The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/0263-5577.htm

Interplay between cyber supply chain risk management practices and cyber security performance

Anisha Banu Dawood Gani
Faculty of Industrial Management, Universiti Malaysia Pahang, Gambang, Malaysia
Yudi Fernando
University Malaysia Pahang, Pekan, Malaysia
Shulin Lan
School of Economics and Management, University of the Chinese Academy of Sciences, Beijing, China
Ming K. Lim
University of Glasgow, Glasgow, UK and UKM-Graduate School of Business, Universiti Kebangsaan Malaysia, Bangi, Malaysia, and
Ming-Lang Tseng
Institute of Innovation and Circular Economy, Asia University, Taichung, Taiwan; Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan and UKM-Graduate School of Business, Universiti Kebangsaan Malaysia, Bangi, Malaysia

Received 19 May 2022
Revised 27 July 2022
21 September 2022
25 October 2022
Accepted 20 November 2022

Abstract

Purpose – This study aims to examine whether the cyber supply chain risk management (CSCRM) practices adopted by manufacturing firms contribute to achieving cyber supply chain (CSC) visibility. Studies have highlighted the necessity of having visibility across interconnected supply chains. Thus, this study examines the extent of CSCRM practices enabling CSC visibility to act as a mediator in achieving CSC performance.

Design/methodology/approach – A survey method was used to obtain data from the electrical and electronics manufacturing firms registered with the Federations of Malaysian Manufacturers directory. Data from 130 respondents were analysed using IBM SPSS and PLS-SEM.

Findings – This study empirically proves a dedicated governance team's integral role in setting the security tone within its CSC. The result also confirms the significant role that CSC visibility plays in achieving CSC performance. As theorised in the literature, there is also a strong direct relationship between CSC visibility and CSC performance, assuring manufacturing firms that investments and policies devised to improve CSC visibility are fruitful.

Originality/value – The significance of supply chain visibility in an integrated supply chain is recognised and studied using analytical models, behavioural techniques and case studies. Substantial empirical evidence on the CSCRM practices which contributes towards achieving supply chain visibility is still elusive. This study's major contribution lies in identifying CSCRM practices that can contribute towards achieving CSC visibility, and the mediating role CSC visibility plays in achieving CSC performance.

Keywords Cybersecurity, Supply chain visibility, Supply chain risk management, Cyber supply chain risk management

Paper type Research paper

The authors convey their appreciation to the Division of Research and Innovation, Universiti Malaysia Pahang (RDU1903126). This study is partially supported by NCTS 111-2221-E-468-008-MY3, Taiwan.

Industrial Management & Data Systems
© Emerald Publishing Limited
0263-5577
DOI 10.1108/IMDS-05-2022-0313

1. Introduction

Cybersecurity challenges are becoming a daily struggle for manufacturing firms, one of the most vulnerable industries to cyber-attacks. The advancement in automation and digitalisation technology, which the manufacturers are embracing to enhance and better monitor their operations, comes with a cyber threat landscape equally as sophisticated (Rehman *et al.*, 2021; Zhu *et al.*, 2022). The concept of cyber supply chain risk management (CSCRM) has emerged as a new management construct in the supply chain discipline. CSCRM advocates a cross-functional strategy to avoid and address disruptions resulting from the extensive interconnection of today's systems' operations (Colicchia *et al.*, 2018). All supply chain members become as strong as the weakest member because of shared information and security practices within an interconnected supply chain (Pandey *et al.*, 2020; Tseng *et al.*, 2021). Cyberattacks may originate in any network within the cyber supply chain (CSC) because of poor security controls. Therefore, a trait necessary for a CSC is visibility across its supply chain network. CSC visibility has been identified as a critical organisational competency for decision-making and attaining sustainable and competitive business performance (Kalaiarasan *et al.*, 2022). Visibility also improves supply chain coordination and information sharing among supply chain members (Fernando *et al.*, 2020, 2022). As CSCRM is concerned with the security and integrity of information transferred over a company's communication network, having visibility is critical to several facets of an efficient CSCRM.

