Supply chain information sharing: challenges and risk mitigation strategies

Thi Thanh Huong Tran
College of Economics, University of Danang, Danang, Vietnam
Paul Childerhouse
School of Engineering, Massey University, Palmerston North, New Zealand, and
Eric Deakins
*Department of Management Systems,
University of Waikato, Hamilton, New Zealand*

Abstract

Purpose – The purpose of this paper is to investigate how managers perceive risks associated with sharing information with trading partners, and how they attempt to mitigate them.

Design/methodology/approach – In this exploratory New Zealand study, qualitative research was conducted involving semi-structured interviews with boundary spanning managers who are responsible for inter-organizational interfaces. Multiple case studies in different industries are used to highlight managers' perceptions of risks in data exchange process throughout the supply network, and their underlying reasoning.

Findings – Managers perceive several types of risks when exchanging information across external supply chain interfaces, and adopt different approaches to handling them. The research also reinforces the vital role played by interpersonal relationships and trust as key enablers of inter-organizational cooperation.

Research limitations/implications – The findings are based on a small sample of 11 case companies based in a single New Zealand province, thereby potentially restricting generalizability. Future work could usefully extend the sample size in order to investigate the correlations between firm sizes, levels of trust, and degrees of data integration within particular industry sectors.

Practical implications – The findings will help managers understand and evaluate different types of risks in the data exchange process, and enable them to make better decisions that enhance information sharing and supply chain performance.

Originality/value – Perceived information sharing risks are peculiar to the individual actors, and as such need to be mitigated through changes to their socially constructed perceptions. This work extends the literature on understanding the various dimensions of inter-organizational information sharing.

Keywords New Zealand, Information sharing, Supply chain risks

Paper type Research paper

1. Introduction

The evolving nature of industry competition, from inter-organizational to inter-supply chain (Christopher, 1992), calls for high levels of cooperation and information between supply chain actors. Advocates of sharing stress the increased profit that will accrue from reduced uncertainty and improved efficiency and effectiveness (Tan *et al.*, 2015; Wang *et al.*, 2014). They also claim that increased supply chain responsiveness to volatile customer demands (Lau *et al.*, 2002; Roh *et al.*, 2014) will enhance customer value and competitive advantage over the long term (Klein and Rai, 2009). The contrary view is that managers will always be sceptical about sharing information with trading partners due to the perceived complexities, risks, and costs (Kembro and Näslund, 2014). Thus, willingness to exchange information becomes a "trade-off between

efficiency and the responsiveness of the information resources", particularly when sophisticated information systems are used (Du *et al.*, 2012, p. 89).

Willingness to share commercially sensitive information with trading partners is crucial if end-customers are to be completely satisfied and the total costs to the supply chain minimized (Ellinger *et al.*, 2012; Yu *et al.*, 2013). However, the risks associated with information sharing across supply chains are still not well-defined and await rigorous investigation (Baker *et al.*, 2007; Du *et al.*, 2012; Wang *et al.*, 2014). Thus, academics and supply chain managers have an interest in gaining a deeper understanding of the critical success factors for sharing information across supply chain interfaces (Kembro and Näslund, 2014).

We posit that the inherent complexities of the supply chain information sharing process call for a holistic theoretical framework that goes beyond the more usual formal assessments of risk. We also contend that when supply chain managers reflect on their information sharing experiences with upstream and downstream trading partners, a social realization of one's position within the supply chain/network results. Hence, an understanding of managers' perceptions of the risks and benefits associated with information sharing is key to gaining deeper insights into the information- sharing process. Thus, the overarching goal of this research is to investigate manager perceptions of the challenges and security risks involved when exchanging information with other supply chain actors, and the nature of risk mitigation strategies.

The exploratory character of this study dictated that a qualitative, multiple case study approach should be adopted. The study involved a total of 11 New Zealand-based companies (predominantly in the manufacturing sector). Together with secondary data sources, semi-structured interviews yielded valuable contextual information regarding the history and characteristics of each case company and its information exchange process. Interviews with supply chain managers also enabled the researchers to gain deeper insights into the relationship aspects of information sharing with external trading partners.

By linking separate concepts of information sharing and supply chain risk management, this paper contributes to the extant literature in several ways. First, it uses a qualitative approach to elicit in-depth understanding of managers' perceptions of the specific challenges and security risks involved when sharing information with supply chain trading partners. It also extends the supply management literature by shining more light on risk mitigation strategies. Finally, the main study findings are synthesized into a theoretical framework that gestures towards further quantitative studies with larger samples and also raises questions for further study. The findings will also enable managers to make better-informed decisions concerning information sharing across their supply chain/network, and will help them develop an appropriate risk mitigation strategy.

This paper is structured as follows. A review of prior studies on information sharing and the risks of data integration is followed by formulation of four specific research questions. Description of the multiple-case research design follows. Findings and implications are presented and the paper concludes with a discussion of knowledge contributions and limitations, plus suggestions for valuable further studies.

2. Supply chain information sharing risks
Supply chain information sharing can be defined as the extent to which critical and proprietary information is communicated to one's trading partners (Kocoglu *et al.*, 2011), and a willingness to make strategic and tactical data available to other members

of the supply chain (as cited in Mentzer *et al.*, 2001). Marquez *et al.* (2004) argue that information sharing include real-time, two-way data exchanges on different aspects of operations management (material flow, order entry, shipping, and billing) as well as forecasts and plans with supply chain partners. By sharing information, each participant receives undistorted, accurate, up-to-date information that is useful for making timely production, inventory, and logistics management decisions (Bargshady *et al.*, 2016). Reduced total system cost results (Chen *et al.*, 2013; Kocoglu *et al.*, 2011).

At the same time, data integration potentially enables supply chain members to offer extra value to consumers and experience an equal distribution of benefits to every supply chain actor (Kwon and Suh, 2005). For example, a well-established benefit of information sharing throughout a supply chain relates to the bullwhip effect (Levary, 2000; Zhang and Chen, 2013). Mason-Jones and Towill (1997) highlight how information is a strategic asset that can enrich upstream supply chain actor decision making. Timely demand information enables reduced reliance on forecasting and buffer stocks, allowing smooth and seamless supply chain operations. Extra emphasis is therefore placed on the downstream members of the chain to share market information in a timely and efficient manner with less knowledgeable upstream members (Chu and Lee, 2006).

Despite the many substantial benefits claimed for information sharing, organizations are often reluctant to divulge true or complete information. They face many challenges and security risks related to the reliability and security of the data being exchanged (Hassini *et al.*, 2008; Vanpoucke *et al.*, 2009), and also fear adverse competitive implications (Barkataki and Zeineddine, 2013).

2.1 Technical aspects of effective supply chain collaboration

Decisions regarding type, and amount and frequency of information sharing with supply chain partners is often complex and the design and implementation of information systems costly (Samaddar *et al.*, 2006). Despite contemporary information communication technology (ICT) being able to offer real-time capture, transmission, and sophisticated analysis of supply chain data (Li and Lin, 2006), poor data quality or a lack of shared information can result in operational problems. These have costly repercussions for every supply chain partner (Madenas *et al.*, 2015). Thus, researchers posit that effective supply chain collaboration requires consideration of technical and social aspects of information sharing in equal measure (e.g. Wu *et al.*, 2014).

Many researchers (e.g. Smith *et al.*, 2007) highlight that ICT-related risks exist in the data exchange process itself, with different impacts on business operations depending on the type of threat. Thus, confidence in the perceived security of supply chain information systems determines the willingness and capability of a firm to share confidential data with trading partners (Zhang and Li, 2006). This results in there being a clear relationship between collaboration level and ICT threat level from internal security issues, employee abuse, and threats from external sources (Baker *et al.*, 2007). Hence, managers should consider the trade-offs between the benefits of sharing information and the ICT threat level when they develop their supply chain information strategy (Zhu, 2002). The risks associated with inter-organizational information sharing can escalate as the volume of exchanged information increases, and as automated systems require reduction/removal of company firewalls (e.g. Anand and Goyal, 2009; Baker *et al.*, 2007; Tan *et al.*, 2015).

