroy, 2016; Rajagopal *et al.*, 2017).

In performing the review, we aimed at systematizing and rationalizing the existing contributions on the investigated topic, grouping previous works in the thematic categories presented in the previous pages. This effort allowed appreciating that the extant literature appears to be scattered, and covers in a piecemeal fashion a very wide range of topics and fields. These span from technical IT studies, to investigations on standards and protocols, to contributions focused on organizational issues. Also, research on risks, sources of risks and initiatives to manage them in the cyber space exist, but again these are investigated within specific studies focused on single themes or technical contexts and do not embrace the concept of supply chain resilience as a whole.

As mentioned, given the growth of the level of connectedness of supply chains worldwide, and the emerging need for managing cyber and information risks in the supply chain, cohesive and comprehensive studies on the topic are necessary to include a cross-functional holistic approach in the supply chain at a network level (Bartol, 2014; Soomro *et al.*, 2016). Traditionally cyber and information risks were prerogative of information security or software engineering practitioners.

Recent literature acknowledges the need for a cross-functional holistic approach to manage them in the supply chain. This approach should look at the interactions between processes, people and information technology (Intel Security, 2014; Secci and Murugesan, 2014), and at the coordination mechanisms that allow supply chain partners to adopt an end-to-end approach beyond the dyad (Herrera and Janczewski, 2015).

However, our review of the existing literature shows that this need has yet to be fulfilled in a holistic and cohesive way. It also shows the need for providing the scientific and industrial communities with

empirical evidence aimed at advancing the knowledge and managerial practice on the topic of CSCRM for building a resilient supply chain. In fact, a substantial dearth of empirical studies on cyber and information risk management conducted according to the abovementioned perspectives has been highlighted by previous research (Boyson, 2014; Karlsson *et al.*, 2016) and thus further empirical studies are called for by the managerial implications of cyber-attacks shown in recent examples (e.g. Williams, 2017). These gaps provide the motivations for our study and offer to the authors the possibility to complement the existing body of knowledge by providing the academic community with the results of our study, especially shedding light on the managerial implications of the choices made by companies in terms of approaches to managing cyber and information risks, the adopted initiatives, and to what extent in the supply chain. Along with the objectives of this research, these gaps inform the design of our empirical investigation, described in the next section.

Methodology

The aim of this study is to contribute to the development of theory on CSCRM as a combination of SCRM and resilience, and information risk. This is a subject that needs further exploration as shown in the previous sections.

As a consequence, we decided to adopt a qualitative research approach and selected a multiple case study investigation as a research method. Focused case studies are suitable for analyses of current phenomena including the social dimension, implanted in complex environments (Yin, 2018), being particularly recommendable to exploratory research on matters in need of a deeper understanding (Jüttner and Maklan, 2011).

In fact, we believe that this research is part of the "mapping/relationship building stage of theory building" (Stuart *et al.* 2002), where we aim at identifying and describing critical factors and the relationships that drive behaviours (Golicic and Sebastiao, 2011). Also, by enabling direct interaction with people and informants, case research provides an advantage over other research techniques, such as surveys (Miles and Huberman, 1994). We present our research process following the steps recommended by standard case based research methodology: case selection, data collection, and data analysis and validation (Stuart *et al.*, 2002).

Case selection

The case selection process was aimed at creating a diverse but coherent universe for our exploration on a focused matter (Robinson, 2014). The following three inclusion criteria were applied:

(i) Companies operating at different stages of the supply chain. Given the supply chain perspective of this study, we decided to sample companies setting a quota of one supply chain actor for each supply chain stage, according to a quota sampling approach (Robinson, 2014). Hence, we decided to include one manufacturing/supplier company, one logistics service provider operating in the packaged/palletized goods sector, one logistics service provider operating in the bulk goods sector, one

shipping company and one retailer. In particular, the logistics service provider operating in the bulk sector and the shipping company were included as key stages of the supply chain to encompass the CSCRM process taking place in seaports, which are targeted for criminal activities due to the increased use of mobile devices (Rushmere, 2015).

(ii) Large companies, which usually have structured supply chain processes and complex supply chain network relationships. Large companies typically have more technology in place, more mature security processes and intense activities in the cyber supply chain. They are often targeted by threat actors due to the large amount of information they manage and that can be exploited, sold or used (PwC, 2014). Hence they constitute an adequate territory of exploration for the purpose of this study.

(iii) Multinational companies with headquarters or a branch in the UK. The purpose was to control for factors such as culture, language, legal system and economic environment through geographic location: factors such as regulations, legislation, and stakeholder pressure differ among countries and this could create relevant deviations in the exploratory results (Mena *et al.*, 2013).

Based on the above criteria, five companies constituted our sample. This decision is in line with the methodological literature on case study research, which acknowledges that four to 10 cases are generally sufficient to draw meaningful insights on the phenomena under investigation (Ellram, 1996). Moreover, we consider this number of case studies to be sufficient, given the purpose of our research (Strauss, 1987; McCracken, 1998).

As for the nature of the selected companies, the adopted inclusion criteria allowed obtaining a sample of organizations that is not constrained by the typical specificities of a certain industry or of a certain type of supply chain. In fact, this could influence results and prevent one from obtaining a first understanding of the phenomena under investigation.

For confidentiality reasons, the names of the case companies have not been disclosed and each company has been referred to by using an alphabetical letter. Table 2 gives an overview of the case companies, along with additional background information.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Table 2. Profile of the case companies

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Data collection

Following the literature review, we designed our data collection instrument and developed a formal interview protocol (Yin, 2018). It contains a mixture of open questions and multiple choice questions and it is composed of five main sections: (1) Company profile, (2) The importance of managing

supply chain risks and cyber and information risks, (3) The SCRM process, (4) Cyber and information risks in the supply chain, (5) Initiatives to managing cyber and information risks in the supply chain.

The questionnaire was designed with the aim to allow investigating the CSCRM process originating in the focal company and its branching across the supply chain towards customers and suppliers beyond the dyad and Tier 1. The specific questions focused on relationships that spread upstream and downstream across the supply chain and connect players beyond the dyad. Questions pointed at unveiling what happens when the CSCRM process is implemented and stretched beyond the dyad and Tier 1, to appreciate the underlying mechanisms in the relationships with partners upstream and downstream the supply chain.

A pilot test was performed with a panel of academics and experts in the field of SCRM and information management. As a result, amendments were made on the wording of some questions so that they became clearer and more focused. The pilot test assisted in avoiding misinterpretations (Yin, 2018), providing a solid questionnaire and a facilitated comparison of the cases.

We identified the most suitable informants in each participating company: the supply chain manager/director and the information systems/technology director, which were both interviewed in each company (or the equivalent professional role). Two of the authors participated in each of the interviews at the companies' premises. Interviews lasted approximately 1.5 hours each; they were audio recorded, transcribed and interview reports were prepared to enable data analysis. Reports and transcripts were included in a case study database. Websites and third party reports were analysed and the collected evidence was included in the case study database to enable triangulation. The use of multiple respondents and different types of data were intended to mitigate the biases of single sources of information (Miles and Huberman, 1994).

The gathered information was matched with the recorded interview data to obtain a clear picture of the investigated phenomena. Interview reports were shared with the interviewees (Yin, 2018) and remaining discrepancies were resolved by recalling respondents via e-mails or phone calls.

Data analysis and validation

A within-case analysis allowed producing case study reports, which were shared with and reviewed by the key informants, as suggested by Yin (2018). Researchers first scanned the collected data and formalized coding, writing and reflecting remarks (Miles and Huberman, 1994). Templates were used, including charts and tables (Miles and Huberman, 1994; Crabtree and Miller, 1999). Patterns in the data were identified and categorized within the single cases. A subsequent cross case analysis was performed to search for emergent themes, patterns of commonality and key differences, by comparing the outcomes of the within-case analysis after coding data and generate the interpretations presented in the research findings (Miles and Huberman, 1994).

In terms of validation of the outcomes of our research steps, we followed the practices recommended by established methodological literature. Empirical validity was assessed by means of the criteria

presented by Yin (2018), and made explicit in Table 3. Construct validity was ensured through the establishment of a chain of evidence linking the research objectives to the protocol and to the results (through the involvement of multiple informants to seek feedback and observations, and through the demonstration of the convergence of patterns from multiple data sources), and by developing our data collection tool on the basis of our literature. Internal validity was ensured through building our research on recognized principles of CSCRM and related literature, which acted as foundation to identify critical factors and relationships driving behaviours; also through a structured analysis of the collected data, the use of templates containing charts and tables, which helped in maintaining the chain of evidence, and through pattern matching within and across the cases, triangulating data, and reaching an agreement among researchers (Miles and Huberman, 1984; Yin, 2018). External validity was ensured by setting suitable sampling criteria driven by the research objectives, which allowed building a coherent and diverse sample, along with describing the context and the cases; also, we compared data gathered from companies operating in different supply chains and different stages of the supply chain. Reliability of the research was ensured on the rigour of the applied process (protocol developed and validated; clear and structured sampling criteria; shared interview protocol for all interviewers; creation of a database including the interviews and questionnaires), and on the level of detail provided in a formalized coding that involved multiple researchers: this allows for replicability of the study for future research.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Table 3. Assessment of the empirical validity of the research (based on Yin, 2018; and Reuter *et al.*, 2010)

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Findings and discussions

After describing in the previous section the adopted research methodology, in this section the empirical findings of this study are reported and depicted in Tables 4, 5, 6 and 7. We first present the outcomes of the within case analysis, according to a thematic template (Ellis *et al.*, 2011; Gualandris and Kalchschmidt, 2014). For each company, the template includes: the key types of cyber and information risks and related sources as perceived by our respondents; the adopted approaches to SCRM and CSCRM; the initiatives currently in place within organizations to manage cyber and information risks in the supply chain. Subsequently, a cross case analysis is performed by concurrently looking at the outcomes of the within case analysis from an overall combined perspective, so that patterns, commonalities and key divergences can emerge across the sample.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Table 4. Perception of the main cyber and information risks in the supply chain

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Table 5. Main sources of information and cyber risks in the supply chain

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Table 6. SCRM and CSCRM at the case companies

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Table 7. Security safeguards and initiatives

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Within Case Analysis

Company A

Company A shows a low perception of the probability of occurrence of the main cyber and information risks. Data breach and disclosure is the only one with a medium score, given the large amount of relationships with supply chain partners that, according to our interviewee, can increase the likelihood of leakage of data. While this is acknowledged for all stages of the supply chain, our interviewee pointed out that for Company A this seems to be more critical on the supply side, where they have several worldwide suppliers connected in a network of different layers that go beyond Tier 1. Sharing information on product and process design is mandatory for ensuring good product quality

but on the other hand can be critical. In fact, this company generally perceives as high or medium the potential impact on business of cyber and information risks. When risks actually disrupt the operational life of the company they produce business critical effects, able to put in jeopardy their competitive advantage.