Series of CSCRM practices have been proposed to increase visibility along the value chain. Gani and Fernando (2021) reported that mature CSCRM practices comprise several tiers, ranging from establishing a governance body, operations management and systems integration to assess the level of preparedness of the supply chain in defending itself from cyberattacks. On the other hand, Kalaiarasan *et al.* (2022) has identified visibility antecedents as consisting of people, process and technology sub-categories. Despite this, it was found that firms predominantly implement only technical security measures to strengthen internal firewalls rather than extending them to their supply chain (Colicchia *et al.*, 2018). The existing literature is also unclear on CSC visibility's attainment and exact role in a CSCRM context. This is because the literature on CSCRM practices and visibility is still limited (Saqib and Zhang, 2021). Furthermore, the lack of precise standards and practices that firms can leverage and the managerial capabilities to implement them limit firms' ability to manage cybersecurity challenges (Pandey *et al.*, 2020).

This study attempts to analyse the CSCRM practices and their role in achieving CSC visibility; and gives the importance of having visibility for an efficient CSCRM (Creazza *et al.*, 2021). Consequently, examine if CSC visibility mediates the relationship between CSCRM practices and CSC performance. Thus, the objectives of this study are as follows:

(1) To investigate the relationship between CSCRM practices and CSC visibility

(2) To examine the relationship between CSC visibility and CSC performance

(3) To investigate the role of CSC visibility as a mediator between CSCRM practices and CSC performance.

This study examines empirically and undertaken from a management perspective to fill the gap in the CSCRM literature (Pandey *et al.*, 2020). In the CSCRM context, this study argues that CSC visibility is critical for defending supply chain networks from cyberattacks and improving strategic performance in decision-making and competitiveness. Furthermore, it supports the company in sharing critical information and coordinating across multiple supply chain networks. However, the CSCs visibility is not well addressed, and the concept is not clearly justified in the literature. This study makes a significant contribution by proposing CSC visibility as an intervening domain to strengthen the theoretical model of

CSCRM practices. The model not only adds to the CSCRM literature but can also be used to improve current practices.

The remainder of this study is as follows: section 2 describes the relevant theoretical foundations which form the basis for the hypothesis's derivation. Section 3 then describes the methodology and the sample before presenting the respective empirical results in section 4. Section 5 discusses key findings, and finally, the study's limitations and future directions conclude the study.

2. Literature review

This section discusses literature reviews on the main variables and the theoretical foundation to justify the argument on hypothesis development.

2.1 Theoretical underpinning (contingency theory)

Contingency theory is a management theory that has its roots in organisational behaviour. It has gained popularity since it contradicts traditional management theory's assertion that there is just one ideal way to accomplish things (Csaszar and Ostler, 2020). Instead, contingency theory promotes the notion that there is no one-size-fits-all approach to doing things or managing firms. A task is carried out differently in firms based on environmental and contextual circumstances. Hence, contingency theory is used in this study in alignment with its proponents who argue that there is no single optimum strategy to protect a CSC; rather, a balanced review of its use and enforcement must consider a variety of environmental, organisational and individual considerations (Abedin, 2021). Such understanding is essential for building and maintaining a CSC's integrity and its stakeholders' trust.

Risks in CSC are based on uncertainty caused by environmental factors. Correspondingly, several risk management frameworks have been suggested, such as Gani and Fernando (2021) and Tse *et al.* (2018). Those frameworks give firms the foundation to collect data and analyse risk. Most significantly, firms can gather intellectual information and accurately analyse and assess the current situation to make the most appropriate decision contingent upon the firm's environment (Abedin, 2021). The contingency view has been applied in an integrated supply chain, illustrating that the relationship between integration and firm performance relies on several contingencies. This study argues that CSC performance is affected by contextual variables, allowing us to enrich our understanding of the circumstances under which a certain practice achieves CSC security. Hence, this study uses contingency theory as an underpinning theory to explain the nexus of the contextual variables and CSCRM practices.

2.2 CSC security performance

A compromised supply chain smears the operational and proprietary knowledge integrity of CSC. Firms can eliminate or reduce CSC vulnerabilities by implementing CSCRM. Although there are studies on supply chain security, not many have empirically examined the effect of supply chain security management on the firm's security performance. For example, a study by Cheung *et al.* (2021) analysed 103 articles on cybersecurity and found half to be conceptual in nature. For instance, Pandey *et al.* (2020) reported that firms largely rely on firewalls and encryption as a means of protection, which is proven inadequate given the various risk categories across inbound and outbound CSC. An effective CSCRM practice needs to incorporate people, process and technologies to effectively manage various risk types to achieve a CSC security performance (Creazza *et al.*, 2021; Fernando *et al.*, 2022). Firms with maturity in managing cybersecurity would have processes governing the confidentiality, integrity and availability of the information within the CSC. These can help firms achieve CSC security since their supply chain is more robust and resilient to breaches and attacks.