Despite well-publicized news events, top managers and system administrators, in particular, can often blind to the types of ICT risk that can cause a dramatic loss of profit, market share, and credibility (Kavoura *et al.*, 2015; Khan and Burnes, 2007).

Such risks include degradation in information quality and leakage of private information both within the focal firm and across the wider supply network (Madenas *et al.*, 2015; Whitman, 2004). If inter-organizational systems are not sufficiently security protected, this can lead to reduced trust by supply chain partners (Zhang and Li, 2006) because the effect of a security breach may be able to propagate into the wider supply chain and impact its competitiveness (Bandyopadhyay *et al.*, 2010). Thus, Kolluru and Meredith (2001) propose that automated ICT-oriented security solutions are essential for assuring confidentiality and privacy of shared information when coupled with authorized and authenticated access to each partner's database.

Arguably, data integration involving different levels of collaboration deserve varying levels of security. Thus, Kolluru and Meredith (2001) propose a three-stage model of information sharing, as indicated in Table I. At Level 1 the focus is on simple communication and coping with threats to integrity, loss of privacy, or repudiation of transactions. Organizations that manage to achieve Levels 2 and 3 states face additional unauthorized access and denial of service risks.

Leakage of proprietary information is often referred to as the dark side of data integration across the supply chain (Anand and Goyal, 2009; Tan *et al.*, 2015; Zhang *et al.*, 2012). Unintentional disclosures of confidential information to unauthorized parties (Zhang *et al.*, 2011) may be deliberate or unintentional (Anand and Goyal, 2009). Moreover, direct disclosure happens when confidential information is shared (Zhang *et al.*, 2012), whereas indirect disclosure occurs when sensitive business data are inferred from non-confidential and shared information because of "the inherent engineering relationships" among different parts of the information (p. 1355). Intentional leakage may happen via organizational inducement (e.g. cash award, technology acquisition, or reputational gains) or personal inducement that is more readily detectable. However, companies can remain ignorant of the effects on daily operations when "proprietary information and knowledge are accidentally or forcibly transferred to any unauthorized parties either through verbal or written communications" (Tan *et al.*, 2015, p. 622).

	Level 1 Asynchronous one-way	Level 2 Asynchronous and synchronous	Level 3 Synchronous communication
Relationship Technologies	Transaction Simple methods: phone, e-mail, fax	Collaboration Complicated methods: advanced planning and scheduling, ERP	Partnership Interconnected IS: EDI, collaborative planning, forecasting and replenishment
Risks	Threats of integrity, spoofing, privacy, lost transactions, lack of trust and commitment, information leakage	Unauthorized access and denial of services, information leakage	More complex regarding unauthorized access and denial of services in highly interconnected networks, information leakage
Risk mitigation	Identification and authentication, data confidentiality, data integrity	Access control, authorization, auditing	Trust management, delegation of credentials across multiple tiers and across supply chain interactions

Source: Adapted from Kolluru and Meredith (2001)

Table I.
Information
sharing levels and
types of risks

Assurance of three primary security goals: confidentiality, data integrity, and availability (Stoneburner *et al.*, 2002) are essential for guaranteeing accuracy and fairness of data exchange processes within the supply chain. Confidentiality refers to accidental or intentional disclosure of information, whereas data integrity requires that information be secured against unauthorized modification. The objective of availability is assurance of accessible and uninterrupted information at every node within the supply chain since the implications of interruptions due to degraded ICT system availability can be a dramatic reduction in market responsiveness for the focal firm and wider supply chain. Tan *et al.* (2015) offer empirical evidence of the positive relationship between the level of data integration and the frequency of information and knowledge leakage in a supply chain. Companies face greater exposure to information and knowledge leakage when they achieve a higher arc of data integration.

2.2 Social aspects of effective supply chain collaboration

Barkataki and Zeineddine (2013) highlight the close link between trust level and type of technology-enabled cooperation in a supply chain. Successful data integration requires parties to strongly commit to creating and maintaining a consistent enduring relationship that is based on mutual trust (Kocoglu *et al.*, 2011; Kwon and Suh, 2005; Wang *et al.*, 2014). An absence of trust and commitment hinders information sharing and may lead to considerable increases in transaction costs, ineffective communication, low productivity, and a higher perceived risk of opportunistic abuse in the supply network (Sridharan and Simatupang, 2013).

Supply chain trust can be defined as, "an expectancy of positive (or negative) outcomes that one can receive based on expected actions of another party in interactions characterized by uncertainty" (Sahay, 2003, p. 556). Trust and long-term partnerships positively influence the enhancement of seamless information flows within the focal organization and among supply chain actors (e.g. Cheng, 2010; Kolluru and Meredith, 2001; Kwon and Suh, 2005).

However, even when an organization has sufficient capability to share information, managers are often unwilling to release sensitive information to partners when there is a lack of trust (Fawcett *et al.*, 2007).

Most researchers appear to favour the concept of supply chain collaboration and favour inter-organizational information exchanges (e.g. Balsmeier and Voisin, 1996; Damiani *et al.*, 2011; Daugherty *et al.*, 2005; Ferdows *et al.*, 2004; Fine, 2000; Kembro and Näslund, 2014; Zhonghua and Ling, 2013). However, there are many downsides; for example, requiring supply chain partners to reduce security walls around their ICT assets, and make business processes more accessible, can create issues and adverse consequences for performance. Hence, researchers and practitioners are interested in understanding the risks associated with supply chain collaboration and the process of data exchange.

It is currently not well understood how managers perceive and evaluate risk in the context of supply chain information sharing. Similarly, few scholarly articles explore how organizations deal with specific risks related to the use of ICT applications during the data exchange process. Recent studies tend to examine the aspects of supply chain risk management and information sharing separately. For this study, we consider how supply chain managers perceive the importance and role of trust when sharing information with other supply chain members. Manager perceptions of associated threats and the strategies used to mitigate them are also considered. For example, Table II indicates how Whitman (2004) classified ICT risks into 12 major groups, based on their likely consequences, a feature that helps managers set appropriate levels of

Name of categories	Examples
1. Act of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial of service
8. The forces of nature	Fire, flood, earthquake, lightning
9. Quality of service deviations from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11.Technical software failures or errors	Bugs, code problems, unknown loopholes
12.Technological obsolescence	Antiquated or outdated technologies

Source: Adapted from Whitman (2004)

Table II.
ICT-related risks

security investment. According to Tan *et al.* (2015), although deliberate attacks (virus, worms, and hackers) are the top ICT hazards, intentional acts of information extortion are the most frequent.

2.3 Research questions
New Zealand is a particularly interesting setting for this study due to its geographic location that gives rise to long lead times and extended supply chains for many companies. New Zealand has traditionally experienced slow rates of ICT adoption for information sharing purposes (Basnet *et al.*, 1999) and high levels of contact between supply chain members (Soon and Gutiérrez, 2010). However, globalization pressures and a more volatile economic landscape increasingly require New Zealand firms to compete by collaborating with other supply chain members. The specific research questions are:

RQ1. What information is shared across supply chain interfaces?

RQ2. How does a company share supply information with trading partners?

RQ3. What are the challenges and security risks of sharing supply information?

RQ4. How are the risks mitigated?

3. Research methodology
This study investigates manager perceptions concerning identification and management of the risks associated with sharing inter-organizational supply-related information. The study of supply chain management and information management topics tends to involve complex phenomena and contextually rich settings, as evidenced by the current state of knowledge of each discipline being characterized as "at an early formative development stage and subject to rapid change" (Zsidisin, 2003). Because information systems can be understood differently by individuals, and given meaning by the shared understanding of such phenomena via social interaction (Doolin, 1994), a case research strategy is ideal for eliciting the deep knowledge and experience of practitioners in these emergent fields (Walsham, 1995). Moreover, since our research objectives focus on explanations, case studies based on a variety of data sources provide rich empirical descriptions of particular examples of the phenomenon in the real-world context (Yin, 1994). As a result, theories built from

multiple cases are robust, generalizable, and testable, compared with single-case research (Eisenhardt, 1991). A qualitative research approach is particularly suitable for this study. In addition to its exploratory and explanatory objectives, the central notion of the qualitative approach is the use of multiple cases as the basis to create a theory in an inductive manner, by recognizing the relationships among theoretical constructs and propositions within and across cases (Eisenhardt and Graebner, 2007).