"The impact of cyber risks on our business can be problematic, because we base the majority of our operations on information on products and processes, which needs to be safeguarded." (Company A)

A recent example is represented by the disclosure of confidential information (a picture) on the design of a new variant of a top-selling product that was posted on social media by an employee and quickly became viral. Even though the intention of this employee was only to share "great news" with friends, this caused repercussions on the launch of the new product, on the promotional campaign and on the entire supply chain. A limited array of actions could be undertaken. To contain the negative effects of the leakage, some details on the product and its packaging were changed by working together with suppliers, a refreshed advertising campaign was produced and then shared with retailers in order to avoid disappointment with consumers. To make this possible, the company had to rely on the very strong relationships they have with key customers and suppliers to allow this changes. This shows how important a set of strong relationships with key partners is to ensure a quick reaction for a speedy recovery according to the principles of resilience.

"When it (an industrial secret) is out there…it's out there! You can't do much at that point." (Company A)

Company A is introducing as a consequence of this event additional training for employees, through a programme that enables employees to identify sensitive assets throughout the supply chain in terms of intangible assets and intellectual property. It aims at providing supply chain simulation cases on the impact that non-compliant behaviours can have on the company's competitive advantage and the management of relationships with suppliers and customers. The intention is to extend the scope of these simulations also beyond the traditional dyadic relationships to facilitate a better understanding among trainees of the supply chain implications at a network level. This would create the conditions for a more cyber resilient supply chain especially to prepare participants to potential disruptions and allow them to maintain a robust steady-state.

Company A sees the main sources of risks (both malicious and non-intentional) laying internally to their business and from their supply chain partners. The level of protection is perceived as even lower when the whole supply network is concerned, especially with relationships beyond Tier 1. In fact, they feel it would be more difficult to become aware of disruptions when they have no direct visibility on the processes, procedures and security initiatives in the distant stages of the supply chain. They do

work with contractors in order to share security policies and they ask contractors to comply with them. Additionally, they sign collaborative agreements for sharing information on security incidents and continuity plans and they conduct audits on supply chain partners' security (asking the partner to provide evidence of the adopted security procedures, especially when data storage and sharing are concerned). But all of this happens upstream only and not beyond Tier 1. Still, they don't feel they have full "control" or visibility on what really happens beyond that stage.

To confront the risks, Company A has a proactive approach to SCRM, and the responsibility for this process is given to the various business units. This approach is translated into practice through the deployment of periodic risk assessments at business unit level, which concurrently take into account the downstream and upstream supply chain. They produce enough information to generate specific scenario analyses, with particular emphasis on the potential impact of the detected sources of risks. The ownership to the business unit level allows for a more agile response to local problems. There is a shared ownership of the SCRM process: the operations department along with the market operations. This solution allows for a global coverage of the risks, encompassing the supply, the manufacturing and distribution sides. As far as the ownership of the CSCRM process is concerned, Company A declares an involvement of IT, operations and market operations. The interaction between IT and operations can be "bottom-up" when operations proactively trigger the development of specific procedures or initiatives for addressing local needs, as for the case of a project for sharing master data with one key supplier, which required the activation of a dedicated protocol for data transmission and storage; it can be "top-down" when IT develops organization-wide solutions to respond to top management's requests.

"It should be a shared development process among departments: we, from operations/supply chain, know what it should be done and what we need for making the supply chain work upstream and downstream. We know that IT know how it should be done, they know how to guide and translate our requirements, pointing out technical details that we're not able to see." (Company A)

Consistently with their perception of high impact on business of cyber and information risks and their proactive approach to risk management, Company A adopts a comprehensive range of initiatives. However, a lower level of adoption of organizational initiatives emerges from our data. While the general information security principles are included in the corporate strategy to align with the business needs and shared across departments, our interviewee declares that no visibility of plans for investments or improvement initiatives on cyber and information security is present, since this appears to be an IT domain. The other organizational initiatives seem not to be essential since top management (responsible for those decisions) probably feel that the current wide spanning approach and adoption of initiatives are already fit for purpose and meet their security needs.

Company B

Company B shows a low-medium perception of both probability of occurrence and impact on business coming from cyber and information risks, as it is felt that the real criticality lies in keeping customers' records uncorrupted and secure. They especially perceive this, since they are a logistics service provider. They handle data related to customers' activities for carrying out their logistics operations, and consequently they need customers to trust their ability to handle and store data in a secure way.

Company B believes that the same sources of cyber and information risks can be both malicious and non-intentional. They point out that almost all players in the supply chain can represent a source of risk, since sharing of data is essential for doing business in the supply chain. Customers are seen external to this process, while suppliers and contractors can be problematic when subcontractors and the network of suppliers beyond Tier 1 are concerned. However, according to the interviewee it is necessary to find a compromise that allows companies to run their activities smoothly.

"People along the supply chain handling data can be a risk, but you cannot become too paranoid otherwise you cannot do business" (Company B)

This compromise is achieved through a reactive approach to CSCRM, led by IT and finance departments, which is implemented by means of contingency planning. Supported by the headquarters (providing guidelines/general policies), the business units are empowered to operationalize the plans when it is required by adverse situations, with the aim to adaptably contain and reduce their impact on business, even though these actions are mainly internal to the company.

"We had a data leakage problem a few years ago, when one of our former employees joined a competitor and downloaded our customers' data on his laptop before leaving. While checking his laptop our IT guy detected this massive download. As a security policy, we deactivated data storage on USB sticks and other external devices so we knew that data shouldn't have gone far away. To contain this problem we formatted his laptop and erased all attachments in his e-mail *account. Apparently it worked as no effects were detected." (Company B)*

As a lesson learned from this incident, Company B reinforced restricted user access within the organization, and in case of subcontractors, they also restricted download and print of data, allowing read-only functionalities. In this case it was the incident to trigger the adoption of security initiatives. However, our interviewee pointed out that in the majority of the cases, customers are the ones driving their privacy and security policies, by setting the principles for storing and using their data.

Consistently with the reactive approach to CSCRM, Company B seems to focus primarily on event management initiatives and on IT security tools. This shows an approach to resilience that focuses

only on the "respond" principle, and still a multi-stage concept is not applied in their practices. However, this company recognizes the need for further developments in the area of training, internal awareness and external collaboration with additional initiatives of people management and mentoring and additional collaborative initiatives with subcontractors and customers. This could be facilitated if a clearer relationship between the investment in this sort of initiatives and the related benefits (both tangible and intangible) existed.

"It's a problem of resources and mind-set along the supply chain. You want to work collaboratively with everyone upstream and downstream, but you want to see the results of your efforts" (Company B)

Company C

Company C presents a profile where probability of occurrence and impact on business are both seen as relevant. This company seems to be aware of the dangers coming from all sort of risks, while they put a special emphasis on the probability of occurrence of those risks related to the theft of intellectual property, crash of their website and failure of the IT network. This seems to be due to the incidents they recently had, which made them aware of the unpredictability of cyber risks and the consequent effects.

"We operate in a tough environment and any disruption can be fatal. It's also a hostile environment, where attacks can come when (and from whom) you don't expect. We recently experienced an incident causing the unavailability of service of our system for three working days. This had severe repercussions on our business, and we fought to get back to normality. A very good lesson learned, we won't let it happen again!" (Company C)

The attack implied the loss of the website and the capability to send/receive e-mails. The domain registry was hacked, the system settings changed and the access security records deleted. As a consequence, the company was unable to send or receive any sort of communication/data from/to suppliers and customers. All planning and execution activities, including live tracking of shipments and invoicing, were blocked. Investigations were carried out and it was discovered that the attack came from an insider. It took three days to restore the system with its functionalities in a multi-site environment, which involved coordination of IT recovery operations across sites. Continuity plans in terms of emergency (telephone) communications were put in place with customers and main subcontractors so that the already planned deliveries could be completed and that urgent orders could be manually managed. A concern raised by our interviewee regarded the fact that they're not completely sure of the presence of similar instruments adopted by other supply chain players, in case of adverse situations.

Customers and subcontractors are seen as relevant sources of cyber risk by Company C, especially in terms of lack of control on how data is managed and used and how collaborative procedures for managing passwords and security access information are managed. Competitors and cyber terrorists are perceived as potential disrupting elements, which can lead to malicious attacks. They see a variety of non-intentional sources, such as power outages and technical problems, as potential internal issues.

Company C stressed the relevance of adopting mixed proactive and reactive approaches to SCRM. The aim is to generate the big picture and be prepared to unforeseen events, to be responsive in case of immediate calls for action and at the same time to be able to maintain a steady-state according to the principles of resilience. This approach is reflected in the level of centralization of the SCRM process, which combines the leading support of the headquarters with local planning and execution responsibilities to business units. Coherently, a range of tools is adopted, including business continuity plan, scenario analysis and decision trees. Owing to the overall approach, the SCRM and the CSCRM ownership is shared among various departments. The human resources department is also involved in driving the key role that the "human factor" can play during adversities and to retain oversight of social media and communications with partners in the supply chain. This kind of solution is also aimed, according to the company, at trying to overcome the communication limits across the chain of supply and go beyond Tier 1 to manage crises by means of social media and their vast reach.