2.3 CSCRM

CSCRM is a strategy and effort to identify and map critical assets, evaluating and mitigating possible cyber and information risks (Creazza *et al.*, 2021). CSCRM's goal is to extend cyber risk control across the CSC network rather than just the focal firm, allowing for standard risk assessment and advocating for transparency across all supply chain participants (Colicchia *et al.*, 2018; Zhu *et al.*, 2022). Studies have attempted to dissect various aspects of CSCRM, such as risk management concepts (e.g. Gani and Fernando, 2018), visibility (e.g. Kalaiarasan *et al.*, 2022) and achieving supply chain resiliency (e.g. Malatji *et al.*, 2021). It has been argued that most have presented conceptual frameworks without empirical data (Cheung *et al.*, 2021). Moreover, previous studies primarily focused on the technical aspects of a single firm (Creazza *et al.*, 2021) rather than extended networks. Therefore, it is necessary to undertake CSCRM from the lens of a management perspective with a fusion of technical and organisational practices.

2.3.1 CSCRM practices. Gani and Fernando (2021) identified governance, system integration and operations to assess a firm's maturity in addressing cybersecurity concerns. The first tier stresses forming a governance team as a unified force to bring coordination and coherence to supply chain security choices. Cybersecurity governance cannot be achieved without an awareness of its importance and ramifications if it is not embraced by every supply chain member of the firm (Gani and Fernando, 2021). As a result, one of the top management's primary responsibilities is to establish a centralised governance body, which is then tasked with: (a) educating stakeholders on cybersecurity risks, (b) developing guidelines and processes to assess, audit and monitor the compliance of all internal and external stakeholders regularly and (c) keeping up with cybersecurity-related updates, trends and technologies and implementing regular patches to the supply chain network in an effort to protect the supply chain network (Gani and Fernando, 2018). However, this approach's success for CSCRM depends on the structural integration across the supply chain.

The second component is systems integration. It represents a set of interconnected systems and processes that facilitate effective decision-making. In an extremely interconnected global environment, the performance and adaptability of the firm are determined by its structure and configuration of the firm. The higher the degree of integration, the better the firm's performance (Tan *et al.*, 2022). This denotes stewardship of cyber or physical asset network maps and emphasises network asset visibility and real-time monitoring of processes.

The third tier is Operations, which is the execution and management of the processes that have been identified as the critical element for cybersecurity hygiene. Operational risks, such as a breakdown in manufacturing or processing capability or technological changes, impact a firm's ability to create goods and services and, thus, its profitability. Validation of IT system components, traceability of hardware certificates, software configuration management, supplier qualification and operational checks, sourcing strategy and protocol to deal with suspected breaches, attacks, or counterfeit parts are elements of this tier.

Other literature which has examined the CSCRM factors is summarised in Table 1. Among the factors that remain the highest enabler for the cybersecurity posture of a firm is top management, IT infrastructure, organisation tools, process and resource capabilities, which aligns with the findings from Gani and Fernando (2021). Therefore, this study recognises that governance, systems integration and operations represent a mature cybersecurity practice, enabling firms to increase visibility and achieve CSC security.

2.4 CSC visibility

Kalaiarasan *et al.* (2022) defined visibility as the degree of accurate and timely information that is available and accessible to the members of the supply chain network. Effective integration and

communication contribute positively towards achieving visibility, which improves supply chain performance. Several studies back this assumption, agreeing that supply chain visibility is obtained via information sharing and connectivity, enabling improvements in the resilience and robustness of the supply chain (e.g. Dubey *et al.*, 2020).

According to Barratt and Oke (2007), visibility mediates the relationship between CSCRM practice and CSC performance, and higher CSC visibility can improve CSC performance. Isolated literature has found that visibility positively influences overall supply chain performance; however, Kalaiarasan *et al.* (2022) concluded that very few contextual variables that affect CSC visibility are known. This is because the contingency factors for visibility are limited to three literature sources, thus calling for more studies to understand the context contributing to antecedents, barriers, challenges, drivers and effects of visibility. Therefore, this study proposes a theoretical framework that examines the relationship between CSCRM practices and CSC performance mediated by supply chain visibility, as shown in Figure 1.

