Annals of Operations Research
https://doi.org/10.1007/s10479-021-04219-5

S.I. : INFORMATION- TRANSPARENT SUPPLY CHAINS

A conceptual framework for information-leakage-resilience

Wai-Peng Wong[1] · Kim Hua Tan[2] · Kannan Govindan[3,4,5] · Di Li[6] · Ajay Kumar[7]

Accepted: 26 July 2021

Abstract
In today's dynamic and competitive business environment, it is critical for firms to share information selectively and develop organizational resilience. However, only a few existing studies examine the relationships between information management and supply chain resilience. Aiming to bridge the gaps between both domains, we propose a model encompassing information security culture, information leakage, information sharing effectiveness and supply chain resilience and to derive insights from their inter-relationships in this research. A cross-sectional survey of the multi-national corporations and small and medium enterprises among their senior managers in the United Kingdom was carried out for data collection. The data set was analysed using a structural equation modelling approach. The results obtained validate the proposed model. The findings ascertain that information security culture and information leakage are negatively correlated, which influence the supply chain resilience. Specifically, information security and information leakage affect the effectiveness of information sharing, which in turn positively and negatively influence the supply chain resilience, respectively. This study posits that information security culture is instrumental to mitigate information leakage and foster effective information sharing to strengthen supply chain resilience.

Keywords Information leakage · Information sharing effectiveness · Information security culture · Supply chain resilience

1 Introduction

For many manufacturers and service providers, a key to success and sustainability, particularly in today's information driven and highly uncertain market, is their organizational resilience i.e., firms are endowed with the flexibility, visibility and velocity in adapting to changes. In this dynamic and highly competitive business environment, firms face constant changes and must respond with appropriate information sharing for in order to be competitive. A resilient response by sharing the timely and correct information with business partners or supply chain members enables organizations to function sustainably. However, while information sharing is desirable in supply chain collaboration, structured methods to ensure the effectiveness of information sharing have not been empirically demonstrated

✉ Ajay Kumar
akumar@em-lyon.com

Extended author information available on the last page of the article

Published online: 05 August 2021

and validated (Mangus et al., 2020; Sener et al., 2019; Shaw et al., 2017). While there are reports of organisations and supply chains on knowledge sharing (Wang & Zhang, 2020; Wei et al., 2020), these investigations are typically anecdotal case studies. There is also a lack of scientific studies on information sharing strategies and issues faced by firms, such as degrees of information security culture and information leakage respectively and linking them to supply chain resilience.

Traditional information leakage studies mainly rely on mathematical principles to solve a particular problem. Recently, there has been an increased emphasis in information security covering a wide range of issues for example, cyberattacks, cybersecurity, information security culture and data/information leakage (Veiga et al., 2020). The present changing business landscape with a drastic increase in the amount of accessible data to businesses requires an approach towards 'information leakage resilience'. This will enable organizations to prevent and respond to potential threats and recover from attacks. Besides, collaborating firms should maximize the integrity of information to remain resilient (Ioannidis et al., 2019; Tabasso, 2019; Wong et al., 2020). Given the diverse research emphasis in the information management field, the issue of supply chain resilience pertaining to the direct and indirect effects of information security, information leakage and information sharing effectiveness has not been fully analyzed, which is the focus and contribution of this research.

A research initiative powered by three goals is defined in this article. The first goal is to understand from a literature perspective how practitioners identify and operationalize information security culture, information leakage, information sharing effectiveness and supply chain resilience. The second goal is to propose a model of conceptual structural equation to formulate the direct and indirect effects of information leakage, information security culture and information sharing effectiveness with respect to supply chain resilience. Finally, to validate the model, this study uses a data set from a survey of 478 senior executives in the UK to assess the relationships. This study contributes to theory by establishing the direct and indirect impacts of the constructs and by introducing a fresh framework. Practically, it indicates to firms seeking to create or sustain resilience that the interplay between information capabilities and risk will have an impact on supply chain resilience, which must be handled intelligently.

In the following sections, the research constructs and hypotheses derived from the literature are presented. Subsequent parts define the survey and methods and explain the demographic characteristics of respondents. This is accompanied by an examination of the outcomes of the survey and a review of the managerial consequences of this study.

2 Literature review

This section presents a review on information security culture, information leakage, information sharing effectiveness and supply chain resilience. The conceptual structural equation model that creates the direct and indirect relationships of the constructs to form the hypotheses is also explained in this section.

2.1 Information security culture

In response to the seriousness of cyber security related challenges, in today's global business environment, companies have invested heavily in advanced technologies to overcome

security threats and nurture information security awareness by promoting information security culture within an organization. Many firms have started to inculcate information security culture so they can more effectively manage information security threat (Veiga & Martins, 2015; Veiga et al., 2020), and promote security behavior and practices among employees in the organization (Nasir, et al., 2019). A strong information security culture can contribute to extraordinary "climate of trust" for a significant assimilation of this practice into everyday work and commitment by employees, therefore protecting organizational information through best practices training of human behaviors (Wiley et al., 2020). Employees will develop a higher security awareness to protect the physical and information assets of the organization. This will safeguard the organization from information leakage, which could otherwise jeopardize the resilience of the firm and subsequently its supply chain.

Although information security culture can increase information security awareness, it takes commitment and action across various parties in an organization to build a successful security culture. A successful security culture is defined as a set of principles shared by everyone in a company and a workforce that is highly engaged with and accountable for security concerns. Some organizations only put secondary emphasis on information security culture for instance, their refusal to prioritise the treatment of information security risks in the same way they treat financial and business risks. Studies have indicated that firms with low information security culture may not be able to address information leakage (Veiga et al., 2020) and foster closer collaboration with suppliers to build organizational resilience (Ulhaq et al., 2016).

While firms are likely to give different emphasis on information security culture, the practice of information security typically focuses on nurturing basic practices of good data protection, computer systems and security-minded thinking in all actions (Veiga & Martins, 2017). The study of Mupepi et al. (2017) discovered that companies use information security culture to classify security risk and build a shared mindset among employees to minimize such risk. The measures range from the use of passwords to protect files and documents, authentication and authorization procedures for accessing confidential information, to verification and scanning of outgoing emails for preventing information leaking to outsiders and unauthorized recipients. Alhogail and Mirza (2014) also asserted that the culture of information security is central to the successful achievement of an organisation's information security agenda.

In this study, six information security culture characteristics used to manage supply chain resilience are selected to represent information security culture practices. On a 5-point Likert scale (1 = low, 5 = high), the respondents have been asked to determine the importance of each information security culture items in their company' activities.

2.2 Information leakage

Over the last decade, information leakage has emerged as a major hurdle in information sharing. Information leakage refers to intentional or unintentional disclosure of exclusive data and/or materials to unauthorised parties. Cheng et al. (2017) argued that information leakage can cause loss to a company and affect its ability to achieve a competitive edge. Intentional information leakage involves employees deliberately disclosing information to unauthorized parties. Huong Tran et al. (2016) suggested that intentional leakage is often caused by employees' dissatisfaction with the company or an inducement for personal benefits. The primary cause of intentional leakage is revenge and/or unethical behaviour

of employees who are willing to betray their companies by leaking sensitive information to competitors (Anand & Goyal, 2009; Huong Tran et al., 2016). These cause harm to the organization's reputation and its business revenue. On the other hand, unintentional information leakage can occur if employees are unclear about how much or little information should be disclosed to outsiders (Huong Tran et al., 2016). The pervasiveness of this uncertainty in the workplace puts the organization's information assets at risk.