Coherently with their perception of the main cyber and information risks Company C adopts a wide range of initiatives, ranging from organizational actions to IT security tools and operational resilience. From a supply chain point of view, they adopt initiatives spanning from upstream to downstream. They require their subcontractors to comply with their security policies in terms of data management, privacy and disclosure restrictions. Even if they do not conduct security audits on subcontractors, they rely on ISO 27000 certified companies only. Downstream they have to comply with the security policies of their customers; even though the compliance process is mainly customer driven, they have a proactive approach to this, which implies that they promote their solutions to customers as facilitators of integration, through collaborative agreements based on secure data sharing via developed/customised interfaces. From the event management perspective, Company C has communication procedures in place along the supply chain. In particular, incident logs are produced and shared with partners where appropriate: these include risk registers, details on operations, implemented recovery actions (from a managerial and IT perspective) and achieved results. Again, concerns were raised about the presence of similar approaches in the extended chain of supply.

Company D

Company D shows a medium-low perception of both probability of occurrence and impact on business of risks. However, they have a higher perception of probability and impact of risks related to the IT system since they rely on a massive amount of data for their international shipping operations

managed through the system. The same was not said about their website, as it was admitted that they probably don't use the website enough for commerce but mainly for providing information. It would be expected to move more activities with customers through a web portal in the future, and risk would certainly rise.
Company D recognizes the relevance of non-intentional risks, and points out that these sources of risk can be difficult to be protected against. According to our interviewee, current employees can be trusted against malicious attacks, but it was pointed out that unintentional situations have occurred.

"We trust our people but we had unintentional cases where e-mails went out to the wrong person disclosing sensitive information, or when someone turned the firewall off to speed activities up." (Company D)

Being a shipping company, they feel exposed to sources of risk coming from foreign nation states, intelligence services and hackers/hacktivists. This is especially critical, according to our interviewee, when they have to exchange information at ports with port operators, which are perceived as vulnerable to cyber-attacks. In many cases around the world their communication channels are outdated or relying heavily on unencrypted satellite communications. This creates situations where port operations can be hacked and blocked with repercussions on the service level provided by the company. Company D says they are always proactive, and devolve the process to the local level to deal with location specific issues.

"We tend to react by building our actions on the specific needs of the situation and of the location where we're operating: we need to be flexible in the way we respond when things go wrong, otherwise we struggle to recover." (Company D)

The plans are shared throughout the firm for best practice and reviewed semi-annually by top management. There are no specific tools that the firm employs, as each case is reviewed on a case by case-by-case basis. In Company D the logistics/operations group is highly involved in the SCRM process. The finance department is also involved, but mainly focuses on issues relating to currency fluctuations. Top management and IT are the only departments involved with CSCRM.
Company D shows a focus on IT security tools, IT operational resilience and event management, while it lacks of engagement internally with organizational initiatives, training and awareness, and data management. Hence, it seems that this company only partially complies with the principles of a multi-stage approach to resilience.
However, they subscribed to an insurance policy for their data, and declared that this is connected to the nature of their business rather than coming as a request by supply chain partners. Company D

thinks that most employees are cyber-aware, but acknowledges the relevance of non-intentional behaviours that need to be addressed through appropriate training programmes.

"An errant click on an e-mail attachment could introduce a virus and damage the system. Participating in this study has prompted a rethink on providing an awareness training programme, even if informal, with e-mail notices of cyber issues." (Company D)

Externally, Company D recognizes the need for improving the level of compliance and awareness along the chain of supply, but this requires also an effort from supply chain partners. On one side, they require their customers and subcontractors to comply with their security policies in terms of data and communication encryption. While larger customers are usually aligned with these requirements, smaller customers and subcontractors tend to be more problematic in this regard, and they tend to lose control and visibility on their actions and initiatives. In those cases Company D includes communication protocols to reduce the risks of uncontrolled flows. On the other side, given the vulnerability of ports, they have introduced some intelligence for mapping the more vulnerable ports. If possible they tend to avoid them (usually smaller ports). Larger ports are perceived as more secure but relying only on those ports can have effects on the optimization of the shipping operations, with repercussions on costs and service level. They wish they could establish collaborative agreements with customers (especially) to allow an allocation of flows that encompasses concurrent considerations on cost and service but also risk to build a more resilient allocation of the flows. According to our interviewee, better visibility on the return of investments related to the implementation of such initiatives would facilitate their adoption.

"Securing the supply chain is a two-way street with both customers and suppliers checking/auditing each other. It takes time and effort to achieve something, all the parties involved need to see the benefits." (Company D)

Company E

Company E generally regards probability of occurrence as low, while it seems to view the impact on business of cyber and information risks as critical for some risks only. In particular, crash of website and failure of company's IT network are perceived as the most crucial ones, as you might expect for an online retailer, with the website and IT systems being the "lifeblood" of the company. They also pointed out that although the probability of the website crashing was low, this was due to the large team in place to make sure this event does not happen, or if it does, they can react and recover as quickly as possible.

"We work on-line. It is vital for us to have our e-commerce platform always working securely. For this reason we have a dedicated team to keep the website secure, or to rectify problems in minutes if and when they arise." (Company E)

They also point out that according to their perspective within the supply chain, maintaining secure customer records is critical due to the trust customers (final consumers for them) put in the company when they buy online. Company E recognises that consumers are very aware of cyber risk and identity theft. Although data is encrypted and thus the probability of occurrence is seen as low, there is a perceived risk that must be dealt with, especially in terms of impact on the reputation and credibility of their whole supply chain. Company E notes that their website/IT system is constantly being attacked/probed, and these attacks are recorded in appropriate logs, but it hasn't brought the site down yet. The impression is that these intentional attacks are on the rise. There has been the occasional technical outage, but any have been of short duration. Again, they point out that there is a dedicated security team (including IT) to deal with these threats.

To confront these challenges, Company E has tried to put in a proactive SCRM system in the beginning, in an attempt to adopt a multi-stage approach to resilience. However, the company now states to being reactive to new threats mainly through ad-hoc interventions for containing the impact of disruptions (e.g. looking for alternative suppliers or service providers when the main ones are not available), focusing mainly on the "respond" and "recover" phases of supply chain resilience. Decisions are taken centrally at the headquarters level, and the ownership of the SCRM process is shared between top management and operations/logistics. Specific tools for SCRM are not adopted as the involved departments feel they are under resourced.

"We would like to use more tools and approaches for managing supply chain risk, especially mapping tools, but we would need more resources for developing and implementing these tools. If we had those tools in place we could be more aware of the potential threats and be proactive in managing unexpected event, instead we're just firefighting bad events." (Company E)

As far as the ownership of the CSCRM process is concerned, various departments are involved, including IT, finance and purchasing, while the supply chain director is accountable. Coherently with the adopted reactive approach and their perception of the criticality of their e-commerce platform, Company E adopts a wide range of initiatives, mainly focusing on IT operational initiatives, IT security tools, data management and event management. It is interesting to underline that Company E is the only one in our sample employing the role of CISO in their organization. Again, this may be connected to the above considerations related to their focus and activities, and it could represent a basis for developing a more pervasive approach to cyber resilience that could overcome the limitations above mentioned. In fact, currently other organizational initiatives, training and internal

awareness are less adopted. From a supply chain perspective, Company E declared that downstream, since they're directly consumer facing, they don't have in place traditional tools to require customers to comply with their policies. However, they offer security solutions to consumers (e.g. requirements on the strength of the password when customers open an account, secure payment channels, encryption of data). Upstream, they require suppliers and contractors to comply with their privacy and security policies, but they do not undertake any collaborative initiative with them. Our interviewee explained that the large number of upstream players in their supply chain adds to the complexity of implementing such initiatives. This hinders the adoption and promotion of collaborations along their supply chain towards enhanced supply chain resilience in the cyber space. They claim that this is even more critical when relationships that go beyond the dyad of Tier 1 are concerned. As a consequence they leverage the internal IT security side to deal with and resolve potential issues.

Cross Case Analysis

Cyber and information risks in the supply chain

By concurrently analysing the whole sample, data show that the probability of occurrence of the main risks is perceived as lower than the impact on business. It appears that companies are more worried about the effects of incidents than the chance of incidents happening, even if literature reports that incidents are growing in frequency (Gaudenzi and Siciliano, 2017).

This seems especially true for those risks such as customer records compromised and the failure of companies' IT network. These are perceived as the most disruptive ones by the sample companies, and with the latter being also generally perceived with a high level of probability of occurrence. It seems that the perception of cyber and information risks is mainly related to the IT infrastructure side, consistently with the involvement of IT in all companies. From a supply chain perspective, the concerns regarding customers' records compromised could be due to the impact on reputation and competitive advantage that a cyber-attack could have downstream in the supply chain, especially given the negative effects that could jeopardize the relationships with customers.

It could be expected to see a similar attitude also with respect to the upstream stages of the supply chain. However our sample companies are less concerned about risky events that could affect suppliers' records. By looking at the nature of the companies, Company A (manufacturer) and Company E (retailer) show high perceptions of the impacts of cyber and information risks on their business, while Company B and Company D (logistics service providers) have a low/medium perception of both the probability of occurrence and the impacts. Company C (logistics service provider) shows a higher level of perception of risks in general, and this could be linked to the fact that they've been recent victims of attacks.

We propose that that the exposure to incidents affects the level of perception of risks, raising the level of awareness compared to other players, especially as far as the effects of incidents are concerned.

This is something suggested by the literature (Järveläinen, 2013), but reinforced by our findings that present an original view by means of novel data gathered during our case studies.

Main sources of cyber and information risks

From an overall perspective, all companies clearly identify the presence of the so-called "enemy within". Employees (current and former) are seen as a main source of cyber and information risks, due to both malicious and non-intentional actions. It is interesting to notice that according to our interviewees, also non-malicious behaviours by employees are a considerable source of cyber and information risks. This seems to be a common feeling across the sample, probably given the difficulty in controlling risks connected to these sources when they inadvertently put their companies at risk. Our work enriches the current body of knowledge by presenting these findings that find confirmation in the literature, as highlighted also by Happ *et al.* (2016): we offer insights that clearly show how in several occasions employees do not even realize they have been manipulated and or that they have inadvertently disclosed sensitive information, so it seems they're not "prepared" according to the principles of supply chain resilience. This lack of "preparedness" could also mean that companies are not completely aligned with an evolutionary resilience approach, given that they seem to struggle in having an adaptive capacity to the changing situations in their own workforce.