2.5 Hypothesis development

Ghadge *et al.* (2019) argued that firms require elements of both IT and organisational tools to address and control the inherent CSC risks. According to Hong *et al.* (2018), ensuring visibility in the CSC network is paramount to resolving rapid changing and dynamic global supply chain problems. Therefore, Dubey *et al.* (2020) postulated that firms should implement practices that increase supply chain visibility through collaborations, systems integration and information sharing. Furthermore, many studies have argued that a firm's governance improves its performance as it favours actions that are in the best interests of all shareholders. Consequently, a direct influence on CSC practices and CSC visibility and, ultimately on risk management is expected (Rehman *et al.*, 2021). In this regard, Wijethilake and Lama (2019) have found that the extent of a practice being adopted as a culture by its stakeholders is driven by the governance team. Similarly, D'Arcy *et al.* (2020) found that governance is among the factors that could impact the likelihood of a firm experiencing a data breach as they can influence the level of practices to be adopted. Others have also reported that systems integration and centralised governance structures contribute positively to breach reductions. According to Dubey *et al.* (2020), the influence of CSCRM practices to

Author(s)	Cybersecurity factors	Maturity framework mapping
Kraemer *et al.* (2009)	Top management, organization culture	Governance
Hsu *et al.* (2012)	IT capability, top management support	Systems integration
Tang *et al.* (2016)	Organization skills	Operations
Nagurney *et al.* (2017)	Collaboration with competitor	
Angst *et al.* (2017)	IT investment	Top management
Pérez-Morón (2022)	Top management, relative advantage, technology, government policy and regulations	All: Governance, systems integration, operations

Table 1. Cybersecurity factors mapping against NIST maturity framework

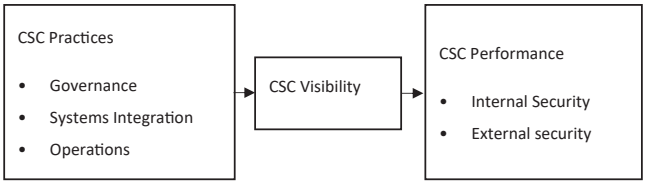

Figure 1. CSCRM theoretical framework

enhance CSC performance could be strengthened by creating visibility amongst members through collaboration using the firm's technological resources. Brun *et al.* (2020) have also found that to address supply chain complexity and achieve visibility, greater collaborations are needed. Supply chain partners use RFID and blockchains as operational tools to exchange information, increase transparency and collaborate on security issues. In addition, Somapa *et al.* (2018) assert that to promote operational effectiveness, information must be aligned with business processes for supply chain visibility to have its transformational effect. Based on the above discussion, the following hypotheses are proposed:

H1a. There is a positive and significant relationship between governance and CSC visibility.

H1b. There is a positive and significant relationship between systems integration and CSC visibility.

H1c. There is a positive and significant relationship between operations and CSC visibility.

Studies are in consensus that improved visibility decreases supply chain disruption and lessens the impact, resulting in increased robustness and resilience. Maghsoudi and Pazirandeh (2016) discovered that visibility had a major effect on resource sharing and business performance. Dubey *et al.* (2020) also found that supply chains' visibility influences stakeholder trust and contributes to firm performance. Findings from previous studies posit that visibility significantly benefits a firm's performance. As a result of gaining visibility, firms build stronger trust among their members, allowing them to be more flexible and responsive to environmental dynamics.

As securing CSC is critical to safeguard the integrity of products and the firm's reputation, firms must now discover ways to combine CSCRM principles to protect their supply chain, much like how environmental practices were incorporated for a sustainable supply chain (Swift *et al.*, 2019). Furthermore, considering the current cyber threat landscape of the manufacturing industry, firms must include CSCRM practices to secure their supply chain networks to assure their stakeholders on their data security and product quality (Afum *et al.*, 2020). From the above, it is evident that many studies agree that supply chain visibility influences the firm's performance. Therefore, the following hypotheses are proposed:

H2a. CSC visibility has a positive impact on CSC internal security.

H2b. CSC visibility has a positive impact on CSC external security.