Anand and Goyal (2009), a pioneer in information leakage in supply chain study, describe the challenges facing exchanging information in the supply chain noting the risk of leakage of information. The findings indicate that initiatives such as projection and replenishment of joint planning and Vendor Controlled Inventory (VMI) can accelerate exchange of data among supply chain members e.g., between retailers and manufacturers as well as between producers and suppliers who use their reciprocal inputs. However, these initiatives increase the risk pertaining to leakage of shared data to unintended recipients in the supply chain. Similarly, Mello (2012) identified confidential information given to an authorized second party in a supply chain could be unwittingly revealed to a third party.

Douglas (2004) and Adewole (2005) studied the fear and negative implications of information that can result in the unwillingness for companies to not exchange data and gain the associated benefits such as allowing better and quicker decision making and improving customer service. According to Douglas (2004), the Collaborative Planning, Forecasting and Replenishment (CPFR) processes were developed to enable Walmart and its vendors exchange forecasts and POS (point of sales) details. However, within the vendor organisations, the sales teams were reluctant to share data with their own corporate offices for fear of disclosure to third parties and getting into trouble with Wal Mart. Similarly, Adewole (2005) pointed out that the UK clothing retailers were unwilling to share information with suppliers because they knew that suppliers could unwittingly provide confidential information to rivals.

From the literature covering academics and practitioners, a variety of viewpoints on information leakage exist. Accordingly, 11 commonly used information leakage scenarios have been selected and translated into information leakage questionnaire items in this study. On a 5-point Likert scale (1 = low, 5 = high), the respondents have been asked to indicate the extent pertaining to each scenarios in their organizations.

2.3 Information sharing effectiveness

The efficacy of exchanging information plays an important role before and after a supply chain disruption (Kamalahmadi & Parast, 2016; Soni & Jain, 2011). Information sharing requires the exchange of real-time, two-way data on various aspects of operations management (e.g., inventory levels, order status, delivery schedules, etc.) as well as forecasts and preparations for supply chain partners. These factors have significant effects on a supply chain's efficiency (Lee & Whang, 2000; Li et al., 2020a, 2020b). By sharing information effectively, each supply chain member receives accurate and timely information at every node (Li et al., 2020a, 2020b; Manatsa & McLaren, 2008). This is useful for timely manufacturing, inventory management, packaging and logistics decision for enhancing supply chain efficiency and performance (Li & Lin, 2006).

The effectiveness of information sharing in the supply chain can be enhanced by technology such as blockchain. Blockchain is a distributed ledger technology which offers transparency of information through real time tracking and tracing (Fan et al., 2020) for members in the supply chain. Choi (2020) showed that a

blockchain-supported supply chain incurs a lower level of operational risk than that of a traditional chain. In a similar vein, Fan et al. (2020) highlighted that factors affecting the adoption of blockchain technology in supply chain are related to the traceability awareness of consumers, the production costs of supplier and manufacturer, and the cost of using the blockchain technology. Given a favourable cost–benefit trade-off, companies are willing to adopt the blockchain technology and those which choose to implement this ground-breaking invention can certainly gain higher information sharing effectiveness. Consequently, the accomplishment of information sharing effectiveness is distinctively valuable, which improves the competitive advantage of a firm. Effective information sharing is advantageous in restoring a supply chain to its initial or better condition following a disruptive event. This directly helps improve supply chain resilience.

Studies in the literature have acknowledged information sharing as a significant supply chain resilience precedent (Kamalahmadi & Parast, 2016; Scholten & Schilder, 2015). According to Brandon Jones et al. (2014), establishing a supply chain culture where knowledge is exchanged among its participants in the supply chain stands as the main priority for collaborative work and risk reduction. The first step towards ensuring accountability and building trust is to share relevant details (Mandal, 2012). Mandal (2012) argued that when each participant receives relevant information efficiently and effectively, a closer cooperation occurs. Collaboration in the supply chain entails sharing of data and implementation of common and confidential information across the chain to minimise ambiguity (Tseng et al., 2020). Information exchange effectiveness also increases visibility (Nishat et al., 2007), operational performance and effectiveness, and enhances customer service. Thus, implementing a proper flow with respect to shared information throughout the supply network is important (Day, 2014).

According to several studies, effective information sharing is critical to improve supply chain efficiency (Baihaqi & Sohal, 2013; Lee & Whang, 2000; Li & Lin, 2006; Manatsa & McLaren, 2008). By taking relevant data and exchanging them with supply chain parties, a company can provide rapid access to the required information to improve the supply chain's quality and efficiency to meet the needs of customers (Li & Lin, 2006). Organizations aim to create strategic relationships with their supply chain participants in a highly unpredictable world with evolving markets to exchange knowledge, improve operational stability and reduce the risk associated with uncertainties (Li & Lin, 2006). Studies have also shown that cooperative information sharing between supply chain members increases the productivity and quality of supply chains (Huong Tran et al., 2016; Li & Lin, 2006; Ponte et al., 2020; Sezen, 2008; Shen et al., 2019). Nevertheless, these studies did not analyze the relationships among vulnerabilities (information leakage), practices (information security culture) and outcome (resilience).

Based on the above account, it is clear that studies in the literature supports the notion that information sharing effectiveness is an important assurance for supply chain resilience. The above literature review also reveals that there is a gap on the linkage between barriers and enablers with respect to information sharing effectiveness, in order to achieve resilience. To operationalize this construct, 10 information sharing effectiveness items have been identified in this study. On a 5-point Likert scale (1 = low, 5 = high), the respondents have been asked to indicate the importance of each criterion of information sharing effectiveness in their organizationss.

2.4 Supply chain resilience

Having an effective supply chain management to remain resilient is becoming a major focus of companies in today's dynamic world, especially for multinationals corporations (MNCs) as well as Small and medium enterprises (SMEs) that have global operations. Most businesses desire to stay resilient by acquiring the ability to recognize and address vulnerabilities and adjust to unexpected disruptions. However, disruptions are highly unpredictable and highly dependent on many factors particularly when information sharing is involved. Effective information sharing across organization with diverse goals and perspectives is difficult because it requires sharing the right information, at the right level of detail, using the right language, at the right time, in the right context, with the right people, and all these factors can lead to information sharing breakdown. Firms participate in supply chain collaboration efforts to utilize the latest information in the market and mitigate the probability of bullwhip effects (de Almeida et al., 2015). Studies in the literature indicate that these collaborative partnerships are formed by firms so that they and their supply chain partners can communicate accordingly to swiftly adjust to changes when disruption hits the organization and supply chain. Li et al. (2020a, b) argued that a direct information acquisition is profitable only if its cost is low and it helps the manufacturers to gain better demand and reduce the expenditure of subsidization. Katsaliaki et al. (2020) showed knowledge of supply chain disruptions and resilience in their in-depth literature review, examining various modeling approaches on the topic. Their findings indicate digital technologies applied in information sharing, especially the more recent ones such as IoT, 3D and blockchain are progressively changing the way supply chains are organized and operationalised. The level of accuracy, transparency, traceability and flexibility are immensely growing, transforming supply chains to systems which continuously evolve and can be reconfigured on demand. Applicability studies of these technologies form the direction of future research. The rapid-spreading pandemic is changing business model by fast-tracking digital transformation to increase chances of survival.