3.1 Research sample
Purposive sampling of firms allows researchers to select organizations that have relevant characteristics for the research questions (Bryman and Bell, 2011). For this study, a key objective was to access a sample of case companies from different settings, to capture a range of sharing experiences and thereby increase the validity and reliability of findings. Hence, the main criteria for selection were:

(1) a propensity to exchange information with supply chain trading partners; and

(2) a commitment to ongoing development of inter-organizational ICT systems.

Initially, 110 New Zealand companies were selected from a business directory and invited to participate. The final empirical data set of 11 New Zealand-based companies comprised eight manufacturers, two distributors, and one export organization (Table AI provides a case company overview). The sample varied by industry type and size, product complexity, position in the supply chain, and level of ICT adoption. Each case company serves as a single analytic unit. The research focussed on the data exchanges that occur between a case company and its principal suppliers, customers, and logistics service providers. Information exchanges unrelated to organizational value-adding activities, such as orders placed with stationery suppliers, were excluded from the findings.

3.2 Data collection
This study employed multiple data collection methods, including qualitative interviews triangulated with secondary sources. The researchers conducted semi-structured interviews with the principal corporate actors, whom all have extensive knowledge of supply chain-related operations, Table III.

Each interview comprised three separate stages of questioning, concerned with: the local business context, information processes, and ICT systems; description of the perceived challenges and security risks associated with information sharing; and

Case (Company)	Defined name of interviewees	Function of respondent	Interview duration (min)
Manufacturer 1	Interviewee A	Purchasing manager	40
Manufacturer 2	Interviewee B	International sales manager	35
Manufacturer 3	Interviewee C	Managing director	45
Manufacturer 4	Interviewee D	Managing director	40
Manufacturer 5	Interviewee E	Supply chain manager	75
Manufacturer 6	Interviewee F	Managing director	35
Manufacturer 7	Interviewee G	Managing director	35
Manufacturer 8	Interviewee H	Managing director	45
Distributor 1	Interviewee I	Sales manager	50
Distributor 2	Interviewee J	Managing director	50
Export	Interviewee K	Sales manager	35

Table III.
Interviewee details

description of risk mitigation strategies. The duration of each interview varied between 35 and 75 minutes. Use of semi-structured interview questions and follow-up questions encouraged a flexible interview procedure (refer to the interview protocol in Figure A1). Hence, the researchers were able to opportunistically capture information relevant to the central constructs (Bryman and Bell, 2011). During the interviews, the researchers were often able to identify supporting secondary sources for each case company, including standard operating procedures, annual reports, mission statements, and financial records.

3.3 Data analysis procedure

Analysis of the qualitative data utilized an explanation building process proposed by Yin (2009), which develops findings through a series of iterations. Hence, the statements of belief espoused by the case managers were organized, categorized, reviewed and re-coded to identify and explain themes. Before synthesizing the data, every company and interviewee (respondent) were assigned a generic name and number to help preserve anonymity. Then, within-case analysis to fully understand the specific challenges, security risks, and mitigation strategies at each dyad was followed by cross-case analysis to identify similar/contrasting themes and patterns. Also included were the associated knowledge sharing and relationship-building activities. In short, the theory-building process involved recursive cycling among empirical case evidence to identify emerging themes and theory (Eisenhardt and Graebner, 2007). The final step involved comparing the findings with the extant literature.

4. Findings

4.1 The importance of information sharing to business operations (cross-case analysis)

Every respondent acknowledges that data exchanges play a critical role in their business dealings and agrees that data integration enables the organization to know what is occurring at each node of the supply chain. In particular communication between trading partners provides a rich picture of the markets and customer needs, which less-informed (upstream) members of the supply chain need to have. Exchanging relevant data downstream and upstream along the supply chain also enables partners to make informed decisions from information that is relatively undistorted, accurate, and timely. According to a supply chain manager at a large manufacturing organization:

> I actually think sharing information is critical. The more we know about customers, the more we know what they expect of us, and the more we can adapt, change, and be prepared to satisfy their needs. And the more we share with our suppliers, the more they are adaptable and can understand what we need to satisfy our requirements as well. It is a partnership […] we can support each other like a family (Interviewee E).

According to the sales manager of a small distributor, data integration has enabled the firm to understand what customers expect and, with the information shared by suppliers, can satisfy customer needs effectively. This has resulted in several benefits:

> Because it is word-of-mouth as well, many of our customers choose to stay with us because we supply them over the year and trust has been built up so much. Its been really successful because of information sharing (Interviewee I).

Sharing that is underpinned by a strong personal relationship helps companies to correct mistakes more quickly and easily and with the understanding of customers since every member tends to understand everyone else's and so can sometimes recognize problems even before they arise.

Information sharing that is the result of a long-term personal relationship is considered to be one of the main competitive advantages. As a managing director of a medium-sized manufacturing organization articulated:

> Information sharing via a personal relationship is absolutely the most important thing, more important than price or even quality. It is not the normal thing people think about. When we make mistakes or send the wrong goods they know who we are, they phone, and say that your service is not good. I say ok, we will fix it. This is much better than them just sending an email to a department if they don't know who to talk to (Interviewee H).

Supply chain companies can also cooperate to find the minimum total cost solution that has maximum benefits for the chain. According to the international sales manager for a large manufacturing organization:

> I think its great to have supply chain partners who are willing to share information and have collaboration. We like to have strong relationships on the sales side so they can tell us exactly what they want. Equally for the supply chain, we want suppliers to tell us what are good and bad margin products and how we can do better, what improvements we can make, and any new materials that are available. Definitely, it should be good for both sides (Interviewee B).

Data exchanges across the supply chain are also vital for companies that have perishable products. As the sales director for an export company stated:

> Because our products are fresh and prices fluctuate so much, sharing information is very important (Interviewee K).

To summarize, the cross-case analysis emphasizes the importance and value of information sharing to every case company irrespective of industry, firm size, or position in the supply chain. In particular, data exchange with trading partners results in a variety of benefits for other supply chain members.

4.2 Supply chain data integration

Table IV positions the majority of the case companies within the first two stages of Kolluru and Meredith's (2001) data integration framework: asynchronous communication (Level 1), or asynchronous and synchronous communication (Level 2). Most of the small and medium-sized enterprises (SMEs) in the sample are at Level 1 since, in addition to face-to-face meetings they rely on well-established and relatively straightforward asynchronous methods like phone, fax, and e-mail to share information with supply chain trading partners.

The SME participants expressed a preference for simpler methods of communication, which are generally judged to be cost-effective, reliable, and convenient for constant keeping in touch with trading partners. As the managing director of a medium-sized manufacturing organization expressed it:

> In a lot of situations I don't think it is better to share information electronically. I couldn't see any more benefits so we'd rather keep what we are doing. We don't have a lot of information to exchange. If more information was being shared, it would be different maybe (Interviewee F).

Simpler methods were also felt to be more personal than machine-based systems, as was expressed by the managing director of a small distributor:

> I like the ideas of phone, fax, and email and the main reason I like them is because they are more personal [...] A more electronic and automatic type of communication may give you good information but it's not personal, and for some suppliers the electronic system is not friendly. Because we are small enough, we choose to use personal contact as much as we can (Interviewee J).