Supply chain visibility is recognised as a critical strategy to improve operational performance. However, a major concern noted by studies in achieving desired supply chain performance is often attributed to a lack of supply chain visibility (e.g. Shibin *et al.*, 2017). Furthermore, previous studies have failed to delineate between supply chain practices and supply chain visibility (Barratt and Oke, 2007). Therefore, the interplay of supply chain practices in building supply chain visibility to achieve supply chain performance needs to be investigated. Since supply chain practices are identified as an immediate antecedent to achieving supply chain visibility that may impact supply chain performance, it is hypothesised that supply chain visibility mediates the relationship between CSCRM practices and CSC performance. Therefore, the following hypotheses are proposed:

H3a. CSC visibility mediates the relationship between governance and internal security.

H3b. CSC visibility mediates the relationship between systems integration and internal security.

H3c. CSC visibility mediates the relationship between operations and internal security.

H3d. CSC visibility mediates the relationship between governance and external security.

H3e. CSC visibility mediates the relationship between systems integration and external security.

H3f. CSC visibility mediates the relationship between operations and external security.

3. Methods

This study employed a quantitative approach, using an electronic survey with adapted measurement items from previous studies. The rationale for using an electronic survey was to gain access to a larger geographical area for the least amount of money and effort. The unit of analysis is Malaysia's electrical and electronics (E&E) manufacturing firms. The selection of E&E firm is attributed to it being the largest contributor to the manufacturing sector in Malaysia. It has been identified as one of the high-impact industries in the Twelfth Malaysia Plan, 2021–2025 (MSIA, 2022). The respondents of this survey hold senior management or executive role. They are assumed to have the authorisation in decision making and conversant in their business operations and possess the ability to represent their firm. Samples of the population were drawn from the automotive, electrical, electronics, ICT and semiconductor sub-sector of E&E manufacturing firms from the Federations of Malaysian Manufacturers (FMM) directory. As this study intends to review the CSCRM practices regardless of the firm's size, no control variable is used. In their study on green management, Younis and Sundarakani (2019) found that control variables do not affect operational performance. It is because firms of all sizes can benefit from supply chain management techniques. To examine improvements in their overall product quality and safety, potential respondent firms were selected via disproportionate stratified sampling after filtering for firms with ISO 9001 certification as preliminary proof of the firm's maturity and awareness of international standards. Stratified random sampling is a prominent approach used in supply chain management studies (Fernando *et al.*, 2021). ISO 9001 was selected because no substantial data on ISO 27001 certification was found in the FMM directory.

A survey questionnaire was developed by adapting instrument items from previous literature. Each item was measured on a five-point Likert scale with anchors ranging from strongly disagree (1) to strongly agree (5). An expert group of industry practitioners and academicians pre-tested and refined the instrument developed. A pilot test on the targeted respondents was carried out next to evaluate actual survey performance. To assess internal reliability and consistency of the instrument, Cronbach's alpha formula was used prior to qualifying the questionnaire administration to remainder of the population. The result of Cronbach's alpha from the pilot study met the requirement with all values being greater than 0.7, indicating that it was reliable and could be understood by the respondents.

As a result, 550 questionnaires were administered via Google form for a duration of 4 weeks. At the end of 4th week, 130 questionnaires were collected, which amounted to a 23.6% response rate. The response rate falls within the range of similar studies conducted in the Malaysian context (e.g. Fernando *et al.*, 2020; Fernando *et al.*, 2022), thus considered enough to represent the population of E&E manufacturing firms in Malaysia. This study's descriptive analysis was conducted using IBM SPSS software version 24. SmartPLS software version 3.3.3 was used to measure the model, which had skewed data as a result of skewness and kurtosis data validation. SmartPLS is endorsed by various writers, including Hair *et al.* (2019). We posit that PLS should be used when the analysis is concerned with evaluating a theoretical framework from a prediction viewpoint and when the sample size is limited due to a small population. The result from the analysis is covered next.

4. Results

4.1 Respondent and firm's profile

The respondents were predominantly from senior or middle management positions, with IT managers accounting for over 40% of the respondents, followed by supply chain managers (19%) and operations managers (17%). In addition, 85% of the respondents have specified that they possess professional cybersecurity certification. Thus, this survey obtained fair replies from the firm's top management, indicating that the manufacturing firm's input on security practices is adequately represented. All 130 respondents have confirmed adopting cyber security practices in their firm, with 21.5% having obtained ISO 27001 certification. Most of the respondent's firm has been operating between 10 and 15 years, making up over 57% of the total respondents. In addition, 42% of the firms were relatively new, with under ten years of operation, while only 5% were mature operators with over 20 years of existence. The remaining 9% were in operation between 16 and 20 years. Respondents were largely from firms dealing with industrial products (66.9%) and consumer products (33.1%), with 16.9% of the firms having more than 500 employees, followed by 251–500 employees (23.1%), 100 to 250 employees (33.8%) and less than 100 employees (26.3%). Most respondents were from fully-owned Malaysian firms (40.8%) or local and foreign joint-venture firms (36.2%).