Muller and Koslowski (2012) and Muller et al. (2013) indicated that managing resilience such as regulating risks within organizational boundaries as well as throughout the network of suppliers are related to information management. The concept of managing information to achieve resilience is assuring security, as well as ensuring efficient and effective information sharing (Singh et al., 2019) to enable rapid adjustment for an organization and the operations in the supply chain. Information sharing and collaborative communication (Guan et al., 2020; Scholten & Schilder, 2015) provide a higher level of visibility, velocity and flexibility thereby making a supply chain more resilient.

Research has also explored the following terms and concepts of supply chain resilience, i.e., agility and sturdiness (Wieland & Wallenburg, 2013), visibility and synchronisation (Brandon-Jones et al., 2014), adaptability and versatility (Ivanov et al., 2014), and the links between the supply chain partnership (Tukamuhabwa et al., 2015). Autry et al. (2013) focused on the strategic dimensions of supply chain management resilience with increasing integration of sustainability consideration. MacDonald et al. (2018) confirmed the effect of resilience on the efficiency of a company and its general supply chain. Govindan et al. (2015) balanced the Lean Six Sigma managerial principles with resilience, while Petit et al., (2019) recommended examining resilience through the linkages between vulnerability and capabilities.

Many concepts of resilience have been proposed in the literature. The recent call to explore linkages between vulnerability and capabilities signify the growing interest

towards connecting the dots between information management and supply chain resilience. From our review, supply chain resilience is operationalized to form linkages with managing information pertaining to the three main dimensions of resilience i.e., visibility, velocity and flexibility (Scholten & Schilder, 2015). In our analysis, fourteen items have been described. On a 5-point Likert scale (1 = low, 5 = high), the respondents have been asked to indicate the importance of each item in their pursuit of supply chain resilience.

2.5 The conceptual framework: research hypotheses

The conceptual model is built on the foundation of Resource-Based View (RBV). The RBV is adopted for analysis of the information security culture, information sharing effectiveness and supply chain resilience and these correspond to the asset-capability, competitive advantage and performance outcome. Information security culture is considered a special and unique ability that contributes to the development of an organisation's competitive advantage. Hence, the RBV is a good approach to analyze and explain the relationships among information security culture, information sharing effectiveness and supply chain resilience.

The use of RBV can be traced back to previous investigations in supply chain risks and resilience (Brandon-Jones et al., 2014; Stevenson & Busby, 2015). Risk management in the supply chain involves identifying risk behaviours in the supply chain activities that can impact the members and prescribing measures to retain their competitive advantage (Dubey et al., 2017). Information leakage is considered a danger in the supply chain in this regard. In the same way, in supply chain risk management, information security culture could address information leakage for competitive advantage.

According to the RBV, an organization is viewed as a set of tools and skills that can result in improved performance (Wernerfelt, 1984). Firm resources apply to all properties, capabilities, organisational processes, company characteristics, knowledge, information and others, and under the organisation's supervision, these resources can be exploited for achieving efficiency and effectiveness in businesses (Barney, 1991). In this study, information is regarded as an asset or resource, while capabilities refer to the organization's competence in utilizing the available resources to perform a task through the use of organizational procedures to achieve a desired end. Therefore, information security culture is a resource capability (Newbert, 2007). This resource-capability cannot be easily transferred from one organisation to another without shifting the ownership of the organisation itself or shifting any relatively self-contained subunit of the organisation.

RBV contends that interaction and coordination of resources are necessary to create effective mitigation (Blackhurst et al., 2011), which include information security culture. In this research, we analyze an organization's mitigation strategy to curb information leakage through coordination and utilisation of its resources to implement information sharing capabilities. Managers can establish a formal risk management infrastructure by cultivating information security culture to enhance information security awareness and mitigate information leakage. Correspondingly, the first hypothesis (H1) is that information security culture and information leakage are inversely correlated. RBV further emphasizes the importance of resource capabilities to help an organisation create or implement methods that maximise its efficacy and performance. By bundling an organization's assets for information security culture, it can enhance information sharing effectiveness as the competitive advantage. Therefore, the second hypothesis (H2) is that Information security

culture significantly influences the advantage of information sharing effectiveness. On the other hand, information leakage is a hurdle in information sharing. Therefore, the third hypothesis (H3) poses that information leakage negatively influences information sharing effectiveness.

From the RBV perspective, companies that nurture information security culture within its operations utilises it as a useful resource-capability to achieve specific objectives or goals for a high level supply chain resilience. Therefore, information is utilized by members for flexibility, velocity and visibility predominantly to build a resilient supply chain (Jüttner & Maklan, 2011; Scholten & Schilder, 2015; Scholten et al., 2014; Sodhi & Tang, 2019). Hence, the fourth hypothesis (H4) is information security culture significantly influences supply chain resilience while the fifth hypothesis (H5) is information sharing effectiveness significantly influences supply chain resilience. Lastly, the bane of information sharing i.e. information leakage compromises an organization's competitive information assets and subsequently hamper the achievement of supply chain resilience. Therefore, information leakage is expected to have a detrimental impact on supply chain resilience (H6).

For operationalization of our proposed model, the items for the constructs are adapted from past studies in the literature i.e. information security culture (ISC) items are adapted from Chen et al. (2015), information leakage (IL) items from Ritala et al. (2015), information sharing effectiveness (ISE) items from Fawcett et al. (2007) and supply chain resilience (SCR) items from Ahimbisibwe et al. (2016). These constructs and their relationships are depicted in Fig. 1.

3 Survey methodology

A survey approach was adopted to collect the primary data for evaluating the conceptual framework. The main body of the survey consists of three parts i.e., background questions, Likert-scale questions, and open-ended questions. In addition, a set of screening questions was formulated to ensure that the participants were qualified for the research designed. The study unit used in this research was the organization, and the method was intended for a single respondent. The data collection started in mid-2019 and finished in March 2020 with the survey administered and distributed online. The target participants were employees or managers with knowledge and practical experience of information sharing as well as information leakage in the UK, irrespective of industry and size. To encourage participation,

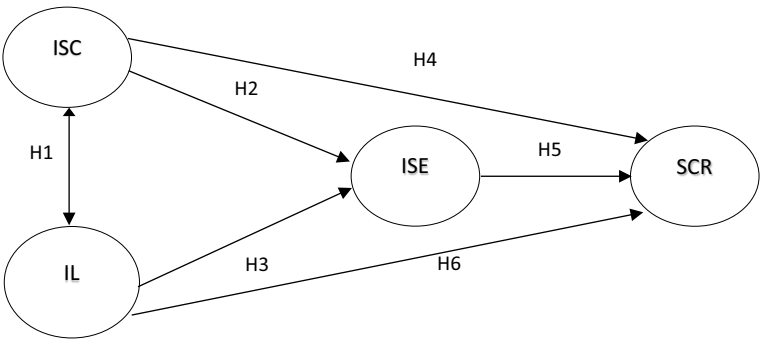

Fig. 1 Conceptual model of information–leakage–resilience

we emphasized the assurance of confidentiality and anonymity of the information collected and in the analysis of our findings. Concomitantly, the respondents were welcomed to provide their email addresses if they wished to receive a copy of the research findings. In total, 1500 responses were received, which went through a thoroughly examination to ensure completeness. Responses with any missing values and unengaged responses were discarded. This resulted in a data set of 478 responses eligible for further analysis representing a response rate of 31.87%. The profiles of respondents are shown in Table 1, which indicate that the sample covers a wide range of industries and company sizes with a fair distribution to offer good generalization of the data set.