Case company	Size	Information sharing method	Type of shared information	Frequency of information sharing	Explanation
Manufacturer 1	Large	Using mainly e-mail and fax, and occasionally phone Level 1: asynchronous communication	Requirements for materials, product-related information, technical documents, price trends, forecasting, ideas for new product development	Weekly	The system is reported to be sound because there are hardcopies in case of a dispute. It is also convenient and especially suitable for interacting with smaller trading partners
Manufacturer 2	Large	Using EDI system to share information electronically with major suppliers Level 2: asynchronous and synchronous communication	Requirements for materials, product-related information, production schedules, pricing, technical documents, OIP information, and forecasting	Based on each project	There is a large volume of information to share with partners. This automatic system helps to process data efficiently and accurately
Manufacturer 3	Large	Using physical meetings and e-mail, although using a web-based purchasing programme with key suppliers Level 2: asynchronous and synchronous communication	Feedbacks on products and prices, forecasting, requirement. Close new product development	Three or four times a month	This system provides for "great conversations and discussion". Ordering and confirming can be done automatically and uses detailed information. Having a private website for ordering was judged to be "a great solution"
Manufacturer 4	Large	Using MRP and GS1 to share information electronically Level 3: synchronous communication	Product-related information, sales history, forecasting	Real-time data	The systems are claimed to be efficient and seldom make mistakes. A huge ICT investment was made
Manufacturer 5	Large	Using Skyline system to share internal information electronically but not capable with other partners Level 2: asynchronous and synchronous communication	Product-related information, technical documents, financial and strategic information (cost structure, common goals, and process evaluation), and marketing-related information	Real-time data for ordering Monthly meetings for strategic information and supply development	Because this firm is part of a global cooperation it needs electronic systems to link partners

(*continued*)

Table IV.
Case by case
summary of supply
chain information
sharing

Case company	Size	Information sharing method	Type of shared information	Frequency of information sharing	Explanation
Manufacturer 6	Medium	Using phone, fax, e-mail and physical meeting Level 1: asynchronous communication	Place and receive orders, some forecasting	Weekly	There are no perceived benefits to using an ICT application because of the small volume of shared information The company believes it is more appropriate to observe trends within the industry because the firm operates in a non-ICT focused sector
Manufacturer 7	Small	Using phone, fax, and e-mail Level 1: asynchronous communication	Place and receive orders, some forecasting	Monthly	Because this is a small company that is dealing with smaller partners, it does not see the need or importance of using ICT
Manufacturer 8	Medium	Using mainly phone and e-mail Level 1: Asynchronous communication	Requirements for materials, forecasting, close new product development	Weekly	There are only a small number of customers. Simple methods are judged to be more personal. However, the database is poorly structured
Distributor 1	Small	Using physical meetings, phone, and e-mail Level 1: asynchronous communication			Simpler methods help the company to maintain constant touch with trading partners. As a family business this style of communication is judged most suitable
Distributor 2	Small	Using confidential website and phone calls Level 2: asynchronous and synchronous communication			Simpler methods are considered to be useful for staff when contacting the small number of suppliers. The company believes it is better to observe what happens within their industry
Exporter	Medium	Using mainly e-mails and phone Level 1: asynchronous communication			They do not have much information to share. Simple methods are useful to make sure that the right person is getting information It is hard to convince other partners about the benefits of a new ICT system

Most of the larger firms in the sample are at Level 2 or Level 3 of Kolluru and Meredith's (2001) data integration framework, having invested in advanced information systems that automate much of the data exchange process. Such systems include material requirements planning, GS1, web-based purchasing applications, and video conferencing. However, these tend to be reserved for working with larger and "more important" partners, and with phone, fax, and e-mail communication for the remainder. As the managing director of a large manufacturing organization elaborated:

> With our key suppliers we log into their private portal and place our orders in their system. Half of such orders are submitted electronically or maybe even 60%. With the other suppliers we simply email them (Interviewee C).

The respondents further explained how advanced information systems systematically store large quantities of complex information, which enables employees to access and share business data quickly and accurately. Employees also have access to dialogue histories so that they have sufficient information to make informed decisions promptly.

Several respondents stressed that information technology is used for manufacturing rather than administrative purposes. For example, the managing director of a large manufacturing organization stated:

> All of our production machinery is managed by computers. That is great technology. But many [manufacturing] companies mostly just apply production technologies production and there isn't much happening in the administration area (Interviewee G).

In summary, some significant differences exist in attitude towards information sharing across external supply chain interfaces. Whereas the larger case companies consider that ICT is providing them with competitive advantages via increased collaboration opportunities, many SMEs feel that the transactional nature of their operations is a compelling reason to continue to use simpler information handling processes.

4.3 Influence of context on information being shared

Table IV also reveals the range of information that is being shared with trading partners. While industry sector and product type influence the type of information being exchanged, the findings emphasize that degree of intimacy of the relationship plays a central role. As the sales manager of a mid-sized export company put it:

> Depending on customers and how open the relationship is, some customers we get on well with, and have a very open and honest relationship with them. They will be happy to give us pricing information […] what is happening in their markets, etc. Other customers are less open to sharing information because they want to keep that for their competitive edge and push down prices (Interviewee K).

Operational data such as product-related pricing information, stock levels, delivery schedules, technical documents, specifications for production, promotions, feedback for products, and after-sales support are the most common types of data being exchanged by the case companies. Many also share short-term demand forecasts with suppliers.

Those firms that maintain closer trading relationships also share strategic data, although this is often limited in scope to marketing-related exchanges. For example,

Manufacturer 5, Distributor 1, and Distributor 2 all receive information from key suppliers related to actual customer demand, marketing strategies, and competitor products. Two (manufacturing) organizations share sensitive research information with suppliers in to jointly develop new products jointly. The export company has managed to increase its negotiating power by acting as a bridge that transmits market updates from customers to suppliers. Only case company Manufacturer 5 shares strategic and finance-related information, which includes cost structures, performance evaluations, and strategic goals. However, arguably this initiative depends on there being a very trusting strategic partnership in place between supply chain members.

4.4 Issues related to information sharing across the supply chain
Table V summarizes the interview data describing the main issues, security threats and mitigation strategies related to supply chain information sharing. Respondents described how, when the company is located far away from its suppliers and end-customers, these challenges are intensified.

Although a wide variety of challenging issues is indicated, they can often be explained by the absence of a meaningful trading relationship between case company and trading partner. Hence, it is unsurprising that so many of the reported stumbling blocks to successful supply chain information sharing can be linked to a basic lack of trust between trading partners. As the sales manager of a mid-sized export company put it:

> Trust is absolutely important. If you don't trust your suppliers you can't share information openly. At the same time, if a supplier doesn't trust me they can't believe what I tell them. If you don't have trust it makes business extremely difficult (Interviewee K).

It is also evident that lack of trading partner commitment can lead to inconsistent supplies and fluctuations in customer demand. As the managing director of a large manufacturing company explained, when referring to the supply side:

> The major challenge we have is how we can make sure we have a good and consistent supply line. We are a long way from our suppliers, and when things go wrong, we can go out of business. So ensuring consistency is really important (Interviewee C).

The sales manager of a small distributor highlighted similar uncertainty on the customer side:

> [Customer] head office, the biggest challenge would be that. The people at head office level change their supplier preferences without notifying their current suppliers. So one day it could be us and next day they change to another supplier/our competition without telling us about it (Interviewee I).

Ensuring integrity of exchanged information is also vital, since only with true, fair and timely data can decisions be effective and timely. As the managing director of a small distributor reported:

> Some of our suppliers do not always provide us with timely information. For example, we sent them an order and they had updated their price list the night before. So we asked, why didn't you tell us? Timeliness is a really big problem (Interviewee J).

Several respondents mentioned intellectual property infringement as a large risk. For example, an international sales manager for a large manufacturer highlighted:

> There is always a risk that our suppliers can go directly to our customers. So there could be a risk that we will be cut out of the supply chain […] We also do a lot of work with XXX Inc., which is an overseas supplier, so we obviously have a risk of being copied (Interviewee B).