Further, to strengthen the validity of the respondents regarding CSCRM practices, several questions have been included in the survey, as shown in Table 2. All respondents (100%) indicated that their firm had experienced some form of cyberattack. Spam was the most commonly experienced cyberattack with 40.8% of the respondent firm having experienced it, followed by phishing (30.8%), malware (20.8%) and hacking (7.7%). In addition, respondents indicated that the top four most worrying cybersecurity issues to their firm are trusting data to a third-party vendor (36.9%), subsequent mismanagement of cloud access (26.9%) and IoT sensor compromise (26.2%) received an almost equal vote and physical device tampering (10%). This result confirms that cybersecurity issues are a cause of concern to manufacturing firms with varying degrees of impact depending on the severity of the attack.

4.2 Measurement model

Before the overall model testing, we conducted the construct validity assessment for CSC Visibility measurement items using EFA (exploratory factor analysis) procedure. The visibility measurement items were adapted from the concept paper and not

Table 2.
Firm's profile

Demographic	Categories	Frequency	Percent
ISO/IEC 27001 Certification	No	102	78.5
	Yes	28	21.5
Type of Industry	Automotive	25	19.2
	Electrical/Electronics	47	36.2
	Information's and Technology	28	21.5
	Semiconductor	30	23.1
Experienced cyberattacks?	Yes	130	100
Type of cyberattack experienced	Hacking (DDOS, Key Logging, Cookie Theft)	10	7.7
	Malware	27	20.8
	Phishing	40	30.8
	Spam	53	40.8
Most worrying cybersecurity issues	IoT sensor compromise	34	26.2
	Mismanagement of cloud access	35	26.9
	Physical device tampering	13	10
	Trusting data to a third-party vendor	48	36.9

established yet. Four measurement items represent the CSC Visibility that has been analysed using principal component analysis (Table 3). Several conditions need to be fulfilled (Aminaimu and Fernando, 2021). First, we found that the Bartlett test of sphericity was significant ($\chi^2 = 0.819$, $p < 0.001$). We found that the adequacy sampling has exceeded 0.50 (*Kaiser-Meyer-Olkin* = 0.819). In the second condition, we examined the correlation matrix's anti-image. We found that all measurement items were acceptable (>0.50). In the third condition, we examine the eigenvalue assessment. We found 75.02% of total variance with a single factor eigenvalue greater than one. We conclude that CSC Visibility measurement items are valid and can be utilised for further structural model analysis (see Appendix).

To ensure that the model is valid and reliable, convergent validity, reliability and discriminant validity were first established. PLS-SEM's Loading, *CR* and *AVE* is used to measure the convergent validity. Figure 2 shows the results of the PLS-SEM study. According to Hair *et al.* (2016), the value for Loadings and *AVE* is > 0.5, while for *CR*, it should be > 0.7. As shown in Table 4, factor loading *CR* and *AVE* results were within the acceptable values. This implies that the individual indicators were reliable, and the reflective constructs

Items	Factor 1 (loadings)
VIS1	0.830
VIS2	0.892
VIS3	0.855
VIS4	0.886
KMO	0.819
Chi-Square	292.177***
Eigenvalue	3.001
Variance	75.026%