4 Data analysis and results

Structural equation modelling (SEM) in AMOS version 23 was employed to validate the model and formulate the structural relationship between predictors and constructs of criteria. The software is a user-friendly statistical package (Joe Jr et al., 2014). It allows researchers to either specify the model by drawing a path diagram in AMOS graphics or to directly write the equation statements through AMOS basics (El-Sheikh et al., 2017).

4.1 Descriptive statistics and correlations of the constructs

The means, standard deviations and Pearson correlations among the constructs are shown in Table 2. The results show that information leakage is below the centre of the scale (M = 1.957, SD = 0.863). The general assessment with respect to supply chain resilience is in the centre of the scale (M = 3.691, SD = 0.717). Information sharing effectiveness

Table 1 Profiles of the responding organisations

	Number	Percentage
Industry sector		
Automotive & transport	31	6.49
Chemical & adhesives products	38	7.95
Electronic & technology	105	21.97
Food & beverage	55	11.51
Furniture, carpets & wood related products	41	8.58
Iron, steel & metal products	65	13.60
Paper, packaging, labelling & printing	26	5.44
Pharmaceutical & medical equipment	44	9.21
Machinery & industry equipment	73	15.27
Total	478	
Number of employees		
< 100	161	33.68
100–500	126	26.36
501–1000	82	17.16
> 1000	109	22.80
Total	478	

Table 2 Descriptive statistics and correlations of the constructs

Constructs	Mean	SD	1	2	3	4
1. SCR	3.691656	0.71713	1			
2. ISC	3.698488	0.835112	.569**	1		
3. ISE	3.719574	0.696345	.705**	.796**	1	
4. IL	1.956976	0.863311	− .391**	− .474**	− .511**	1

N = 478; *$p < 0.05$; **$p < 0.01$

dominates the results of prospects (M = 3.720, SD = 0.696), which is followed by information security culture (M = 3.698, SD = 0.835).

The findings reveal strong correlations between information security culture and supply chain resilience ($r = 0.569$, $p < 0.01$). The importance of organizational awareness to security implications is highly probable that organizations can effectively manage its valuable information within supply chain. Similarly, information sharing effectiveness is positively correlated with supply chain resilience in a strong manner ($r = 0.705$, $p < 0.01$). Indeed, sharing the best knowledge is critical in the supply chain in minimizing the bullwhip impact and increasing the level of situational awareness of supply chain disruptions. There is an inverse relationship between information leakage and supply chain resilience ($r = -0.391$, $p < 0.01$), indicating that the risk of information leakage in supply chains is unwanted and is harmful to an organization.

A very strong positive correlation between information security culture and information sharing effectiveness is found ($r = 0.796$, $p < 0.01$). Information security culture provides significant measures in protecting and securing valuable information through security awareness, actions and responsibility, in order to ensure overall effectiveness. Furthermore, a negative association exists between information leakage and culture of information security ($r = -0.474$, $p < 0.01$). Information security culture is a crucial strategy in mitigating information leakage, which is the crux of the conflict in information sharing. Finally, a negative correlation between information leakage and information sharing effectiveness is found ($r = -0.511$, $p < 0.01$), indicating that information leakage poses a high risk in undermining information sharing effectiveness within a supply chain.

4.2 Model evaluation

4.2.1 Measurement model

Firstly, the measurement model proves to be a good fit. From Table 3, the Root Mean Square Error of Approximation (RMSEA) value is 0.041, suggesting a reasonable match (Kline, 2010), similar to 2.228 value of normed chi-square (Bollen, 1990; Kline, 2010). The Comparative-Fit Index (CFI) is 0.927 and the Tucker-Lewis Index (TLI) is 0.923, both are larger than the threshold value 0.90 for a good fit proposed by Bollen (1990) and Byrne (2010). However, two indices show a not-so-good fit i.e., the Normed- Fit Index (NFI) which has a value of 0.876 and the goodness-of- fit index (GFI), a transformation of the chi-square, with a value of 0.831, both are slightly below the mark of acceptability (Jöreskog & Sörbom, 1993). This is because both NFI and GFI rely strongly on the sample size (Fornell & Larcker, 1981). These goodness-of–fit tests are

Table 3 Model fit of the model of measurement, structural model

	Thresholds for acceptable fit	Measurement model	Structural model
$\chi 2$ (df)		1722.13	1383.251
$\chi 2$/df	1.00–5.00	2.228	1.811
RMSEA	< 0.05–0.08	0.051	0.041
GFI	> 0.90	0.831	0.873
CFI	> 0.90	0.927	0.952
TLI	> 0.90	0.923	0.949
NFI	> 0.90	0.876	0.9

less relevant considering the large sample and the values obtained gave no support for a bad model fit. As can be seen from the values, they are marginal and are close the threshold value of 0.90, therefore the overall fit indices can be considered an acceptable model fit.

Table 4 presents the CFA-factor loadings basis, reliability and average variances extracted (AVE). The standardized factor loadings range between 0.647 and 0.851, which meet the satisfactory threshold of 0.70, while only six coefficients are accepted (Chin, 1998; Hair et al., 2017). In all cases, the composite reliability scores range between 0.918 and 0.943, which exceed the acceptability value of 0.70 for reliable constructs (Hair et al., 2017). Similarly, the AVE scores for individual constructs range between 0.512 and 0.66, which are above the 0.50 cut-off point recommended by Fornell and Larcker (1981).

By using the Fornell-Lacker (1981) criterion for discriminant validity, this study compares the value of AVE square root for each construct, and the outcome should be larger than the value of each inter-correlation construct. The results in Table 5 indicate that the evidence of a construct is distinctly different from other constructs in the model. Table 5 also shows that the Mean Shared Variance (MSV) scores must be lower than their AVE values for confirming discriminant validity. The six main constructs of MSV range from 0.232 to 0.521. They are smaller than the AVE scores, which range from 0.512 to 0.66. Consequently, the discriminant validity pertaining to the full model constructs is met.