We propose that, even if a source of cyber and information risk lies internally to the focal company, the effects of risky events generated by this source cannot be contained within the boundaries of the company itself and spread across the whole chain of supply, both upstream and downstream. These events represent actual "black swans", which are challenging to recover from when they occur (Gaudenzi and Siciliano, 2017), as the examples of Company A and Company C demonstrate.

A commonality emerging from our analysis that adds to the current body of knowledge on cyber and information risks lies again in the supply chain perspective. In fact, across the sample there is a consensus on the criticality of those sources of risks that lie in the upstream stages of the supply chain, especially when suppliers or contractors beyond the Tier 1 are concerned. One of the main literature-acknowledged barriers to enhanced supply chain resilience (i.e. lack of visibility – Ali *et al.*, 2017) emerges from our cases.

Building on our findings, we propose that especially when subcontractors and the other players in the distant stages of the supply chain are concerned, lack of visibility and control makes these supply chain players to be perceived as a major source of cyber risk (both malicious and non-intentional actions). These sources can be represented also by critical infrastructural nodes (e.g. ports) and organizations handling data there (e.g. port operators), as shown by the case of Company D and their concerns on ports/port operators and the related cascading effects due to cyber disruptions. Companies feel particularly exposed to risks coming from these distant sources, especially because they feel that their Tier 1 partners are not always able to have full control, as pointed out by Company

B. Concerns regard also how risk propagates and migrates upstream and downstream in the supply chain, as a consequence of lack of visibility, coordination and control in the extended supply chain. This constitutes interesting evidence, which goes beyond the insights proposed by the literature in the works by Han and Shin (2016) and Tukamuhabwa *et al.* (2017). Our work offers a more holistic view on the end-to-end interactions among supply chain actors and on the mechanisms driving these relationships. From a practical view, our findings also stimulate companies in supply chains to extend their traditional arm's-length transactions towards more coordinated approaches to supply chain resilience at a network level, with the aim to overcome the mentioned barriers preventing companies from achieving enhanced resilience (Ali *et al.*, 2017).

Approaches to SCRM and CSCRM

From an overall perspective, from the performed interviews it appears that companies are aware of the growing importance of cyber and information risks in the supply chain. They also acknowledge the significance of adopting a structured holistic approach to manage them, offering a novel view from the field that shows an interesting alignment with the literature (Bartol, 2014; Soomro *et al.*, 2016).

Notwithstanding this unanimous recognition, our cross case analysis shows that a consistent approach to SCRM is not adopted across the sample companies, and a mixture of reactive and proactive approaches can be detected. This is tightly connected with the approach to the concept of supply chain resilience adopted by companies. From a combined view of the findings, it appears that only a few companies have a focus that embraces all the phases of resilience discussed in the literature, while others tend to concentrate more on the "respond" and "recover" phases (Ribeiro and Barbosa-Povoa, 2018). This focus on the "respond" and "recover" phases seems to suggest again that companies haven't developed that long-term adaptive capacity (Davoudi, 2012) yet, so they are not able to be "prepared", to "maintain" and to adapt to the continuous changes and inner tensions of a turbulent environment such as the one studied in this research. In this sense, our work presents an interesting contribution to theory and practice, since it offers insights on the level of development of this adaptive capacity by companies, when it comes to cyber and information risk management, while the literature is lacking of discussion on this area.

It seems that more uniformity is present with reference to the level of centralization, with the headquarters supporting business units for facing local needs in the majority of the cases. In terms of ownership, it is interesting to notice that consistently with the level of centralization above, there is a considerable involvement of top management in the ownership of the SCRM process (mainly for sponsoring and reviewing purposes). We note also a widespread involvement of operations, supply chain and logistics in terms also of accountability. However, this level of involvement of the supply chain-related functions is not reflected in the ownership of the CSCRM process. The IT department is involved in the CSCRM process within all the investigated companies. On the contrary, only in

Companies A and Company E supply chain related departments have a relatively active role in the concerned matter, with the supply chain director involved at Company E.

This partially confirms the existing literature, which reports the commitment of IT (e.g. BCI, 2016), but also extends it by showing that currently some companies are moving towards a more holistic approach to CSCRM in their organizational structure, allowing for a richer set of supply chain-related details that inform the CSCRM strategy (Soomro *et al.*, 2016). A good example of how this can be achieved is represented by Company A and their mixture of "bottom-up" and "top-down" approaches in the development of IT initiatives for managing risks along the chain of supply: this allows the supply chain world to feed relevant information on their security needs into the technical world of IT.

However, the supply chain department is not fully involved yet in the decision making process concerning investments to CSCRM. As a consequence from our cases it seems that the majority of investments mainly regards the IT domain. It also emerges from our case companies that the adopted approaches do not envisage any involvement of customers and/or suppliers in the design and implementation of initiatives. So they tend to be rather limited in the scope of the involvement of parties external even to the focal company. According to the literature this "isolation" in the approach to the decision-making process could potentially prevent companies from achieving resilience (Ribeiro and Barbosa-Povoa, 2018). Through our investigation, we also found that this isolation also prevents companies from being prepared to change and from being able to continuously adapt to the tensions present in the overall supply chain beyond the dyad, and this constitutes an important extension to the current theory and practice.

Hence, it appears that the management of cyber and information risks (within companies and along the supply chain) is mainly seen as a domain of the IT department. Building on the collected evidence, it emerges that decision making is led by IT and in isolation from supply chain partners: hence, we propose that this leads to ignore supply chain dynamics and ultimately it negatively affects supply chain resilience.

Companies' initiatives to manage cyber and information risk in supply chains

By concurrently looking at the adoption of initiatives as reported in Table 6 as a whole, it immediately appears that event management initiatives are fully adopted across the whole sample. This indicates that all companies have in place procedures and processes to manage the consequences arising from a risky event. This seems to be in line with the literature (BCI, 2016), which reports that a large number of organizations have business continuity arrangements in place to deal with cyber and information risks and responds to the principle of situational awareness (Herrera and Janczewski, 2015).

However, our evidence suggests that companies are not sure about "how far" these initiatives can go and reach the network especially beyond the dyad. They also question if these initiatives are bi-directional through joint relationship efforts (Scholten and Schilder, 2015), or only pushed by the proposers without any guarantee on the reciprocity of the approach (as highlighted by Company C).

This seems also to suggest that companies have developed an approach to supply chain resilience able to cover the "respond" and "recover" phases only (Ribeiro and Barbosa-Povoa, 2018), but not to develop a long-term adaptive capacity to address not only disturbances but also continuous changes. Categories such as data management (especially in terms of control measures on user access), IT security tools and IT operational resilience show a higher degree of adoption across the sample, compared to categories such as organizational initiatives, training and internal awareness, and compliance and external awareness.

This suggests that the majority of CSCRM initiatives seem related to the IT domain. It also suggests that organizations seem very much focused on "firewalling themselves", rather than leveraging a wider range of initiatives to extend the protection from cyber and information risks to the supply chain beyond the focal company and the dyad. While this is confirmed by Linton *et al.* (2014), our findings also confirm that there is lack of a holistic approach to the subject matter, as indicated by Soomro *et al.* (2016), and provide a picture that clearly shows the boundaries of companies' actions, extending what it is available in the literature today.

This is also reflected by the details of the adopted organizational initiatives. The sample companies haven't yet introduced the adoption of the "chief information security officer" (CISO) as a formalized professional role, apart from Company E, which pointed out that this is something related to the strong focus of the company on the e-commerce world. The other interviewees pointed out that a step-change towards a more holistic, pervasive and wide-spanning approach to CSCRM could occur with the presence of a CISO, with better integration and involvement of the different organizational units. Internally, it is felt that the operations/supply chain departments could have a greater involvement in the CSCRM process. According to the interviewees, these departments are not necessarily supposed to lead the CSCRM process, while the CISO should be the "champion", i.e. the most suitable professional taking a coordinating role between the IT department and all the other business functions. The involvement of the operations/supply chain departments is essential in the definition of the requirements of appropriate IT systems and identification of the criticalities when sharing and managing data in the cyber space with supply chain partners. Externally, this would allow facilitating the involvement or communication with suppliers and customers, and providing an understanding of the supply chain dynamics to promote the CSCRM initiatives beyond the boundaries of the focal company stretching also beyond the dyad. This could also enable the development of a long-term adaptive capability according to an evolutionary resilience view. Hence, our work offers an important extension to the existing knowledge and to the current practice, by offering a novel view on the role of the CISO and the architecture of the relationships in the supply chain with reference to the management of cyber and information risk according to a more holistic approach.

The discussed points would have positive implications also from the perspective of external awareness initiatives. From the collected evidence, it appears that companies are able to manage external awareness initiatives up to a certain point, which in the majority of the cases is represented

by the first tier, i.e. dyadic level. Companies can generally achieve a certain degree of alignment (Pradabwong *et al.*, 2017), by requiring suppliers and customers to comply with their security policies. In some cases they conduct security audits on supply chain partners and devise collaborative agreements/arrangements with supply chain partners for security (see for example Company C).
However, as mentioned above, they all declare to be unable to extend the concept of alignment beyond their direct contacts, in other words beyond the dyad. This confirms that an extended holistic approach is still something missing also with reference to this category of initiatives. It seems that all the case companies invest on securing the supply chain both upstream and downstream, with the latter often driven by customers as shown in the case of Company B. But when they are the ones driving the implementation of formal compliance audits along the supply chain, besides facing challenges in going beyond the dyad, it appears that they tend to struggle in operationalizing the idea of compliance. They also seem to be hampered by the trade-off between security and performance of communications and execution of activities at supply chain level, as declared by Company B. Hence, we propose that the presence of the CISO working closely with the supply chain department could facilitate a more holistic view of the whole CSCRM process, allowing for: moving away from the "IT domination"; overcoming decisions taken and initiatives implemented in isolation within the focal companies; developing a long-term adaptive capacity; and ultimately leading to better cyber resilience in the supply chain beyond the dyad.