Case Company	Issues related to information sharing (Example)	Security threats	Mitigation strategies
Manufacturer 1	Lack of a meaningful trading relationship (Needing to have good relationships with suppliers to obtain best prices)	No possibility of an external security breach (internal systems only, with high levels of internal control)	Endeavouring to build good personal relationships with partners via constant interactions
Manufacturer 2	Lack of a meaningful trading relationship (Suppliers trading directly with customers) Lack of respect for others' possessions (Risk of copyright infringements) Lack of a meaningful trading relationship (Risk of poor quality from overseas suppliers) Local context consideration (Isolated location and different time zones)	No threat from external entities Information leakage due to a supplier being uncommitted to maintaining agreed arrangements Information leakage by ex-employees Pricing information disclosed by mistake	Proactive forecasting and being well prepared for production Using different suppliers to those of the competition Using many suppliers simultaneously Keeping pricing information confidential
Manufacturer 3	Lack of a meaningful trading relationship (The challenge of ensuring quality and consistent supply) Local context consideration (Isolated location and different time zones)	Many security threats, although with no serious consequences	Being honest and open with key partners Only sharing information with trusted partners Building good relationships with key suppliers
Manufacturer 4	No perceived challenges	No security issues reported	–
Manufacturer 5	Local context consideration (Isolated location and different time zones)	No security issues reported	Employing confidentiality agreements and legal contracts Improving forecasting to minimize risks Acquiring additional supply sources
Manufacturer 6	Lack of a meaningful trading relationship (Suppliers do not always tell the truth about stock levels)	No external security issues reported Information integrity issue	Data only shared among staff with secure services Customer information not being shared Employing legal contracts

(*continued*)

Case Company	Issues related to information sharing (Example)	Security threats	Mitigation strategies
Manufacturer 7	Lack of a meaningful trading relationship (A customer not paying for goods received)	No possibility of an external security breach (internal systems only, with high levels of internal control) A bad experience with purposive information leakage	Employing legal contracts
Manufacturer 8	Lack of a meaningful trading relationship (Suppliers do not always tell the truth about stock levels)	No external security issues reported Information integrity issues (ad hoc data storage) Information leakage due to personal conversations with close friends	Building "smarter" systems that share information Not sharing information with untrusted partners Staff awareness training
Distributor 1	Lack of a meaningful trading relationship (Inability to prevent key customers from switching preferred supplier without notice)	No possibility of an external security breach (internal systems only, with high levels of internal control) Purposive disclosure of pricing information	Keeping in close touch with key partners Building close personal relationships and trust via face-to-face communication Flexible pricing strategy
Distributor 2	Lack of a meaningful trading relationship (Difficult to convince customers of the benefits and technical side of products)	No security issues reported (sensitive customer information is not stored) Information integrity issue evidenced by untimely information	Does not share information about customers Does not share information with untrusted partners
Exporter	Lack of a meaningful trading relationship (Risk of giving too much information away and losing competitive advantage)	No external security issues reported Some information disclosure events both unintentional and intentional Information integrity issues	Building good relationships with partners Building good relationships with partners

Table V.

Thus, respondents feel that they need to be careful when deciding on whom to work in close collaboration with, and the type/quantity of data to exchange with partners, especially when sensitive information is involved. As the sales manager of a mid-sized export company put it:

> Market information is very important, and it is your advantage over someone else. If you give too much information away, you ruin your advantage in the market or ruin somehow your ability to buy effectively. So you have to be careful about how much and what information you share and when (Interviewee K).

The case companies are also coping with local contextual issues within the supply chain. New Zealand is geographically isolated and has a small-scale economy. Also, the majority of NZ companies are SMEs and have only a small influence on the wider supply chain. Consequently, some are experiencing significant uncertainty around supply sources, which cause frequent production delays. However, as the supply chain manager of a large manufacturing organization also points out:

> I think that because New Zealand is remote, SMEs have not been exposed to global shipping because of isolation; they seem to be very slow to want to change (Interviewee E).

4.5 Security threats related to information sharing across the supply chain
Table V also highlights the main security threats reported by case respondents, which are directly linked to supply chain information sharing. The case organizations that do not use ICT to share information with external parties expressed confidence in having tight security, which includes information only being accessible to authorized personnel. For example, the managing director of a large manufacturing organization stated:

> Everything is protected. No person or another company can do anything to attack this company. It is impossible. Nobody can touch it (Interviewee D).

Such companies simply refuse to exchange confidential data at all or share small amounts of carefully selected information with those they do not trust. As stated by the supply chain manager of a large manufacturing organization:

> I don't think we have any security issues. Only senior managers and ICT people have full access to everything. That's how we control internal security and fortunately our system is not linked to our suppliers, so we don't have any reason for a confidential breach (Interviewee E).

Many of the organizations that did share information report a range of problems involving information leakage. Some had experienced serious (unintentional and intentional) issues when sharing information with their trading partners. As the sales manager for a small distributor reported:

> Somebody gives our information to other firms all the time. Ethically, it is wrong. A lot of people reveal our prices to competitors (Interviewee I).

The managing director of a mid-sized manufacturing organization describes how this type of situation could arise via social engineering, which is hard to control:

> This is quite a small town so you might work here and your sister might work for the competition, which is just down the road. And you might say to your sister, "we have a big order coming up". Before you know it, your sister might find information on that big order (Interviewee H).

Although data disclosure can happen when suppliers or customers deliberately share the company's information with competitors, sensitive information may also be disclosed due to human error, such as sending the document to the wrong place. However, some respondents reported no instances of direct or indirect information leakage. For example, the supply chain manager of a large manufacturing organization stated:

> Nothing I am aware of at this point of time. Our company and its suppliers sign a confidentiality agreement, and we do have other legal contracts as well. According to the confidentiality agreement, if anyone breaks that contract, they would be taken to court, so I believe that nobody would take the risk (Interviewee E).

Interestingly, although the case data provides evidence of various information security issues, examples of serious consequences were not volunteered.

4.6 Risk mitigation strategies

Several approaches to risk reduction are reported by the case companies, Table V. The most commonly employed strategy is to maintain a strong relationship, particularly with collaborating organizations. As the purchasing manager for a large manufacturing organization explains:

> The most important thing is to have good relationships with trading partners, and especially personal relationships. A good relationship is when they come and visit us frequently many times a year (Interviewee A).

Social dimensions of personal relationship, openness and honesty are also effective when problem-solving; with face-to-face communication judged especially important. The managing director of a large manufacturing organization stated:

> When we have challenges we talk to our partners; we just sit down and are honest. We tell them our problems and they tell us theirs […] We argue the points honestly, tell them what we want. Be consistent and always honest. Honesty is very important (Interviewee C).

In reality, the case companies rely a great deal on mutual trust and credibility that has been built up over an extended period. Moreover, while several of the case companies do use confidentiality agreements before sharing sensitive data, it was further explained that:

> No trust, no jobs. The formal agreement just verifies and writes down what we agree. Trust is built between two people, who are being honest in sharing information (Interviewee C).

The managing director of a large manufacturing organization also explained how:

> It is just a part of doing business. Sometimes people simply don't pay. If you do business, you have to accept it happens sometimes, and we just have to move on. I don't think we can do anything more than what we are doing to safeguard it from happening. I think it is good to have a face-to-face agreement and shake hands […] I [also] do use a formal agreement, and we put trust into words in the agreement (Interviewee G).

Only one respondent argued strongly for formal agreements to be the primary mechanism for preventing information leakage, possibly because that manager had experienced a significant problem in the past. Also, firms that produce technical products thought that it was better for them to use some suppliers in tandem, or to use a different supplier from that of their competitors, to reduce the risk of intellectual property violations and information leakage. Some companies try to avoid the issues altogether by

simply refusing to share information with trading partners whom they do not trust. This was affirmed by the managing director of a mid-sized distribution company:

> For the suppliers who are not open with us we only answer in general terms questions related to our sales, and don't tell them who our customers are (Interviewee J).

Several of the case companies stated their intention to update their information systems with more sophisticated applications, and to train staff and standardize data transmission. However, a common feeling was highlighted by the supply chain manager of a large manufacturing organization:

> To be honest, there is nothing else that we could do. These concerns are not only facing us; it is a challenge for all New Zealand companies. It is a concern for the whole country (Interviewee E).