Table 4 Factor loadings, estimates of composite reliability and AVE (N = 487)

	Standardized factor loadings	Composite reliability	Average variance extracted (AVE)
IL (11 items)	0.715–0.851	0.942728	0.600035
ISC (6 items)	0.792–0.830	0.921032	0.660393
ISE (10 items)	0.647–0.782	0.917815	0.528161
SCR (14 items)	0.654–0.756	0.936213	0.512366

Table 5 Discriminant validity

	MSV	MaxR(H)	IL	ISC	ISE	SCR
IL	0.232	0.945	0.775			
ISC	0.521	0.922	− 0.430	0.813		
ISE	0.521	0.920	− 0.482	0.722	0.727	
SCR	0.429	0.937	− 0.366	0.465	0.655	0.716

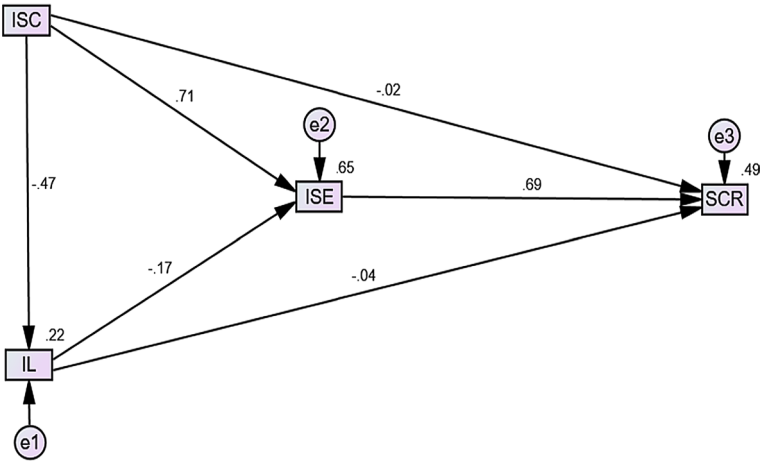

Fig. 2 The results of the structural model evaluation

Table 6 Direct effects

Hypothesis				Estimate	*P*	Conclusion
H1	IL	<––	ISC	– 0.474	***	Significant negative direct effect
H2	ISE	<––	ISC	0.714	***	Significant positive direct effect
H3	ISE	<––	IL	– 0.173	***	Significant negative direct effect
H4	SCR	<––	ISC	0.014	0.797	Not significant
H5	SCR	<––	ISE	0.674	***	Significant positive direct effect
H6	SCR	<––	IL	– 0.041	0.286	Not significant

***Correlation is significant at the 0.001 level (2-tailed); **Correlation is significant at the 0.01 level (2-tailed); *Correlation is significant at the 0.05 level (2-tailed)

4.2.2 Structural model

Before the path coefficients of the proposed hypothesis are determined, the model fit is first evaluated (see Table 3). RMSEA is 0.041, which is under the cut-off value, and this signifies a good fit. The GFI, CFI, TLI and NFI are 0.873, 0.952, 0.949 and 0.9, respectively, and all are almost equal to or above the 0.90 level, which indicate an acceptable fit (Bollen, 1990; Byrne, 2010). Therefore, the structural model has a good match and meets the fitness model threshold criterion. Figure 2 shows the constructs, namely information leakage (IL), information security culture (ISC), information sharing effectiveness (ISE) and supply chain resilience (SCR), in AMOS version 23 graphics.

After obtaining the fitness of structural model, the direct effects are analyzed. Table 6 shows the standardized direct effects between predictors and outcome variables. Hypothesis 1 posits that information security culture and information leakage are inversely correlated. As expected, a significant negative relationship exists between both variables ($\beta = -0.474$, $p < 0.001$), indicating that information security culture has a negative impact on information leakage (H1 is therefore supported). Hypothesis 2 suggests that information security culture influences information sharing effectiveness. The findings indicate a

significant positive relationship between information security culture and information sharing effectiveness ($\beta = 0.714$, $p < 0.001$). This means developing an organizational information security culture is a vital practice enabling a smooth flow of confidential information (H2 is supported). H3 postulates that information leakage negatively influences information sharing effectiveness. This is ascertained by the significant negative impact of information leakage on the information sharing effectiveness ($\beta = -0.173$, $p < 0.001$). The leakage of confidential data and vital information to unauthorized parties can damage the reputation and trust of organizations (H3 is supported). Hypothesis 4 recommends that information security culture significantly influences supply chain resilience. Surprisingly, information security culture is not statistically significant with respect to supply chain resilience, as indicated by the path coefficient ($\beta = 0.014$, $p = 0.797$); therefore H4 is not supported. Furthermore, Hypothesis 5 proposes that information sharing effectiveness significantly influences supply chain resilience. Indeed, information sharing effectiveness affects supply chain resilience, and the relationship is positive ($\beta = 0.674$, $p < 0.001$). Information sharing effectiveness can ensure fairness, reliability and transparency in business activities, which can improve supply chain resilience (H5 is supported). Lastly, Hypothesis 6 expects that information leakage negatively influences supply chain resilience. The results explain that the relationship between information leakage and supply chain resilience are not statistically significant ($\beta = -0.041$, $p = 0.286$); therefore Hypothesis 6 is not supported. In conclusion, all proposed hypotheses of this study are supported, except H4 and H6.

Table 6 reports the direct effects. We discover interesting findings as compared with our posited hypotheses. Specifically, a mediation analysis is employed to explain more clearly why H4 and H6 are not supported. To calculate the indirect results at the 95% confidence interval, we use the bias-corrected bootstrap method suggested in Preacher and Hayes (2004, 2008).

Table 7 shows the mediation analysis results. An indirect relationship exists between information security culture and supply chain resilience through information sharing effectiveness. Correspondingly, information security culture is significantly associated with supply chain resilience ($\beta = 0.569$, $p < 0.001$), which fully satisfies the condition for direct effect without mediator. Continuing the direct effect with mediator indicates that it is not positively correlated ($\beta = 0.021$, $p = 0.691$). Lastly, the indirect relationship between information security culture and supply chain resilience ($\beta = 0.548$, $p = 0.001$) is significant by adding information sharing effectiveness in the model. These results point to a full mediation.

Meanwhile, the results indicate the relationship between information leakage and supply chain resilience can be mediated by information sharing effectiveness. The direct effect without mediator between information leakage and supply chain resilience ($\beta = -0.391$, $p < 0.001$) is significant, and information leakage is not associated with supply chain resilience ($\beta = -0.042$, $p = 0.267$). Finally, the outcome indicates the indirect effect between information leakage and supply chain resilience through information sharing effectiveness is significant ($\beta = -0.35$, $p = 0.001$), which leads to full mediation.

Similarly, Table 7 shows the results of the indirect effects between information security culture and information sharing effectiveness through information leakage. The relationship between both elements is significant ($\beta = 0.796$, $p < 0.001$), which fully satisfies the condition of direct effect without mediator. Continuing the path coefficient of direct effect with mediator shows that information security culture is positively correlated with information sharing effectiveness ($\beta = 0.714$, $p < 0.001$). Lastly, the results signify that the indirect relationship between information security culture and information sharing effectiveness ($\beta = 0.082$, $p = 0.001$) is significant by adding information leakage in the model.