Better supply chain resilience can also be achieved through supply chain coordination (Ali *et al.*, 2017), which in turn can be built on synchronization and shared and mutually-created knowledge (Herrera and Janczewsky, 2015; Scholten and Schilder, 2015). These factors are not completely reflected in the set of adopted initiatives by the sample companies. If, on one hand, sharing information and data to create that shared knowledge is recognized to improve supply chain efficiency and effectiveness (Kembro and Selviaridis, 2015), on the other hand collaborative agreements/arrangements with supply chain partners are essential for companies to be reassured that data and information sharing will not negatively impact their level of security and privacy, as stressed by the literature (Barkataki and Zeineddine, 2015). On the contrary, it could also prove to be a tool for strengthening the level of protection and trust as leverage for better managing incidents and allowing for better resilience (Ali *et al.*, 2017). Such an approach should extend beyond the supply chain to embrace the whole supply chain network beyond Tier 1, including subcontractors, suppliers, and also customers.
However, from our analysis this seems to be very far from being a reality, and this constitutes evidence not present in the current body of knowledge. It also appears to be a common pattern among the sample companies, regardless the stage of the supply chain in which they operate. The sample companies (see for example Company E) highlighted that this could be linked to the level of complexity of their connections with suppliers, especially when the tiers beyond the dyad are

concerned. Consequently they prefer to protect what they directly "see" instead of trying to manage the complexity of their connections upstream, through methods and tools for reducing this complexity and prioritizing the most critical links. The "natural" loss of control and visibility of data and information as you move further up or down the supply chain should be compensated by the trustworthiness (Windelberg, 2016) of appropriate secured data sharing systems and collaborative processes (Barkataki and Zeineddine, 2015). Hence, we propose that conformance to standards, certifications and collaborative practices for a more coordinated approach at the network level could also facilitate more information sharing across the supply chain at network level, assisting in the exploitation of the value of information for better resilience.

Another piece of evidence emerging from our cross-case analysis is the necessity to introduce training programmes for employees, to educate them in the correct use of the available technology, tools and systems (cyber hygiene). Given the raising concerns about the "enemy within", companies seem to be considering the implementation of appropriate internal security awareness training programmes for employees.

However, as it emerged in the case of Company A, training shouldn't be only focused on an internal development of people, but should empower employees to appreciate the impact of their behaviour and actions on the entire supply chain (e.g. by delivering training programmes and simulations able to tackle these challenges and to help employees in breaking the boundaries of their workplace). Hence, we propose that this kind of initiatives should be shared with supply chain partners to allow for a more "educated" supply chain overall, which would lead to a supply chain better "prepared" and able to "respond" and to continuously adapt, according to the evolutionary resilience view.

In fact, people need to be educated to avoid cyber security non-compliant behaviours, usually more convenient, less time consuming and perceived as more productive in terms of performance and speed of business. A common non-compliant behaviour is to look for better network performance by disabling protection tools (e.g. antivirus, firewall), which generated a debate in the literature on the trade-off between network security and performance (Intel Security, 2014). In line with the literature (Windelberg, 2016), these cyber security non-compliant behaviours are also connected to deliberate choices based on implicit trust assumptions, which lead to underestimating the consequences of actions internally but even more importantly on the supply chain, and to be "unaware victims" of social engineering attacks.

Finally, in the selection and implementation of appropriate initiatives, it emerged from our sample companies that it is important to identify a good fit between investments in these initiatives and the level of cyber risks in the supply chain. As suggested by the literature, this fit, which is defined as balanced resilience, is affected by the nature of the business and its supply chain (see for example the case of Companies D, which adopted a data insurance product given the nature of their business).

From our interviews it also emerges that this balance should be explicitly shared with supply chain partners. In this sense, in a connected supply chain the concept of balanced resilience should evolve in the concept of cyber supply chain balanced resilience, which represents another novel element emerging from our original work. This can be expressed as the focused application of the mentioned "right fit" between level of risk and investments in SCRM process to the cyber space that connects the supply chain players at a network level. From our study, it emerges that at the moment companies tend to work on the balanced resilience at a firm level, extending in some case at a dyadic level with Tier 1 partners. Hence, we propose that the extension of the balanced resilience concept to embrace the supply chain network would lead to improved CSCRM, and in this sense we extend the current knowledge through the proposal of the new concept of cyber supply chain balanced resilience. Literature recognizes the value of extending this concept to the network level (Hanf and Dautzenberg, 2006; Pradabwong *et al.*, 2017).

Conclusions

In this research we addressed the management of cyber and information risks in todays connected supply chains, through multiple case studies, with the aim to push the boundaries of supply chain research and practice. This allowed extending and developing the theory on the subject area as a combination of SCRM and resilience, and information risk management. In doing this we also filled the identified gap in the literature, which lacks of contributions that address CSCRM from a supply chain and not solely from a technical perspective, and we extended supply chain knowledge beyond a dyadic perspective.

Our study in fact furthers our understanding of the subject matter, laying the first foundations to shed light on the studied phenomena and it stimulates further research on the topic. Also, our investigation provides the scientific and industrial communities with empirical data on this under explored matter, embracing the challenges posed by rapidly changing technologies that directly affect supply chain management. This investigation provides both theoretical and practical implications.

Theoretical implications

To begin with, this study contributes to theory by extending the current theory on the field through a combination of the theories on SCRM and resilience and information risk management. It adds to the SCRM and resilience theory since it is specifically focused on one of the main risks (i.e. cyber and information risk) that are now very high in the agenda of companies (Trombley, 2015), and that have been recognized but overlooked by the literature (Rajagopal *et al.*, 2017). It adds to the information risk management theory since it addresses the complex issue of cyber and information risk in massively connected environments through a holistic approach including technology, people and processes at an extended supply chain level that goes beyond the dyad. As a result, researchers can

now appreciate the uniqueness of CSCRM compared to the traditional approach to information risk management.

Second, this is one of the first studies focusing on the concept of supply chain resilience connected to cyber and information risk management, which is something missing in the existing theory on supply chain resilience. Building on the definition of supply chain resilience and related theory, this study has investigated how the concept of resilience and its phases are deployed in the CSCRM process. Our empirical results show that the advocated multi-stage approach to resilience including the phases of "prepare, respond, recover and maintain", leading to a long-term capacity to adapt to continuous changes and inner tensions of today's complex systems, is far from being pervasively adopted. Companies in fact, appear to be focused mainly on the "respond" and "recover" phases. It also emerged that resilience driven actions and related CSCRM initiatives have been implemented by companies in isolation, and consequently this seems to prevent organizations from achieving resilience at a supply chain level as far as cyber and information risks are concerned.

Third, our study stresses the importance of understanding the role of people in the supply chain within the CSCRM process. Previous research has identified human resources as pivotal elements for advancing information management in companies and communities (Happ *et al.*, 2016). However, as an extension to the existing theory on SCRM and information risk, our research showed that the impact of human behaviours can hardly be contained within the boundaries of the single organizations or dyadic relationships, but on the contrary can generate risky events that affect the supply chain at a network level. It also showed how difficult predicting or controlling the related risky events and consequences is when these propagate across the supply chain. This is especially true due to the complex and massively connected structure of modern global supply chains, which calls for an extended holistic approach leading to enhanced resilience.

Fourth, our investigation extends the current theory on the subject by providing an overall view of the approach to the deployment of cyber security initiatives. Our results show that companies are mainly investing in IT initiatives, and that decisions regarding the investments on security initiatives are mainly in the hands of the IT department. Existing contributions focus primarily on the punctual implementation of clusters of actions and the underlying decision making process (e.g. Mukhopadhyay *et al.*, 2013; Keegan, 2014; Kim and Im, 2014). From our research it emerges that a holistic approach to the deployment of initiatives is needed. A stronger involvement of the supply chain department in the decision making process (potentially with a CISO leading) is advocated to allow for a pervasive and network-spanning supply chain perspective in the CSCRM process. This could eventually lead to better supply chain resilience also through a better exploitation of the value of information.

An unclear relationship between the required efforts and investments in initiatives and the tangible/intangible benefits coming from their implementation emerged too. This especially applies to those initiatives that go beyond the level of the pure IT solution, software or infrastructural intervention and reach some non-assessed areas such as people working in connected organizations. In

fact, previous contributions are focused on the study of the return on investment or on models for making economically rational information security investments (Yeo *et al.*, 2014). This finding is linked to the relevance of a supply chain perspective, and confirms the need for ways in which real benefits should be isolated for enabling decision making. This should be done also by analysing the level of risk of the supply chain in order to identify the most suitable investment initiatives. This will allow companies to achieve cyber supply chain balanced resilience and to define appropriate cost-benefit sharing mechanisms among the partners of the supply chain, when CSCRM initiatives are adopted in a collaborative way; something that currently is missing in the existing theory.

Finally, existing literature has appreciated the complexity and the multi-faceted nature of cyber and information risks and the related sources of risks (Boyson, 2014), but no previous study has provided a rationalization of these items in order to make sense of this research subject. The present study adds to the existing theory by producing a classification of the main cyber and information risks and sources of risks, built through a literature review that adopts a supply chain perspective. According to this, the extent of cyber and information risks and related sources well beyond the boundaries of the focal company and dyadic relationships emerges, and researchers can use this classification as a reference framework for future investigations. The same applies to the suite of identified initiatives to managing cyber and information risks along the chain of supply. Previous research has mainly provided an overview of the various initiatives in a scattered way and from a technical perspective, and focus especially on the internal side of organizations (Linton *et al.*, 2014; Soomro *et al.*, 2016). By adopting a supply chain perspective, our work succeeds in proposing an exhaustive yet agile representation of the various initiatives that companies operating in connected supply chains potentially have at their disposal for addressing cyber and information risks, going beyond the boundaries of their organizations at a supply chain network level.