5. Discussion

Earlier studies emphasize that the main benefit of information exchanges across external supply chain interfaces is the knowledge of end-customer demand to every supply chain member (Kavoura *et al.*, 2015; Mentzer *et al.*, 2001; Zhonghua and Ling, 2013). This results in timely and informed decision making throughout the supply chain (Madenas *et al.*, 2015). The findings of this research strongly support these propositions and extend the literature by demonstrating a broad range of additional benefits.

In line with findings by Zhang and Li (2006), our results indicate that proprietary information is continuing to find its way into unauthorized hands, either intentionally or unintentionally. However, it is clear that New Zealand managers have a good understanding of the many security threats involved when sharing information with trading partners. They also stress how the challenges intensify when the enterprise is remote from its suppliers and end-customers, and can appreciate that many of the challenges occur when their company has no meaningful relationship with a trading partner. Hence, this research extends the literature by providing insights into manager perceptions of sharing information across the external supply chain interface.

Figure 1 highlights how loss of proprietary information is perceived to be the primary concern. It also indicates six threats which collectively are perceived to increase the risk of proprietary information loss: Lax IT security; poor data integrity; theft of intellectual property; threats posed by the local context; information leakage; and, lack of partner commitment. Moreover, because building and maintaining a
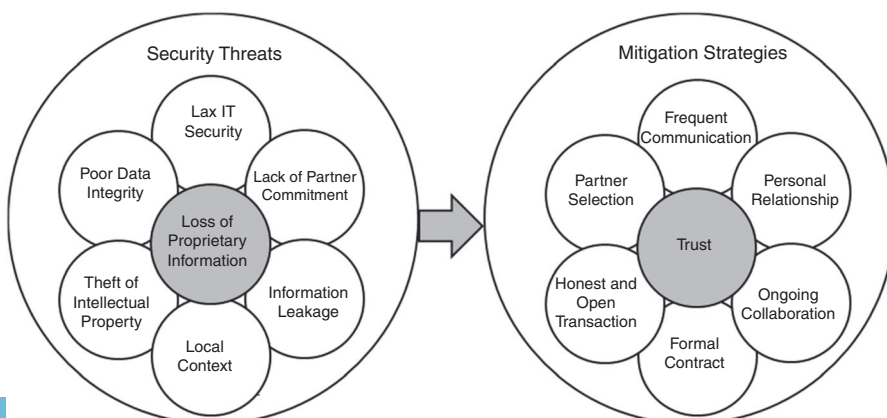

Figure 1.
Perceived security threats and mitigation strategies for supply chain information sharing

trust-based partnership is reported to be the central goal of the mitigating strategies, the figure also indicates six activities which are perceived to be effective for reducing the risks: frequent communication; partner selection; honest and open transaction; formal contract; ongoing collaboration; and, personal relationship.

Thus, the study extends the literature by showing how trust between trading partners can be encouraged, via personal relationships and long-term collaborations that involve working together honestly and openly; rather than simply relying on legally binding contracts. It also confirms the important part played by trust in creating a virtuous cycle of engagement, since trust between the trading partners increases partner commitment to engage in information sharing, which in turn reinforces the feelings of trust, and so on (e.g. Kolluru and Meredith, 2001; Kwon and Suh, 2004). Of course, if trust is unrefreshed the cycle can shift into a reverse pattern of negative consequences.

Prior studies also indicate that the effectiveness of risk mitigation strategies depends both on manager awareness and the level of preparation (e.g. Chen *et al.*, 2013; Jüttner *et al.*, 2003; Khan and Burnes, 2007). Our research findings affirm these studies by highlighting the critical role played by key personnel in applying methods that reduce the effects of risk. Interestingly New Zealand managers appear to rate their company security very highly, which is in contrast with studies in the USA (Baker *et al.*, 2007; Whitman, 2004) and more recently in Australia, indicating low levels of confidence in information system security.

Finally, despite claims that technical aspects of information sharing are of equal importance to social aspects (Kocoglu *et al.*, 2011; Wu *et al.*, 2014), this study clearly shows that managers believe that frequent, personal communication is far more effective for encouraging trust between trading partners than any computer system yet invented.

6. Conclusions and implications

This study highlights that, since the turn of the century, managers have come a long way in appreciating the benefits and risks associated with sharing information across external supply chain interfaces (e.g. Basnet *et al.*, 1999). As the trend towards inter-supply chain competition intensifies, and companies strive to deliver the best value to customers at lowest cost, information exchanges with trading partners are set to become a strategic necessity for many firms (Mentzer *et al.*, 2001; Wu *et al.*, 2014).

The literature tends to neglect manager perceptions of the risks and challenges associated with exchanges of information between trading partners in a supply network. Most of this research also adopts a positivist approach and examine risk management and information sharing separately. In contrast, this study focusses on the social aspects and thereby demonstrates that the majority of the information sharing issues which arise are due to a basic lack of trust between trading partners. It also shows how the case company managers attempt to maintain close and personal collaborative relationships with key trading partners that are judged to be intrinsically trustworthy.

This study also offers a range of strategic initiatives for effectively addressing the challenges. Hence, practitioners can now make decisions regarding risk mitigation strategies that address the lack of trust between trading partners.

The finding that many of the case companies have only limited negotiating power and high levels of uncertainty agrees with earlier findings concerning New Zealand's manufacturing sector (Basnet *et al.*, 2006). Hence, it is interesting that SME managers, in particular, continue in their belief that the tangible and intangible costs associated with automated electronic systems far outweigh the benefits of greater supply chain certainty. Clearly, incompatibility between information systems employed by many

SMEs and the more sophisticated ones used in larger companies will make it very challenging to implement real-time data transactions throughout the entire supply chain. Arguably, it may be necessary for the larger, less financially constrained supply chain members to take the lead (Johnson, 2008).

Regarding study limitations, the exploratory nature of this research required that attention be focussed on acquiring rich descriptive case information. Hence, the sample is not entirely representative of all the stages and business operations conducted within a supply chain. Also, because the findings are based on data collected from 11 New Zealand case companies that have a relatively limited range of products and software applications, the conclusions cannot be claimed to be generic or applicable to other countries, or even to every company in New Zealand. Thus, there are many avenues for further research.

Application of a large-scale survey to verify the exploratory insights of this research and triangulate its findings is recommended. Future research could also usefully investigate if a correlation exists between the level of achieved data integration and firm size, industry sector, type of partnership, and so on. Also, because it was reported that companies far removed from the marketplace experience additional communication problems, it would be valuable to examine how the trust-building process changes as one travels through the supply chain echelons. For example, is it possible to maintain trust between trading partners when regular face-to-face meetings are no longer possible, or as exchanges become more automated? Does such a thing as an ideal personal relationship decoupling point exist, and if so, under what circumstances […]?

References

Anand, K.S. and Goyal, M. (2009), "Strategic information management under leakage in a supply chain", *Management Science*, Vol. 55 No. 3, pp. 438-452.

Baker, W.H., Smith, G.E. and Watson, K.J. (2007), "Information security risk in the e-supply chain", in Zhang, Q. (Ed.), *E-Supply Chain Technologies and Management*, Idea Group Publishing, London, pp. 142-161.

Balsmeier, P. and Voisin, W.J. (1996), "Supply chain management: a time-based strategy", *Industrial Management*, Vol. 38 No. 5, pp. 24-27.

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

Bargshady, G., Zahraee, S.M., Ahmadi, M. and Parto, A. (2016), "The effect of information technology on the agility of the supply chain in the Iranian power plant industry", *Journal of Manufacturing Technology Management*, Vol. 27 No. 3, pp. 427-442.

Barkataki, S. and Zeineddine, H. (2013), "On achieving secure collaboration in supply chains", *Information Systems Frontiers*, Vol. 17 No. 3, pp. 691-705.