Table 7 Standardized direct without mediator, direct with mediator and indirect effects

Relationship	Path				Direct without Mediator/P	Direct with Mediator/P	Indirect/P	Conclusion
SCR	<––	ISE	<––	ISC	0.569 (***)	0.021 (0.691)	0.548 (0.001)	Significant, full mediation
SCR	<––	ISE	<––	IL	− 0.391 (***)	− 0.042 (0.267)	− 0.35 (0.001)	Significant, full mediation
ISE	<––	IL	<––	ISC	0.796 (***)	0.714 (***)	0.082 (0.001)	Significant, partial mediation
SCR	<––	IL	<––	ISC	0.569 (***)	0.495 (***)	0.074 (0.001)	Significant, partial mediation

***Correlation is significant at the 0.001 level (2-tailed); **Correlation is significant at the 0.01 level (2-tailed); *Correlation is significant at the 0.05 level (2-tailed)

Note that the magnitude of the beta coefficient value decreases, signifying that information leakage suppress the relationship. From this study, one can conclude that information leakage partially mediates the relationship between information security culture and information sharing effectiveness.

In addition, the mediation effect of information leakage between information security culture and supply chain resilience is depicted in Table 7. Information security culture is significantly associated with supply chain resilience ($\beta = 0.569$, $p < 0.001$), which fully satisfies the condition of direct effect without mediator. The direct effect with mediator of both elements is positively associated ($\beta = 0.495$, $p < 0.001$). Lastly, the finding shows the indirect relationship exists between information security culture and supply chain resilience via information leakage is significant ($\beta = 0.074$, $p = 0.001$). It can be concluded that is a partial mediation in the relationship. In other words, the relationship between information security culture and resilience of supply chain is suppressed by information leakage.

The amount of variation in the dependent variables elucidated by the independent variables is indicated by the R^2 value (Chin, 1998). To attain a minimum degree of explanatory capacity, the R^2 values should be high enough for the model (Urbach & Ahlemann, 2010). The model is able to explain 22% of the variation in information leakage. In comparison, the model indicates 65% of the variation in effectiveness of information sharing and 49% of variation in supply chain resilience.

5 Discussion and managerial implications

Several observations and conclusions can be drawn from this analysis. In general, the evidence from the survey supports the proposed structural equation model pertaining to information-leakage-resilience as derived from the literature and RBV. A direct inverse relationship exists between information security culture and information leakage. Information leakage negatively affects supply chain resilience on both direct and indirect manners through information sharing effectiveness. In addition, information security culture affects information sharing effectiveness. The sample data set also indicate that information security culture influences supply chain resilience directly and indirectly through information sharing effectiveness.

The significant inverse relationship between information security culture and information leakage (H1) implies that firms should use information security culture to mitigate information leakage. As an example, since information leakage is caused by employees intentionally or unintentionally to disclose confidential information to unauthorized parties, firms should proactively inculcate information security culture in the company to raise employees' security mindfulness when handling information. The respective information security culture should emphasize on employees' ethical conduct at workplace and implement punitive measures on employees who leak information intentionally. Mitigation of information leakage helps protect an organization's information assets and sustain its competitive advantage. To circumvent information leakage, a firm must nurture its information security culture and focus on ethical and responsible practices in information handling and transmission. Otherwise, information leakage which is the Achilles heel of information sharing can destroy supply chain resilience.

A significant positive relationship between information security culture and information sharing effectiveness (H2) indicates that the former is instrumental for fostering information sharing capabilities and enduring their effectiveness. An organizational culture

practices mindfulness in information handling, prioritizes ethical conduct, responsibility and information security leads to effective information sharing internal and external to the organization. Effective information sharing forms the foundation of strong collaboration which is the backbone for supply chain resilience (H5).

A supply chain with strong resiliency often exhibits a company's competitive position in the marketplace. Correspondingly, a weak supply chain resilience delays or hinders an organisation to recover swiftly from information leakage or theft. Such a company could lose its clients, therefore fail and perish. In contrast, information leakage negatively affects information sharing effectiveness (H3), or in other words, mitigation of information leakage enhances information sharing effectiveness. As an example, when an attempt to leak information is thwarted, an organisation could preserve its information integrity and avoid losing its competitive advantage. Ethical and security conscious employees are more likely to act in the interest of their organization. When employees are inclined to handle information ethically and with care, the process of sharing information becomes more effective.

Information leakage is caused by employees' behaviours. Employees may intentionally leak confidential information to competitors for personal benefits, thus risking an organization's competitive edge. There are also cases where employees unintentionally disclose information to unauthorised recipients. This is often due to a low awareness among employees with respect to the asset value of information. Both scenarios can be mitigated by enhancing information security culture. With a strong information security culture, employees are trained to be careful in handling information. This can reduce deliberate leakage by insiders, especially when they know more employees are vigilant about suspicious behaviours. These watchful employees act as extra pairs of eyes to help safeguard confidential information of their organization.

Interestingly, insignificant relationship exist between information security culture and supply chain resilience (H4) as well as between information leakage and supply chain resilience (H6), which could be caused by the existence of a mediator. Further analysis on mediation reveals that information sharing effectiveness is a full mediator between these two relationships. On the one hand, information security culture facilitates an organization to share information effectively and subsequently information sharing effectiveness leads to enhanced supply chain resilience. The mediation effect of information sharing effectiveness in this case is positive. On the other hand, information leakage negatively impacts supply chain resilience by making an organization unresponsive to information sharing. In other words, an organization is not able to share information effectively, therefore aggravating its resiliency which depends tremendously on an effective information sharing mechanism.

The mediation analysis also reveals that information leakage is a partial mediator between information security culture and information sharing effectiveness. The effect of information leakage is negative in this case. In other words, information leakage suppresses the relationship between information security culture and information sharing effectiveness. When information leakage occurs, the intent and benefits of information security culture on information sharing effectiveness is badly affected.

6 Conclusion, limitation and future research

This study has analyzed and demonstrated empirically, the relationships among information security culture, information leakage, information sharing effectiveness and supply chain resilience. Supply chain managers who comprehend these relationships can exploit

this information to manage information assets in their organisations and ensure a competitive edge in the market. Furthermore, understanding of these relationships are crucial to help managers in considering and planning how different capabilities within an organization can work together. The ability to secure information and foster an environment with security-minded people enables the firm to improve its supply chain resilience through sharing information effectively throughout the supply chain. This is particularly important when information leakage is the most serious hurdle in information sharing, where its inevitable effects are irreversibly detrimental. The findings of our study allow organisations to administer strategies for neutralizing this predicament by inculcating a strong information security culture in the workplace.

The contribution of this paper is two-fold. Firstly, this study contributes to theory by establishing the direct and indirect impacts of the constructs and by introducing a fresh framework. Secondly, from the practical perspective, this paper emphasises to companies seeking to build and sustain resilience that the interaction of information capabilities and risk will have an influence on supply chain resilience, which must be managed wisely.

This study is not without its limitations, however. The sample was restricted to MNCs and SMEs from various subsectors in the UK. Therefore, the results of the study may not be generalizable to other countries. Future studies may extend the research into other countries in Europe and Asia. Nevertheless, despite this limitation, the study offers valuable insight into the inter-relationships between information, leakage and resilience in the UK. Likewise, longitudinal studies may also be used in future as resilience is built not in an instant but a over a passage of time.

Acknowledgements The authors would like to thank the British Academy Newton-Ungku Omar Fund and Academy of Sciences Malaysia [Grant Number 304/PMGT/650912/B130] for supporting this research sproject.