Practical implications

First, the imbalance towards the IT side of CSCRM emerged, while the discussed examples show the importance for companies to look at cyber and information risks also from a supply chain perspective given the negative effects of risky events that spread across the chain of supply. Concerns included lack of visibility and control beyond Tier 1 and how risk propagates in the various layers of the supply chain when it originates in distant stages. Hence, managers and employees should stretch their view outside the traditional boundaries of their “silo” activities. Rather than focussing on the technical aspect of CSCRM within the boundaries of the focal company, organizations need to adopt a holistic and extended approach to contemplate the sources of cyber and information risks. They also need to consider initiatives to cope with these risks by looking at the whole supply chain beyond the dyad and at the whole spectrum of factors involved (including people and their potential impact on the entire supply chain). The set of adopted initiatives should contemplate the four phases of the modern concept of resilience (i.e. prepare, respond, recover and maintain). They should also be bi-directional through

joint relationship efforts. It means that all partners involved in a critical link should be involved in the design and implementation of measures to manage cyber and information risks, in order to remove that isolation that prevents from developing a long-term adaptive capacity and achieving enhanced resilience.

Critical links and most problematic "paths" from a cyber and information risk perspective in the supply chain could be identified through tools such as big data analytics, for example. These would allow managing the complexity of the massive connectivity of modern supply chains and allow decomposing the "overall picture" to target the main critical points first. This would permit companies to prioritize their initiatives to extend their CSCRM practices to partners beyond the Tier 1, and facilitate a bi-directional CSCRM process through joint relationship efforts.

The adoption of security initiatives related to the IT technical infrastructure should be considered as a tool for leveraging the CSCRM process, and not the ultimate objective of the implementation of a risk management process. Companies should work on the concurrent adoption of a suitable and secure IT infrastructure combined with the development of collaborative and external awareness initiatives with partners to achieve better supply chain coordination. Through supply chain coordination mechanisms and secure communication tools, companies could leverage the value of information. Information sharing could be exploited as a tool to improve the shared knowledge and synchronization to support the CSCRM process and enhance companies' resilience on all its four phases.

As a further practical implication, managers are urged to invest in people to turn employees from sensitive targets or unaware disruptors to cyber-aware guardians of the cyber security of their supply chain. This should create awareness of the whole set of implications deriving from their actions that, as shown by the discussed examples, have severe and hardly controllable repercussions also on the activities of supply chain partners beyond the dyad. To this aim, the involvement of the human resources department seems to be a relevant factor, as showed by some of the investigated companies.

Moreover, along the same lines, human resources departments could be seen as critical for exploiting their capability of controlling and leveraging the use of social media as tools for sharing and distributing information across the extended supply chain, making the most of the vast reach of these communication media.

Further, for a successful decision making process, companies need to find an appropriate balance between required efforts and costs, and tangible/intangible benefits related to the adoption of the initiatives, according to the concept of balanced resilience as previously discussed. Our findings suggest that this relationship is still quite unclear and consequently as a fourth practical contribution our study invites organizations to explore the trade-off between efforts and benefits. In doing this, a holistic approach is necessary, and consequently the involvement of the supply chain department in the decision making process is crucial for embracing the vast range of implications that CSCRM initiatives can have. At the moment it appears that investment and decisions regarding this matter are

mainly an IT domain. This could be also a driver for implementing collaborative actions where all the partners involved have clarity on the cost-benefit sharing mechanisms and the related required efforts.
As a final practical contribution, the present study provides a complete list of cyber and information risks, sources of risks in the supply chain and initiatives for CSCRM. Managers may be aware of the potential sources of risks and actions to take for increasing the level of cyber security in their supply chain.

Limitations and directions for future research

The main limitation relates to the number of case companies investigated that hinder the generalisability of findings. Hence it would be necessary: i) to increase the number of case studies, and subsequently ii) to carry out a wider questionnaire survey. Another limitation concerns the focus of this study. The set of sample companies is representative and valuable for achieving the objectives of this research, and it allows for results that are not influenced by a specific stage of the supply chain or a specific industrial sector. However, the set of companies is not able to provide deep insights on the implications of CSCRM for different stages of the supply chain and sectors. This could be addressed in future research works that could focus on vertical analyses to better explain the potential reasons underpinning the choices made and the actions undertaken by companies.
Additionally, another limitation of our sample is represented by the fact that it does not include multiple players belonging to the same supply chain. This could be relevant especially when supply chains particularly affected by cyber and information risks are concerned (such as the fast moving consumer goods sector for the amount of exchanged data, or the pharmaceutical sector for the sensitivity of exchanged data). By overcoming this limitation it would be possible to explore the implications for the achievement of cyber supply chain resilience in different supply chain contexts. Also, it would be interesting to conduct analyses able to shed light on the initiatives and coordination efforts for CSCRM within same supply chains at a network level. In fact, our results stimulate researchers to deepen the study of the supply chain coordination mechanisms at network level.
Furthermore, the outcome of the present study opens as a further research stream the investigation on the identification of challenges and drivers to establish an efficient and effective CSCRM process for enhanced resilience in the context of cyber and information risk. It would be interesting to deepen the study of what companies need to do/implement for extending the scope of their CSCRM process beyond the dyad and achieve cyber resilience in the whole supply chain, and what kind of factors can facilitate the overcoming of the barriers to this. To corroborate this aspect, we deem that investigating the relationship between the efforts/investments on CSCRM initiatives and related tangible/intangible benefits for supply chain and organizational performance, through empirical evidence, would be necessary. This should be carried out also along with the development of a cost-benefit sharing framework related to these supply chain relationships. Likewise, the development of appropriate

performance measures to drive and enhance cyber resilience in the supply chain would further help, beyond the prescriptions and indications already provided by the extant literature.

Acknowledgments

This research was supported by a Chartered Institute of Logistics and Transport (CILT) Seed Corn Research Fund 2014 – 2015.

The authors would like to express their gratitude to the anonymous reviewers and to the proofreaders who helped in enhancing the quality of this manuscript.

References

- Ambulkar, S., Blackhurst, J. and Grawe, S. (2015), "Firm's resilience to supply chain disruptions: Scale development and empirical examination", *Journal of Operations Management*, Vol. 33 No. 1, pp. 111-122.
- Ali, I., Nagalingam, S. and Gurd, B. (2017), "Building resilience in SMEs of perishable product supply chains: enablers, barriers and risks", *Production Planning & Control*, Vol. 28 No. 15, pp. 1236-1250.
- Barkataki, S. and Zeineddine, H. (2015), "On achieving secure collaboration in supply chains", *Information Systems Frontiers*, Vol. 17 No. 3, pp. 691-705.
- 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 (2015), "Supply Chain Resilience 2015", available at: http://www.thebci.org/index.php/bci-supply-chain-resilience-2015
- BCI (2016), "Cyber Resilience Report 2016", available at: http://www.thebci.org/index.php/obtain-the-cyber-resilience-report-2016
- Ben-Daya, M., Hassini, E. and Bahroun, Z. (2017), "Internet of things and supply chain management: a literature review", *International Journal of Production Research*, DOI: 10.1080/00207543.2017.1402140
- 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.
- Bode, C. and Wagner, S.M. (2015), "Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions", *Journal of Operations Management*, Vol. 36 No. 5, pp. 215-228.
- Boulesnane, S. and Bouzidi, L. (2013), "The mediating role of information technology in the decision making context", *Journal of Enterprise Information Management*, Vol. 26 No. 4, pp. 387-399.
- Boyson, S. (2014), "Cyber supply chain risk management: revolutionizing the strategic control of critical IT systems", *Technovation*, Vol. 34 No. 7, pp. 342-353.
- Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS quarterly*, Vol. 34 No 3, pp. 523-548.
- Bühler, A., Wallenburg, C.M. and Wieland, A. (2016), "Accounting for external turbulence of logistics organizations via performance measurement systems", *Supply Chain Management: An International Journal*, Vol. 21 No. 6, pp. 694-708.
- Caridi, M., Moretto, A., Perego, A. and Tumino, A. (2014), "The benefits of supply chain visibility: A value assessment model", *International Journal of Production Economics*, Vol. 151, No. 1, pp. 1-19.

- Chen, T.-Y., Chen, Y.-M., Wang, C.-B., Chu, H.-C. and Yang, H. (2007), "Secure resource sharing on cross-organization collaboration using a novel trust method", *Robotics and Computer-Integrated Manufacturing*, Vol. 23 No. 4, pp. 421-435.
- Chowdhury, M. M. H. and Quaddus, M. (2016), "Supply chain readiness, response and recovery for resilience", *Supply Chain Management: An International Journal*, Vol. 21 No. 6, pp. 709-731.
- Christopher, M. and Holweg, M. (2011), ""Supply Chain 2.0": managing supply chains in the era of turbulence", *International Journal of Physical Distribution & Logistics Management*, Vol. 41 No. 1, pp. 63-82.
- Colicchia, C. and Strozzi, F. (2012), "Supply chain risk management: a new methodology for a systematic literature review", *Supply Chain Management: An International Journal*, Vol. 17 No. 4, pp. 403-418.
- Crabtree, B.F. and Miller, W.L. (1999), *Doing Qualitative Research*, Sage, Thousand Oaks, CA.
- Daugherty, P.J., Richey, R.G., Roath, A.S., Min, S., Chen, H., Arndt, A.D. and Genchev, S.E. (2006), "*Is collaboration paying off for firms?*", *Business Horizons*, Vol. 49 No. 3, pp. 61-70.
- Davoudi, S. (2012), "Resilience: A bridging concept or a dead end?", *Planning Theory & Practice*, Vol. 13 No. 2, pp.299–333.
- Ellis, S.C., Shockley, J. and Henry, R.M. (2011), "Making sense of supply disruption risk research: A conceptual framework grounded in enactment theory", *Journal of Supply Chain Management*, Vol. 47 No. 1, pp. 65-96.
- Ellram, L.M. (1996), "The use of the case study method in logistics research", *Journal of Business Logistics*, Vol. 17 No. 2, pp. 93-138.
- Eurich, M., Oertel, N. and Boutellier, R. (2010), "The impact of perceived risks on organizations' willingness to share item-level event data across the supply chain", *Electronic Commerce Research*, Vol. 10, pp. 423-440.
- 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.
- Fine, C.H. (2000), "Clockspeed-based strategies for supply chain design", *Production and Operations Management*, Vol. 9 No. 3, pp. 213-221.
- Fisher, M.L. (1997), "What is the right supply chain for your product?", *Harvard Business Review*, March, pp. 105–116.
- Forrester, J.W. (1962), *Industrial Dynamics*, MIT Press, Cambridge, MA.
- 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.
- Golicic, S.L. and Sebastiao, H.J. (2011), "Supply chain strategy in nascent markets: The role of supply chain development in the commercialization process", *Journal of Business Logistics*, Vol. 32 No. 3, pp. 254-273.
- Gualandris, J. and Kalchschmidt, M. (2014), "Mitigating the effect of risk conditions on supply disruptions: the role of manufacturing postponement enablers", *Production Planning & Control: the management of operations*, Vol. 26 No. 8, pp. 637-653.
- 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.
- Han, J. and Shin, K. (2016), "Evaluation mechanism for structural robustness of supply chain considering disruption propagation", *International Journal of Production Research*, Vol. 54 No. 1, pp.135-151.
- Hanf, J. and Dautzenberg, K. (2006), "A theoretical framework of chain management", *Journal on Chain and Network Science*, Vol. 6 No. 2, pp. 79-94.
- Hao, J. and Cai, W. (2011), "Trusted block as a service: towards sensitive applications on the cloud", *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011)*, 16-18 November, 2011, IEEE, Changsha, pp. 73-82.
- Happ, C., Melzer, A. and Steffgen, G. (2016), "Trick with treat - Reciprocity increases the willingness to communicate personal data", *Computers in Human Behavior*, Vol. 61 No. 3, pp. 372-377.