Basnet, C., Childerhouse, P., Foulds, L.R. and Martin, V. (2006), "Sustaining supply chain management in New Zealand", *International Journal of Logistics Systems and Management*, Vol. 2 No. 3, pp. 217-229.

Basnet, C., Corner, J., Wisner, J. and Tan, K.-C. (1999), "A survey of supply chain management practice in New Zealand", *Proceedings of the 34th Annual Conference of the Operational Research Society of New Zealand, Hamilton, December*, pp. 309-318, available at: http://citeseerx.ist.psu.edu

Bryman, A. and Bell, E. (2011), *Business Research Methods*, 3rd ed., Oxford University Press, Oxford.

Chen, J., Sohal, A.S. and Prajogo, D.I. (2013), "Supply chain operational risk mitigation: a collaborative approach", *International Journal of Production Research*, Vol. 51 No. 7, pp. 2186-2199.

Cheng, J.-H. (2010), "Inter-organizational relationships and information sharing in supply chains", *International Journal of Information Management*, Vol. 31 No. 4, pp. 374-384.

Christopher, M. (1992), *Logistics: The Strategic Issues*, Chapman and Hall, London.

Chu, W.H. and Lee, C.C. (2006), "Strategic information sharing in a supply chain", *European Journal of Operational Research*, Vol. 174 No. 3, pp. 1567-1579.

Damiani, E., Frati, F. and Tchokpon, R. (2011), "The role of information sharing in supply chain management: the security approach", *International Journal of Innovation & Technology Management*, Vol. 8 No. 3, pp. 455-467.

Daugherty, P.J., Richey, R.G., Genchev, S.E. and Chen, H. (2005), "Reverse logistics: superior performance through focused resource commitments to information technology", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 41 No. 2, pp. 77-92.

Doolin, B. (1994), "Case research in information systems: an alternative perspective (research report series)", Department of Management Systems, University of Waikato, Hamilton.

Du, T.C., Lai, V.S., Cheung, W. and Cui, X. (2012), "Willingness to share information in a supply chain: partnership-data-process perspective", *Information & Management*, Vol. 49 No. 2, pp. 89-98.

Eisenhardt, K.M. (1991), "Better stories and better constructs: the case for rigor and comparative logic", *Academy of Management Review*, Vol. 16 No. 3, pp. 620-627.

Eisenhardt, K.M. and Graebner, M.E. (2007), "Theory building from cases: opportunities and challenges", *The Academy of Management Journal*, Vol. 50 No. 1, pp. 25-32.

Ellinger, A., Shin, H., Magnus Northington, W., Adams, F.G., Hofman, D. and O'Marah, K. (2012), "The influence of supply chain management competency on customer satisfaction and shareholder value", *Supply Chain Management: An International Journal*, Vol. 17 No. 3, pp. 249-262.

Fawcett, S.E., Osterhaus, P., Magnan, G.M., Brau, J.C. and McCarter, M.W. (2007), "Information sharing and supply chain performance: the role of connectivity and willingness", *Supply Chain Management: An International Journal*, Vol. 12 No. 5, pp. 358-368.

Ferdows, K., Lewis, M.A. and Machuca, J.A.D. (2004), "Rapid-fire fulfilment", *Harvard Business Review*, Vol. 82 No. 11, pp. 104-117.

Fine, C.H. (2000), "The clock-speed chronicles", *Supply Chain Management Review*, Vol. 4 No. 2, pp. 60-64, available at: http://trid.trb.org

Hassini, E., Jungbae Roh, J., Hong, P. and Park, Y. (2008), "Organizational culture and supply chain strategy: a framework for effective information flows", *Journal of Enterprise Information Management*, Vol. 21 No. 4, pp. 361-376.

Johnson, M.E. (2008), "Information risk of inadvertent disclosure: an analysis of file-sharing risk in the financial supply chain", *Journal of Management Information Systems*, Vol. 25 No. 2, pp. 97-123.

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.

Kavoura, A., Sakas, D.P., Tomaras, P., Marinagi, C., Trivellas, P. and Reklitis, P. (2015), "Information quality and supply chain performance: the mediating role of information sharing", *Procedia – Social and Behavioral Sciences*, Vol. 175, February, pp. 473-479.

Kembro, J. and Näslund, D. (2014), "Information sharing in supply chains, myth or reality? A critical analysis of empirical literature", *International Journal of Physical Distribution & Logistics Management*, Vol. 44 No. 3, pp. 179-200.

Khan, O. and Burnes, B. (2007), "Risk and supply chain management: creating a research agenda", *International Journal of Logistics Management*, Vol. 18 No. 2, pp. 197-216.

Klein, R. and Rai, A. (2009), "Interfirm strategic information flows in logistics supply chain relationships", *MIS Quarterly*, Vol. 33 No. 4, pp. 735-762.

Kocoglu, I., Imamoglu, S.Z. and Ince, H. (2011), "Inter-organizational relationships in enhancing information sharing: the role of trust and commitment", *The Business Review*, Vol. 18 No. 2, pp. 115-123.

Kolluru, R. and Meredith, P.H. (2001), "Security and trust management in supply chains", *Information Management & Computer Security*, Vol. 9 No. 5, pp. 233-236.

Kwon, I.W. and Suh, T. (2005), "Trust, commitment and relationships in supply chain management: a path analysis", *Supply Chain Management: An International Journal*, Vol. 10 No. 1, pp. 26-33.

Kwon, I.-W.G. and Suh, T. (2004), "Factors affecting the level of trust and commitment in supply chain relationships", *Journal of Supply Chain Management*, Vol. 40 No. 2, pp. 4-14.

Lau, J.S.K., Huang, G.Q. and Mak, K.L. (2002), "Web-based simulation portal for investigating impacts of sharing production information on supply chain dynamics from the perspective of inventory allocation", *Integrated Manufacturing Systems*, Vol. 13 No. 5, pp. 345-358.

Levary, R.R. (2000), "Better supply chains through information technology", *Industrial Management*, Vol. 42 No. 3, pp. 24-30.

Li, S. and Lin, B. (2006), "Accessing information sharing and information quality in supply chain management", *Decision Support Systems*, Vol. 42 No. 3, pp. 1641-1656.

Madenas, N., Tiwari, A., Turner, C. and Peachey, S. (2015), "An analysis of supply chain issues relating to information flow during the automotive product development", *Journal of Manufacturing Technology Management*, Vol. 26 No. 8, pp. 1158-1176.

Marquez, A.C., Bianchi, C. and Gupta, J.N.D. (2004), "Operational and financial effectiveness of e-collaboration tools in supply chain integration", *European Journal of Operational Research*, Vol. 159 No. 2, pp. 348-363.

Mason-Jones, R. and Towill, D.R. (1997), "Information enrichment: designing the supply chain for competitive advantage", *Supply Chain Management: An International Journal*, Vol. 2 No. 4, pp. 137-148.

Mentzer, J.T., DeWitt, W., Keebler, J.S., Min, S., Nix, N.W., Smith, C.D. and Zacharia, Z.G. (2001), "Defining supply chain management", *Journal of Business Logistics*, Vol. 22 No. 2, pp. 1-25.

Roh, J., Hong, P. and Min, H. (2014), "Implementation of a responsive supply chain strategy in global complexity: the case of manufacturing firms", *International Journal of Production Economics*, Vol. 147, January, pp. 198-210.

Sahay, B.S. (2003), "Understanding trust in supply chain relationships", *Industrial Management & Data Systems*, Vol. 103 No. 8, pp. 553-563.

Samaddar, S., Nargundkar, S. and Daley, M. (2006), "Inter-organizational information sharing: the role of supply network configuration and partner goal congruence", *European Journal of Operational Research*, Vol. 147 No. 2, pp. 744-765.

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

Soon, C.B. and Gutiérrez, J.A. (2010), "Adoption of RFID in supply chains: a motivation and ability perspective", in Wang, J. (Ed.), *Supply Chain Optimization, Management and Integration: Emerging Applications*, IGI Global, Hershey, pp. 54-55.