Note(s): ***$p < 0.001$; Extraction Method: principal component analysis

Table 3.
EFA results of CSC visibility

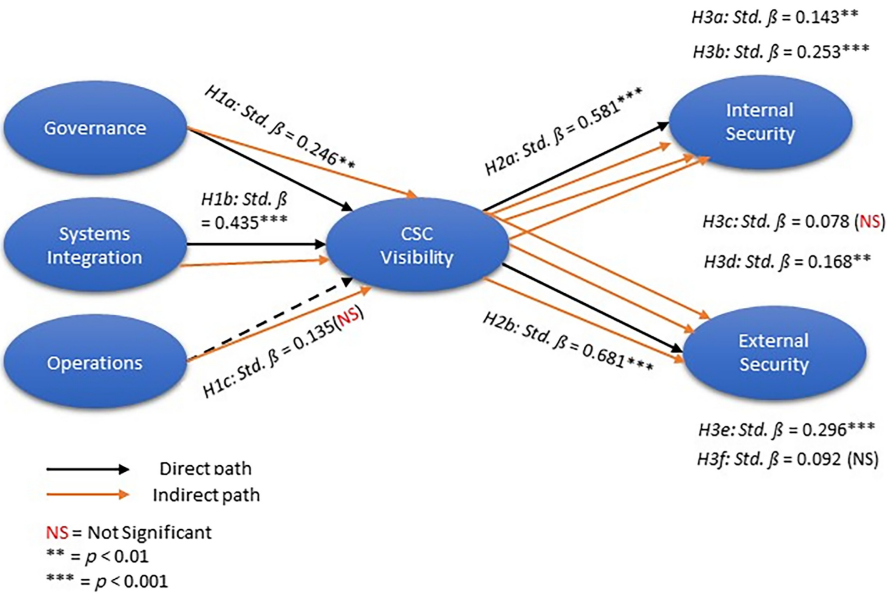

Figure 2.
The path analysis with SmartPLS

Construct	Item	Loadings	CR	AVE
Governance	GVN1	0.918	0.971	0.870
	GVN2	0.917		
	GVN3	0.959		
	GVN4	0.929		
	GVN5	0.940		
Operations	OPS1	0.831	0.875	0.585
	OPS2	0.796		
	OPS3	0.719		
	OPS4	0.759		
	OPS5	0.713		
Systems Integration	SI1	0.946	0.974	0.880
	SI2	0.955		
	SI3	0.953		
	SI4	0.964		
	SI5	0.870		
Visibility	VIS1	0.827	0.923	0.750
	VIS2	0.888		
	VIS3	0.849		
	VIS4	0.897		
Internal Security	I_SEC1	0.871	0.895	0.682
	I_SEC2	0.731		
	I_SEC3	0.853		
	I_SEC4	0.841		
External Security	X_SEC1	0.726	0.857	0.600
	X_SEC2	0.776		
	X_SEC3	0.796		
	X_SEC4	0.798		

Table 4.
Convergent validity

have a high level of convergent validity and internal consistency, respectively. Similarly, discriminant validity was evaluated to measure how one construct differs from another. Table 5 shows the heterotrait-monotrait ratio of correlations (*HTMT*) correlation matrix. The result shows that most of the *HTMT* values fall under the stringent range of 0.85 except for internal and external security. However, all the *HTMT* values are below 0.9, the most conservative acceptable value. This implies that each construct is unique and does not overlap in definition or understanding. Thus, our results have established discriminant validity between two reflective constructs.

4.3 Structural measurement

The structural model was evaluated using the coefficient of determination (R^2), predictive relevance (Q^2) and path coefficients of the independent variables from the model. The typical

	[1]	[2]	[3]	[4]	[5]	[6]
External security [1]						
Governance [2]	0.664					
Internal security [3]	0.88	0.507				
Operations [4]	0.479	0.518	0.314			
Systems integration [5]	0.637	0.733	0.516	0.668		
Visibility [6]	0.803	0.665	0.659	0.562	0.739	

Table 5.
Heterotrait-Monotrait ratio of correlations (HTMT)

way to evaluate the structural model's predictive power is the R^2 measure. Significant, moderate and weak R^2 values are defined as 0.75, 0.50 and 0.25, respectively (Hair *et al.*, 2016). The R^2 indicated that the present model's factor could explain 33.7% (internal security) and 46.4% (external security) of CSC performance variations. For Q^2, the value > 0 for internal security ($Q^2 = 0.221$), external security ($Q^2 = 0.262$) and visibility ($Q^2 = 0.379$) establish the fact that the PLS structural model has predictive relevance. A collinearity test is also performed to determine whether the data in this study is free of biases. Because the data was collected from a single respondent from each firm, this study used variance inflation factors (VIF) to test for common method bias. According to Hair *et al.* (2016), the acceptable VIF score is less than 5. As shown in Table 6, all variables were found to be free of common method bias with VIF scores less than 5.