References

Ahimbisibwe, A., Ssebulime, R., Tumuhairwe, R., & Tusiime, W. (2016). Supply chain visibility, supply chain velocity, supply chain alignment and humanitarian supply chain relief agility. *European Journal of Logistics, Purchasing and Supply Chain Management, 4*(2), 34–64.

Adewole, A. (2005). Developing a strategic framework for efficient and effective optimization of information in the supply chains of the UK clothing manufacture industry. *Supply Chain Management an International Journal, 10*(5), 357–366.

Alhogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology, 64*(2), 540–549.

Anand, K. S., & Goyal, M. (2009). Strategic information management under leakage in a supply chain. *Management Science, 55*(3), 438–452.

Amit, R., & Schoemaker, P. J. (1993). Strategic assets and organizational rent. *Strategic Management Journal, 14*(1), 33–46.

Autry, C., Goldsby, T., & Bell, J. (2013). *Global macrotrends and their impact on supply chain management: Strategies for gaining competitive advantage*. Upper Saddle River: Pearson Education.

Baihaqi, I., & Sohal, A. S. (2013). The impact of information sharing in supply chains on organisational performance: An empirical study. *Production Planning & Control, 24*(8–9), 743–758.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120.

Blackhurst, J., Dunn, K. S., & Craighead, C. W. (2011). An empirically derived framework of global supply resiliency. *Journal of Business Logistics, 32*(4), 374–391.

Bollen, K. A. (1990). Overall fit in covariance structure models: Two types of sample size effects. *Psychological Bulletin, 107*(2), 256–259.

Brandon-Jones, E., Squire, B., Autry, C. W., & Petersen, K. J. (2014). A contingent resource-based perspective of supply chain resilience and robustness. *Journal of Supply Chain Management, 50*(3), 55–73.

Byrne, B. M. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. Routledge.
Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research, 295*(2), 295–336.
Chen, Y., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11–19.
Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention and future directions. *Wires Data Mining and Knowledge Discovery, 7*, 1–14.
Choi, T.-M. (2020). Supply chain financing using blockchain: Impacts on supply chain selling fashionable products. *Annals of Operations Research*. https://doi.org/10.1007/s10479-020-03615-7
Day, J. M. (2014). Fostering emergent resilience: The complex adaptive supply network of disaster relief. *International Journal of Production Research, 52*(7), 1970–1988.
de Almeida, M. M. K., Marins, F. A. S., & Salgado, A. M. P. (2015). Mitigation of the bullwhip effect considering trust and collaboration in supply chain management: A literature review. *International Journal of Advanced Manufacturing Technology, 77*, 495–513.
Douglas, M. (2004). Trust me! The human side of collaboration. Inbound Logistics (Jan). Accessed 21 Jun 2020
Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Blome, C., & Luo, Z. (2017). Antecedents of resilient supply chains: An empirical study. *IEEE Transactions on Engineering Management, 66*, 8–19.
El-Sheikh, A. A., Abonazel, M. R., & Gamil, N. (2017). A review of software packages for structural equation modeling: A comparative study. *Applied Mathematics, 5*(3), 85–94.
Fan, Z.-P., Wu, X.-Y., & Cao, B.-B. (2020). Considering the traceability awareness of consumers: Should the supply chain adopt the blockchain technology? *Annals of Operations Research*. https://doi.org/10.1007/s10479-020-03729-y
Fawcett, S. E., Osterhaus, P., Magnan, G. M., Brau, J. C., & McCarter, M. W. (2007). Information sharing and supply chain performance: The role of connectivity and willingness. *Supply Chain Management: An International Journal, 12*(5), 358–368.
Feng, N., Chen, Y., Feng, H., Li, D., & Li, M. (2020). To outsource or not: The impact of information leakage risk on information security strategy. *Information & Management*. https://doi.org/10.1016/j.im.2019.103215
Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research, 13*(8), 382–388.
Govindan, K., Azevedo, S., Carvalho, H., & Cruz-Machado, V. (2015). Lean, green and resilient practices influence on supply chain performance: Interpretive structural modeling approach. *International Journal of Environmental Science and Technology, 12*(1), 15–34.
Guan, X., Liu, B., Chen, Y. J., & Wang, H. (2020). Inducing supply chain transparency through supplier encroachment. *Production and Operations Management, 29*(3), 725–749.
Hair, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: Updated guidelines on which method to use. *International Journal of Multivariate Data Analysis, 1*(2), 107–123.
Huong Tran, T. T., Childerhouse, P., & Deakins, E. (2016). Supply chain information sharing: Challenges and risk mitigation strategies. *Journal of Manufacturing Technology Management, 27*(8), 1102–1126.
Ivanov, D., Sokolov, B., & Dolgui, A. (2014). The ripple effect in supply chains: Trade-off 'efficiency-flexibility-resilience' in disruption management. *International Journal of Production Research, 52*(7), 2154–2172.
Ioannidis, C., Pym, D., William, J., & Gheyas, I. (2019). Resilience in information stewardship. *European Journal of Operational Research, 274*(2), 638–653.
Joe, F., Jr., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review, 26*(2), 106–121.
Jöreskog, K., & Sörbom, D. (1993). *LISREL 8: Structural equation modeling with the SIMPLIS command language*. Scientific Software International Inc.
Jüttner, U., & Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management: An International Journal, 16*(4), 246–259.
Kamalahmadi, M., & Parast, M. M. (2016). A review of the literature on the principles of enterprise and supply chain resilience: Major findings and directions for future research. *International Journal of Production Economics, 171*, 116–133.
Katsaliaki, K., Galetsi, P., & Kumar, S. (2020). Supply chain disruptions and resilience: A major review and future research agenda. *Annals of Operations Research*. https://doi.org/10.1007/s10479-020-03912-1
Kline, R. B. (2010). *Principles and practice of structural equation modeling* (3rd ed.). The Guilford Press.