Sridharan, R. and Simatupang, T.M. (2013), "Power and trust in supply chain collaboration", *International Journal of Value Chain Management*, Vol. 7 No. 1, pp. 76-96.

Stoneburner, G., Goguen, A. and Feringa, A. (2002), "Risk management guide for information technology systems", *NIST Special Publication*, Vol. 800 No. 30, pp. 1-41.

Tan, K.H., Wong, W.P. and Chung, L. (2015), "Information and knowledge leakage in supply chain", *Information Systems Frontiers*, Vol. 18 No. 3, pp. 621-638.

Vanpoucke, E., Boyer, K.K. and Vereecke, A. (2009), "Supply chain information flow strategies: an empirical taxonomy", *International Journal of Operations & Production Management*, Vol. 29 No. 2, pp. 1213-1241.

Walsham, G. (1995), "Interpretive case studies in IS research: nature and method", *European Journal of Information Systems*, Vol. 4 No. 2, pp. 74-81.

Wang, Z., Ye, F. and Tan, K.H. (2014), "Effects of managerial ties and trust on supply chain information sharing and supplier opportunism", *International Journal of Production Research*, Vol. 52 No. 23, pp. 7046-7061.

Whitman, M.E. (2004), "In defense of the realm: understanding the threats to information security", *International Journal of Information Management*, Vol. 24 No. 1, pp. 43-57.

Wu, I.-L., Chuang, C.-H. and Hsu, C.-H. (2014), "Information sharing and collaborative behaviors in enabling supply chain performance: a social exchange perspective", *International Journal of Production Economics*, Vol. 148, February, pp. 122-132.

Yin, R.K. (1994), *Case Study Research: Design and Methods*, 2nd ed., Sage Publications, Thousand Oaks, CA.

Yin, R.K. (2009), *Case Study Research: Design and Methods*, 4th ed., Sage Publications, Los Angeles, CA.

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

Zhang, C. and Li, S. (2006), "Secure information sharing in internet-based supply chain management systems", *The Journal of Computer Information Systems*, Vol. 46 No. 4, pp. 18-24.

Zhang, D., Cao, X., Wang, L. and Zeng, Y. (2012), "Mitigating the risk of information leakage in a two-level supply chain through optimal supplier selection", *Journal of Intelligent Manufacturing*, Vol. 23 No. 4, pp. 1351-1364.

Zhang, D.Y., Zeng, Y., Wang, L., Li, H. and Geng, Y. (2011), "Modeling and evaluating information leakage caused by inferences in supply chains", *Computers in Industry*, Vol. 62 No. 3, pp. 351-363.

Zhang, J. and Chen, J. (2013), "Coordination of information sharing in a supply chain", *International Journal of Production Economics*, Vol. 143 No. 1, pp. 178-187.

Zhonghua, Y. and Ling, Z. (2013), "Information sharing in supply chain: a review", *Journal of Digital Information Management*, Vol. 11 No. 2, pp. 125-130.

Zhu, K. (2002), "Information transparency in electronic marketplaces: why data transparency may hinder the adoption of B2B exchanges", *Electronic Markets*, Vol. 12 No. 2, pp. 92-99.

Zsidisin, G.A. (2003), "A grounded definition of supply risk", *Journal of Purchasing and Supply Management*, Vol. 9 Nos 5-6, pp. 217-224.

Further reading

Lim, J. S., Maynard, S. B., Ahmad, A. and Chang, S. (2015), "Information security culture: towards an instrument for assessing security management practices", *International Journal of Cyber Warfare and Terrorism*, Vol. 5 No. 2, pp. 31-52.

Appendix 1

Case (Company)	Size	Turnover (1,000 NZD)	Products	Value adding	Domestic/Export
Manufacturer 1	Large	28,500	A wide range of milking systems and components	Design, develop and test new systems	Domestic and export
Manufacturer 2	Large	28,500	Agricultural equipment and animal health delivery systems	Develop genuine innovation and do customization based on customers' requirements	Mainly export
Manufacturer 3	Large	62,150	Polyethylene flexible films, ready-made bags, promotional materials and labels	Custom manufacture according to clients' specifications and packaging	Domestic and export
Manufacturer 4	Large	31,500	Broad range of adhesive products	Manufacture, package and distribute	Domestic and export
Manufacturer 5	Large	19,513	Handling and process equipment for mining, construction	Design and manufacture large handling systems	Domestic market only
Manufacturer 6	Medium	7,695	Solid timber doors and accessories	Designs, customize and manufacture specialized doors	Domestic and export
Manufacturer 7	Small	2,752	Industrial and agricultural pneumatic wheels	Design, customize, and manufacture in small unit	Domestic and export
Manufacturer 8	Medium	7,125	Plastic injection moulding, blow moulding, and tool-making	Design, manufacture, post-sales services	Domestic and export
Distributor 1	Small	1,892	Pipe support systems and plumbing products	Wholesale and package	Domestic market only
Distributor 2	Small	2,093	Various types of software and applications for education and business purposes	Distribute, provide expert pre-sales advice, and training and after-sales support	Domestic market only
Exporter	Medium	4,235	Fish and mussels	Process, package and export	Mainly export

Table AI.
Overview of the 11
case companies

Appendix 2. Interview protocol
Based on the literature review an interview plan with developed using a mind-map technique. The interview guide provided the general structure of data collection and ensured consistency during the interview process across the sampled companies.
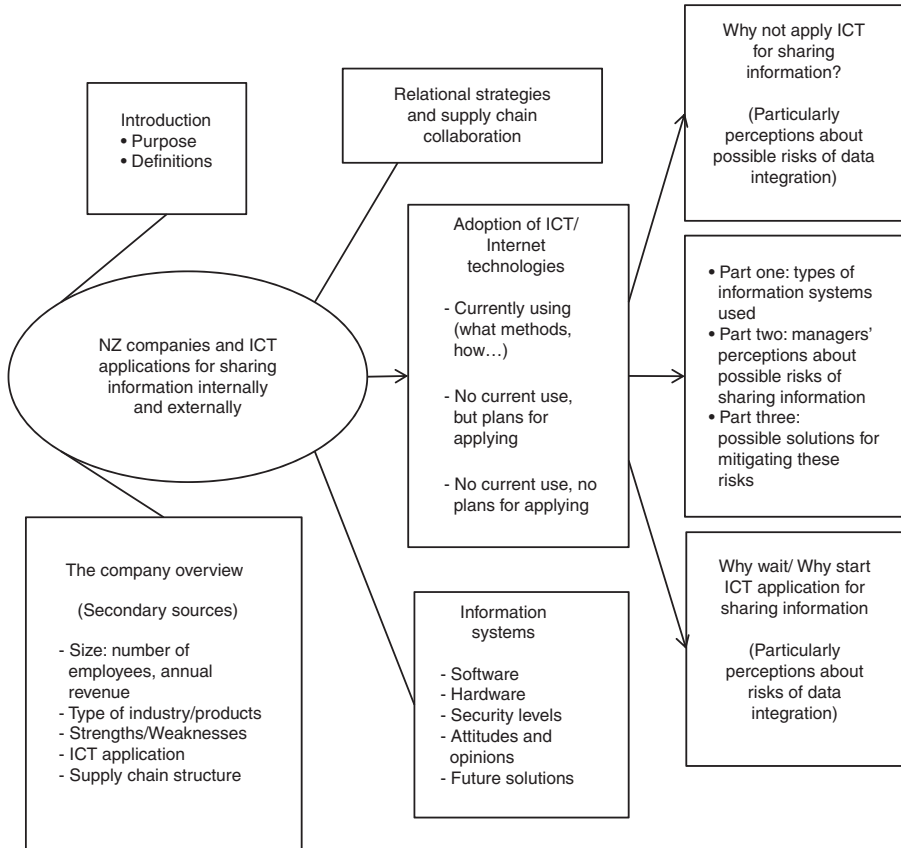
Figure A1.
Preliminary
interview guide

Corresponding author
Paul Childerhouse can be contacted at: p.h.j.childerhouse@massey.ac.nz