- Herrera, A. and Janczewski, L. (2015), "Cloud supply chain resilience", in *Information Security for South Africa (ISSA)*, pp. 1-9, IEEE.
- 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.
- Hohenstein, N.O., Feisel, E., Hartmann, E. and Giunipero, L. (2015) "Research on the phenomenon of supply chain resilience: A systematic review and paths for further investigation", *International Journal of Physical Distribution & Logistics Management*, Vol. 45 No. 1/2, pp.90-117.
- Ifinedo, P. (2012), "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31 No. 1, pp. 83-95.
- Intel Security (2014), "Industry Experts Speak Out: The Network Performance and Security Trade-Off", available at: http://whitepaper.techweekeurope.co.uk/resource/industry-experts-speak-network-performance-security-trade-off
- 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.
- Jüttner, U. and Maklan, S. (2011), "Supply chain resilience in the global financial crisis: an empirical study", *Supply Chain Management: An International Journal*, Vol. 16 No. 4, pp. 246-259.
- 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.
- Karlsson, F., Kolkowska, E. and Prenkert, F. (2016), "Inter-organisational information security: a systematic literature review", *Information & Computer Security*, Vol. 24 No. 5, pp. 418-451.
- Keegan, C. (2014), "Cyber security in the supply chain: A perspective from the insurance industry", *Technovation*, Vol. 34 No. 7, pp. 380-381.
- Kembro, J. and Selviaridis, K. (2015), "Exploring information sharing in the extended supply chain: an interdependence perspective", *Supply Chain Management: An International Journal*, Vol. 20 No. 4, pp. 455-470.
- 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.
- Kumar, R., Park, S. and Subramaniam, C. (2008), "Understanding the value of countermeasure portfolios in information systems security", *Journal of Management Information Systems*, Vol. 25 No. 2, pp. 241-279.
- 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, pp. 339-341.
- Luiijf, E., Besseling, K. and de Graaf, P. (2013), "Nineteen national cyber security strategies", *International Journal of Critical Infrastructures*, Vol. 9 No. 1/2, pp. 3-31.
- March, J.G. and Shapira, Z. (1987), "Managerial perspectives on risk and risk taking", *Management Science*, Vol. 33 No. 11, pp. 1404-1418.
- McCracken, G. (1988), *The long interview (Vol. 13)*, Sage.
- Mena, C., Humphries, A. and Choi, T .Y. (2013), "Toward a theory of multi-tier supply chain management", *Journal of Supply Chain Management*, Vol. 49 No. 2, pp. 58-77.
- Miles, M.B. and Huberman, A.M. (1994), *Qualitative Data Analysis*, Sage, Thousand Oaks, CA.
- 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.
- O'Connell, M. E. (2012), "Cyber Security without Cyber War", *Journal of Conflict and Security Law*, Vol. 17 No. 2, pp. 187–209.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers & Security*, Vol. 42 No. 5, pp.165-176.

- 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.
- Pilbeam, C., Alvarez, G. and Wilson, H. (2012), "The governance of supply networks: a systematic literature review", *Supply Chain Management: An International Journal*, Vol. 17 No. 4, pp. 358-376.
- Prabhakaran, M.M. and Sahai, A. (2013), *Secure multi-party computation*, IOS press.
- Pradabwong, J., Braziotis, C., Tannock, J. D. T. and Pawar, K. S. (2017), "Business process management and supply chain collaboration: effects on performance and competitiveness", *Supply Chain Management: An International Journal*, Vol. 22 No. 2, pp. 107-121.
- Prasanna Venkatesan, S. and Kumanan, S. (2012), "Supply chain risk prioritisation using a hybrid AHP and PROMETHEE approach", *International Journal of Services and Operations Management*, Vol. 13 No. 1, pp. 19-41.
- PwC (2014), "Managing Cyber Risks in an interconnected world", available at: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml
- Rajagopal, V., Prasanna Venkatesan, S. and Goh, M. (2017), "Decision-making models for supply chain risk mitigation: A review", *Computers & Industrial Engineering*, Vol. 113, pp. 646-682.
- Reuter, C., Foerstl, K.A.I., Hartmann, E.V.I. and Blome, C. (2010), "Sustainable global supplier management: the role of dynamic capabilities in achieving competitive advantage", *Journal of Supply Chain Management*, Vol. 46 No. 2, pp.45-63.
- 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.
- Robinson, O.C. (2014), "Sampling in interview-based qualitative research: a theoretical and practical guide", *Qualitative Research in Psychology*, Vol. 11 No. 1, pp. 25-41.
- Rushmere, M. (2015), "Hidden in full view", available at: http://www.portstrategy.com/news101/port-operations/planning-and-design/hidden-in-full-view
- Santos-Pereira, C., Augusto, A.B., Cruz-Correia, R. and Correia, M.E. (2013), "A secure RBAC mobile agent access control model for healthcare institutions", in Rodrigues, P.P., Pechenizkiy, M., Gama, J., Correia, R.C., Liu, J., Traina, A., Lucas, P. and Soda, P. (Eds), *2013 IEEE 26th International Symposium on Computer-Based Medical Systems (CBMS)*, IEEE Xplore Digital Library, Porto, pp. 349-354.
- Sarter, N.B. and Woods, D.D. (1991), "Situation awareness: a critical but ill-defined phenomenon", *The International Journal of Aviation Psychology*, Vol. 1 No 1, pp. 45-57.
- 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", *IEEE Computer Society*, Vol. 47 No.10, pp. 82-85.
- Sheffi, Y. (2005), *The resilient enterprise: overcoming vulnerability for competitive advantage*, MIT Press Books.
- Singh, A. N., Picot, A., Kranz, J., Gupta, M. P. and Ojha, A. (2013), "Information security management (ISM) practices: lessons from select cases from India and Germany", *Global Journal of Flexible Systems Management*, Vol. 14 No. 4, 225-239.
- Singh, H., Garga, R. K. and Sachdevaa, A. (2018), "Supply chain collaboration: A state-of-the-art literature review", *Uncertain Supply Chain Management*, Vol. 1 No. 6, pp.149-180.
- Siponen, M., Mahmood, M. A. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information & Management*, Vol. 51 No. 2, pp. 217-224.
- Soni, U., Jain, V. and Kumar, S. (2014), "Measuring supply chain resilience using a deterministic modeling approach", *Computers & Industrial Engineering*, Vol. 74 No. 1, pp. 11-25.
- Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: A literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

- Spekman, R.E. and Davis, E.W. (2004), "Risky business: expanding the discussion on risk and the extended enterprise", *International Journal of Physical Distribution and Logistics Management*, Vol. 34 No. 5, pp. 414-433.
- Stevenson, M. and Busby, J. (2015), "An exploratory analysis of counterfeiting strategies", *International Journal of Operations & Production Management*, Vol. 35 No. 1, pp. 110-114.
- Strauss, S. (1987), *Qualitative Analysis for Social Scientists*, New York: Cambridge University Press.
- Stuart, I., McCutcheon, D., Handfield, R., McLachlin, R. and Samson, D. (2002), "Effective case research in operations management: a process perspective", *Journal of Operations Management*, Vol. 20 No. 5, pp. 419-433.
- Tang, C. S. (2006), "Perspectives in supply chain risk management", *International Journal of Production Economics*, Vol. 103 No. 2, pp. 451–488.
- 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.
- Tran, T.T.H., Childerhouse, P. and Deakins, E. (2016), "Supply chain information sharing: challenges and risk mitigation strategies", *Journal of Manufacturing Technology Management*, Vol. 27 No. 8, pp. 1102-1126.
- Trombley, S. (2015), "Managing your information risk", *Computer Fraud & Security*, July 2015, pp. 5-9.
- Tukamuhabwa, B., Stevenson, M. and Busby, J. (2017), "Supply chain resilience in a developing country context: a case study on the interconnectedness of threats, strategies and outcomes", *Supply Chain Management: An International Journal*, Vol. 22 No. 6, pp.486-505.
- Vanpoucke, E., Vereecke, A. and Muylle, S. (2017), "Leveraging the impact of supply chain integration through information technology". *International Journal of Operations & Production Management*, Vol. 37 No. 4, pp. 510-530.
- Wagner, S.M., Grosse-Ruyken, P.T. and Erhun, F. (2012), "The link between supply chain fit and financial performance of the firm", *Journal of Operations Management*, Vol. 30 No. 4, pp. 340-353.
- Wang, M., Liu, J., Wang, H., Cheung, W.K. and Xie, X. (2008), "On-demand e-supply chain integration: a multi-agent constraint-based approach", *Expert Systems with Applications*, Vol. 34 No. 6, pp. 2683-2692.
- 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, No. 7/8, pp. 710-716.
- WEF (2014), "Risk and Responsibility in a Hyperconnected World", available at: http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience
- 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.
- Williams, P. (2017), "Why Latin port, shipping and supply chain security is getting more complex - and what it means for training", available at: https://www.linkedin.com/pulse/why-latin-port-shipping-supply-chain-security-getting-rachael-white/?trackingId=Rzjy0I5pF8Dy7YG3Vsm5Rg%3D%3D
- Windelberg, M. (2016), "Objectives for managing cyber supply chain risk", *International Journal of Critical Infrastructure Protection*, Vol. 12, pp. 4-11.
- Yang, C. and Wei, H. (2013), "The effect of supply chain security management on security performance in container shipping operations", *Supply Chain Management: An International Journal*, Vol. 18 No. 1, pp. 74-85.
- Yeo, M.L., Rolland, E., Ulmer, J.R. and Patterson, R.A. (2014), "Risk mitigation decisions for IT security", *ACM Transactions on Management Information Systems (TMIS)*, Vol. 5 No. 1, pp. 5-21.