Lee, H. L., & Whang, S. (2000). Information sharing in a supply chain. *International Journal of Manufacturing Technology and Management, 1*(1), 79–93.
Li, G., Zheng, H., Sethi, S. P., & Guan, X. (2020a). Inducing downstream information sharing via manufacturer information acquisition and retailer subsidy. *Decision Sciences, 51*(3), 691–719.
Li, G., Li, L., Choi, T. M., & Sethi, S. P. (2020b). Green supply chain management in Chinese firms: Innovative measures and the moderating role of quick response technology. *Journal of Operations Management, 66*(7–8), 958–988.
Li, S., & Lin, B. (2006). Accessing information sharing and information quality in supply chain management. *Decision Support Systems, 42*(3), 1641–1656.
Manatsa, P. R., & McLaren, T. S. (2008). Information sharing in a supply chain: Using agency theory to guide the design of incentives. *Supply Chain Forum: An International Journal, 9*(1), 18–26.
Mandal, S. (2012). An empirical investigation into supply chain resilience. *IUP Journal of Supply Chain Management, 9*(4), 46.
Mangus, S. M., Bock, D. E., Jones, E., & Folse, J. A. G. (2020). Examining the effects of mutual information sharing and relationship empathy: A social penetration theory perspective. *Journal of Business Research, 109*, 376–384.
MacDonald, J., Zobel, C., Melnyk, S., & Griffis, S. (2018). Supply chain risk and resilience: Theory building through structured experiments and simulation. *International Journal of Production Research, 56*(12), 4337–4355.
Mello, J. P. Jr. (2012). Hackers attack Foxconn for the laughs. Macworld (9 Feb). Accessed 2 Jul 2020.
Muller, G., Koslowski, T. (2012). Resilience: A useful Pardigm for IT-Social Infrastructures? Research Cooperation YRL Hitachi and University of Freiburg, Deliverable No.1, Freiburg.
Muller, G., Koslowski, T., & Accorsi, R. (2013). Resilience—A New Research Field In Business Information Systems?". In W. Abramowicz (Ed.), *Business information systems workshops, Lecture notes in business information processing* (Vol. 160, pp. 3–14). Springer.
Mupepi, M., Modak, A., Motwani, J., & Mupepi, S. C. (2017). How can knowledge leakage be stopped: A socio-technical system design approach to risk management. *International Journal of Sociotechnology and Knowledge Development, 9*(1), 26–41.
Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications, 44*, 12–22.
Newbert, S. L. (2007). Empirical research on the resource-based view of the firm: An assessment and suggestions for future research. *Strategic Management Journal, 28*(2), 121–146.
Nishat Faisal, M., Banwet, D. K., & Shankar, R. (2007). Information risks management in supply chains: An assessment and mitigation framework. *Journal of Enterprise Information Management, 20*(6), 677–699.
Pettit, T. J., Croxton, K. L., & Fiksel, J. (2019). The evolution of resilience in supply chain management: A retrospective on ensuring supply chain resilience. *Journal of Business Logistics, 40*(1), 56–65.
Ponte, B., Framinan, J. M., Cannella, S., & Dominguez, R. (2020). Quantifying the Bullwhip Effect in closed-loop supply chains: The interplay of information transparencies, returns and lead times. *International Journal of Production Economics*. https://doi.org/10.1016/j.ijpe.2020.107798
Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior Research Methods, 36*(4), 717–731.
Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods, 40*(3), 879–891.
Ritala, P., Olander, H., Michailova, S., & Husted, K. (2015). Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study. *Technovation, 35*, 22–31.
Scholten, K., Sharkey Scott, P., & Fynes, B. (2014). Mitigation processes–antecedents for building supply chain resilience. *Supply Chain Management: An International Journal, 19*(2), 211–228.
Scholten, K., & Schilder, S. (2015). The role of collaboration in supply chain resilience. *Supply Chain Management: An International Journal, 20*(4), 471–484.
Sener, A., Barut, M., Oztekin, A., Avcilar, M. Y., & Yildirim, M. B. (2019). The role of information usage in a retail supply chain: A causal data mining and analytical modeling approach. *Journal of Business Research, 99*, 87–104.
Sezen, B. (2008). Relative effects of design, integration and information sharing on supply chain performance. *Supply Chain Management: An International Journal, 13*(3), 233–240.
Shaw, D. R., Grainger, A., & Achutan, K. (2017). Multi-level port resilience planning in the UK: How can information sharing be made easier? *Technological Forecasting and Social Change, 121*, 126–138.
Shen, B., Choi, T., & Minner, S. (2019). A review on supply chain contracting with information considerations: Information updating and information asymmetry. *International Journal of Production Research, 57*(15–16), 4898–4936.

Singh, C. S., Soni, G., & Badhotiya, G. K. (2019). Performance indicators for supply chain resilience: Review and conceptual framework. *Journal of Industrial Engineering International, 15*, 105–117.
Soni, U., Jain, V., & Kumar, S. (2014). Measuring supply chain resilience using a deterministic modeling approach. *Computers & Industrial Engineering, 74*, 11–25.
Sodhi, M. S., & Tang, C. S. (2019). Research opportunities in supply chain transparency. *Production and Operations Management, 28*(12), 2946–2959.
Stevenson, M., & Busby, J. (2015). An exploratory analysis of counterfeiting strategies: Towards counterfeit-resilient supply chains. *International Journal of Operations & Production Management, 35*(1), 110–144.
Tabasso, N. (2019). Diffusion of multiple information: On information resilience and the power of segregation. *Games and Economic Behavior., 118*, 219–240.
Tseng, M. L., Tran, T. P. T., Wu, K. J., Bui, D. T., Tan, R. R. (2020). Exploring Sustainable seafood supply chain management in linguistic preferences: collaboration in supply chain and lean management drive economic benefit. International Journal of Logistics Research and Application (Article in Press)
Tukamuhabwa, B., Stevenson, M., Busby, J., & Zorzini, M. (2015). Supply chain resilience: Definition, review and theoretical foundations for further study. *International Journal of Production Research, 53*(18), 5592–5623.
Ulhaq, I., Kuruvilla, K. T., Nkhoma, M., Vu, H. H., & Tuyet, N. T. (2016). Information security risks in supply chain management: A review of literature for the developing country context. *International Journal of Information System and Engineering, 4*(2), 58–70.
Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture–perspectives from academia and industry. *Computers & Security, 92*, 101713.
Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162–176.
Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subculture. *Computers & Security, 70*, 72–94.
Wang, Y., & Zhang, S. H. (2020). Optimal production and inventory rationing policies with selective-information sharing and two demand classes. *European Journal of Operational Research*. https://doi.org/10.1016/j.ejor.2020.05.051
Wei, L., Zhang, J., & Zhu, G. (2020). Incentive of retailer information sharing on manufacturer volume flexibility choice. *Omega*. https://doi.org/10.1016/j.omega.2020.102210
Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal, 5*(2), 171–180.
Wieland, A., & Wallenburg, C. (2013). The influence of relational competencies on supply chain resilience: A relational view. *International Journal of Physical Distribution and Logistics Management, 43*(4), 300–320.
Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security, 88*, 101640.
Wong, C. W. Y., Lim, T.-C., Yang, C.-C., & Shang, K.-C. (2020). Supply chain and external conditions under which supply chain resilience pays: An organizational information processing theorization. *International Journal of Production Economics*. https://doi.org/10.1016/j.ijpe.2019.107610

Authors and Affiliations

Wai-Peng Wong[1] · Kim Hua Tan[2] · Kannan Govindan[3,4,5] · Di Li[6] · Ajay Kumar[7]

Wai-Peng Wong
wongwp@usm.my

Kim Hua Tan
kim.tan@nottingham.ac.uk

Kannan Govindan
kgov@iti.sdu.dk

Di Li
d.li@warwick.ac.uk

[1] School of Management, Universiti Sains Malaysia, 11800 USM Penang, Malaysia

[2] Department of Operations and Innovation Management, Nottingham University Business School, Nottingham, UK

[3] China Institute of FTZ Supply Chain, Shanghai Maritime University, Shanghai 201306, China

[4] Yonsei Frontier Lab, Yonsei University, Seoul, Korea

[5] Center for Sustainable Supply Chain Engineering, Department of Technology and Innovation, University of Southern Denmark, Campusvej 55, Odense M, Denmark

[6] WMG, University of Warwick, Coventry, UK

[7] AIM Research Center On Artificial Intelligence in Value Creation, EMLYON Business School, Écully, France