- Yin, R.K. (2018), *Case Study Research: Design and Methods*. 6th edition. Sage Publications. Thousand Oaks. IL
- Yuan, H., Chen, G., Wu, J. and Xiong, H. (2009), "Towards controlling virus propagation in information systems with point-to-group information sharing", *Decision Support Systems*, Vol. 48 No. 1, pp. 57-68.
- Zuo, Y. and Hu, W.C. (2009), "Trust-based information risk management in a supply chain network", *Information Systems and Supply Chain Management*, Vol. 2 No. 3, pp. 19-34.

Table 1. Sources of cyber and information risks in the supply chain

	Malicious	Natural/Non-intentional	Main Behaviour/Task*
Internal	Current employees	Current employees	Forwarding of infected messages; sharing of account details; replying to phishing messages; retrieving and storing data on uncontrolled devices; being victim of social engineering
	Former employees	Former employees	Forwarding of infected messages; retrieving, storing and disclosing data on uncontrolled devices
		Power outages	NA
		Technical problems	
External	Suppliers/contractors	Suppliers/contractors	Unsecured data sharing and transmission
	Customers	Customers	Unsecured data sharing and transmission
	Competitors		Industrial espionage, misappropriation of data and information
	Foreign nation states		Espionage, misappropriation of data and information
	Domestic intelligence services		Espionage, misappropriation of data and information
	Hackers/Hacktivists		Small and large scale cyber attacks
		Natural disasters	NA
		Power outages	
		Technical problems	

**behaviours/tasks can be malicious or non-intentional depending on the approach of the actor*

Table 2. Profile and background of the case companies

	Company Activities	Profile	Number of Employees (2016)	Annual Turnover (2016)	Geographical Reach (Suppliers)	Geographical Reach (Operations)	Geographical Reach (Customers)
Company A	Manufacturer/supplier of consumer goods	Founded over than 80 years ago, the company operates in a complex and global network of suppliers and customers in the consumer goods industry. This company heavily relies on information and data to be shared in the supply chain regarding products specifications, demand and supply capabilities.	> 250	> £100 M	European	Global	Global
Company B	Logistics Provider (bulk goods)	Founded around 40 years ago, the company is a provider of bulk liquid and powder transport and logistics services. Real-time information on shipments to ensure end to end visibility and transparency to customers and shippers is a key success factor for the company's operations.	> 250	£20-50 M	National	National	National and European
Company C	Logistics Provider (palletized and packaged goods)	Founded around 40 years ago, this third-party logistics provider operates in the Fast Moving Consumer Goods supply chain. The company operates through a network of warehouses and partners in a dynamic market, which requires real time exchange of information to ensure an end to end efficient and seamless logistics service.	> 250	> £100 M	National and European	National	National and European
Company D	International Shipping, Chartering, and Forwarding company	Founded around 30 years ago, the company provides general and specialist logistics services to companies worldwide. They focus also on the maritime segment of international trade, exchanging information and performing transactions with port operators.	> 250	£2-10 M	National and European	National and European	National and European
Company E	Online Retailer	Founded around 20 years ago, the company grew considerably with the rise of e-commerce. They rely heavily on electronic transactions for selling products worldwide through their fulfilment centres in Europe, China and U.S.	> 250	> £100 M	Asia and European	National	National and European

Criterion	Research Phase			
	Design	**Case Selection**	**Data Collection**	**Data Analysis**
Construct Validity	Establishment of a chain of evidence linking the research objectives to the protocol and to the results, questionnaire developed basing on the literature	NA	Involvement of multiple interviewers and multiple sources of information	Informants involved to seek feedback and observations and review the case protocol, demonstration of the convergence of patterns from multiple data sources
Internal Validity	Research built on recognized principles of CSCRM and related literature, acting as foundation to identify critical factors and relationships driving behaviours	Sampling criteria as part of the case study protocol	Multiple informants, multiple sources of information, use of templates with charts and tables	Pattern matching within and across the cases, triangulation of data, reaching agreement among researchers on the outcomes of the analyses
External Validity	Research objectives driving the design of the sampling criteria, multiple sample criteria aligned with the scope of the study to create a coherent sample	Clear description of case companies' background and profile	Comparison of data gathered from companies operating in different supply chains and different stages of the supply chain	NA
Reliability	Case study protocol developed and validated	Clear, structured and explicit sampling criteria	Shared interview protocol for all interviewers, creation of case study database	Formalized coding, involvement of multiple researchers in the analysis

Table 3. Assessment of the empirical validity of the research (based on Yin, 2003; Reuter et al., 2010)

	Company A	**Company B**	**Company C**	**Company D**	**Company E**
Approach to SCRM	Proactive	Reactive	Mixed (proactive + reactive)	Proactive	Mixed (proactive, but mainly reactive)
Level of Centralization of SCRM	Business Unit	Headquarters (support to business units)	Headquarters (support to business units to manage local points of failure)	Local	Headquarters
Tools for SCRM	Risk Assessment and Scenario Analysis	Contingency Plans	Business Continuity Plan, Scenario Analysis and Decision Trees	No specific tool	No specific tools
Ownership of the SCRM Process	Operations and Market Operations	Health and Safety (responsible and accountable), Finance (involved)	Top management (sponsor), Operations and IT (responsible and accountable), Human resources (involved)	Top management (review), operations/logistics (highly involved), Finance (focus on currency issues)	Top management, operations/logistics
Ownership of the CSCRM Process	IT, Operations and Market Operations	IT and Finance	Top management (informed), IT, Finance and Legal (responsible /accountable), Human resources (involved)	Top Management and IT	Supply Chain Director (responsible/accountable), IT, Finance and Purchasing (involved)

Table 4. SCRM and CSCRM at the case Companies

Table 5. Perception of the main cyber and information risks in the supply chain

	Probability of Occurrence (● High / ◑ Medium / ○ Low)					**Impact on Business** (● High / ◑ Medium / ○ Low)				
	Company A	**Company B**	**Company C**	**Company D**	**Company E**	**Company A**	**Company B**	**Company C**	**Company D**	**Company E**
Customer records compromised	○	◑	○	◑	○	●	●	◑	◑	●
Employee records compromised	○	◑	◑	○	○	●	○	●	○	○
Supplier records compromised	○	○	○	◑	○	◑	○	●	◑	○
Data breach/disclosure	◑	○	◑	○	○	●	○	●	○	◑
Theft of Intellectual Property	○	○	●	NA	◑	●	○	●	NA	○
Crash of website	○	○	●	○	○	◑	○	●	○	●
Failure of company's IT network	○	◑	●	●	○	◑	○	●	●	●

Table 6. Main sources of information and cyber risks in the supply chain

	Malicious						**Natural/Non-intentional**					
		A	B	C	D	E		A	B	C	D	E
Internal	Current employees	x	x	x		x	Current employees	x	x	x	x	x
	Former employees	x	x	x	x	x	Former employees		x	x		
							Power outages			x		
							Technical problems			x	x	
		A	B	C	D	E		A	B	C	D	E
External	Current suppliers/contractors	x	x				Current suppliers/contractors	x	x	x		x
	Former suppliers/contractors		x				Former suppliers/contractors	x	x	x		x
	Current customers						Current customers			x		
	Former customers			x			Former customers			x		
	Competitors		x	x		x	Competitors		x	x		
	Foreign nation states				x		Natural disasters					x
	Domestic intelligence services/espionage				x		Power outages					x
	Hackers/Hacktivists			x	x	x	Technical problems					x

Table 7. Security safeguards and initiatives

		Company A	Company B	Company C	Company D	Company E
Organizational initiatives	Information security strategy aligned with the specific needs of the business	X		X		X
	Employ a chief information security officer					X
	Conduct personnel background checks			X	X	
	Specific data and information insurance				X	
Training and internal awareness	Employee security awareness training programme (cyber hygiene)	X		X		X
	Procedures for protecting intellectual property	X				
Compliance and external awareness	Require customers to comply with your privacy and security policies	X	X	X	X	
	Require suppliers/contractors to comply with your privacy and security policies	X		X	X	X
	Conduct supply chain partners security audits	X				
	Collaborative agreements/arrangements with supply chain partners for security	X		X		
Event Management	Business continuity and disaster recovery plans	X	X	X	X	X
	Incident management process	X	X	X	X	X
	Communication procedures with involved supply chain partners	X	X	X	X	X
Data Management	Accurate record of personnel handling data	X		X		X
	Secure data access and control measures	X		X	X	X
	Privileged user access	X	X	X	X	X
	Programme to identity sensitive assets	X		X		
IT security tools	Encryption of email messages	X	X		X	
	Intrusion prevention systems (IPS)	X	X	X	X	X
	Data loss prevention tools			X	X	X
	Mobile security strategy and device management (application awareness)	X	X	X	X	X
	Geo-location and geo-fencing controls (firewall and VPN)	X	X			X
	Data and URL filtering (antivirus and antispam)	X		X	X	X
IT operational resilience	Internal recovery plan process	X	X	X	X	X
	Collaborative recovery plan process with supply chain partners	X		X	X	
	Multiple data backup	X	X	X	X	X
	Geographical distributed datacentres	X			X	X
	Virtual networks / IT infrastructures			X	X	X
	Relying on Cloud systems orchestrators			X	X	X
	Uninterruptible power supplies / power banks	X	X	X	X	X