PLS-SEM's Bootstrapping procedure is used to obtain t-statistics and p-value. The one-tail test is used to measure the direct effect of the hypothesis with a cut-off t-value of 1.645, while two tailed-test is used to measure the indirect effect or mediating hypothesis with a cut-off value of 1.965. The significance of path coefficients for direct effect is shown in Table 6. The result indicates that hypotheses H1a, H1b, H2a and H2b are all supported, but not H1c. The results for H1a showed a positive and significant linkage between governance and CSC visibility ($\beta = 0.246$; t-value = 2.835). H1b which examined the relationship between systems integration and CSC visibility is positive and statistically significant ($\beta = 0.435$; t-value = 3.642). However, H1c relationship between operations and CSC visibility is insignificant and therefore rejected. As for the relationship between CSC visibility and internal security (H2a) and visibility with external security (H2b), both were positive and statistically significant, with $\beta = 0.581$ and $\beta = 0.681$, respectively, with a t-value >1.645.

The result of the indirect effect is depicted in Table 7. H3a–H3f predicted a mediating effect of CSC visibility between CSCRM practices and CSC performance. From the result, hypotheses H3a, H3b, H3d and H3e were found to be positive and statistically significant with a t-value >1.965, thus were all accepted. However, H3c and H3f have a t-value <1.965 and thus were rejected. This shows that the inclusion of CSC visibility as a mediator in the relationship between CSCRM practice and CSC performance did not reveal complete acceptance. However, this result affirms the importance of having a governance structure beyond the IT team alone to drive the standards and policies to tighten CSC security and integrity. Similarly, systems integration among the supply chain partners enables achieving stronger CSC visibility across CSC.

5. Discussion

There are 11 hypotheses in this study. Five direct effect hypotheses address study objectives one and two, while six indirect hypotheses address study objectives three. The acceptance rate for direct effect is 80%, with one direct hypothesis (H1c) rejected, and the acceptance rate for indirect effect is 67%, with two hypotheses rejected (H3c and H3f). This data demonstrates that the conceptualisation of CSCRM practices to achieve CSC performance and the inclusion of CSC visibility as a mediating factor is proven.

Studies have reported that most attacks occur on the weakest link within supply chain members, drastically lowering security capability and visibility (Ghadge *et al.*, 2019). As a result, suppliers must improve visibility and develop a set of adaptable tools to mitigate risks. Better CSCRM practices are expected to enable a company to see risk exposure throughout the supply chain, including financial health and existing and emerging risks. Thus, hypothesis H1a to H1c examines the relationship between CSCRM practices and CSC visibility. From Table 6, only governance and systems integration are proven to impact achieving CSC visibility positively, but the operations relationship is rejected. The positive

Table 6.
Hypothesis result (direct)

Hypothesis	Path	Std. β	Std. Error	t-value	p-value	Decision	VIF	f^2	R^2	Q^2
H1a	Governance → CSC Visibility	0.246	0.246	2.835	0.005	Accept	2.020	0.064	0.527	0.379
H1b	Systems Integration → CSC Visibility	0.435	0.434	3.642	$p < 0.001$	Accept	2.544	0.157		
H1c	Operations → CSC Visibility	0.135	0.139	1.452	0.147	*Reject*	1.697	0.023		
H2a	CSC Visibility → Internal Security	0.581	0.586	11.145	$p < 0.001$	Accept	1.000	0.509		
H2b	CSC Visibility → External Security	0.681	0.688	12.449	$p < 0.001$	Accept	1.000	0.866	0.464	0.262

Hypothesis	Path	Std. β	Std. Error	t-value	p-value	Decision
H3a	Governance → CSC Visibility → Internal Security	0.143	0.145	2.615	0.009	Accept
H3b	Systems Integration → CSC Visibility → Internal Security	0.253	0.255	3.365	$p < 0.001$	Accept
H3c	Operations → CSC Visibility → Internal Security	0.078	0.081	1.461	0.145	*Reject*
H3d	Governance → CSC Visibility → External Security	0.168	0.17	2.665	0.008	Accept
H3e	Systems Integration → CSC Visibility → External Security	0.296	0.297	3.688	$p < 0.001$	Accept
H3f	Operations → CSC Visibility → External Security	0.092	0.097	1.374	0.170	*Reject*

Table 7. Hypothesis result (indirect)

relationship between governance and CSC visibility confirms the importance of governance as a foundation to set the tone of the cyber security culture in a manufacturing firm.

Similarly, firms can achieve greater CSC performance by having enhanced CSC visibility stemming from systems integration as reported by several studies (e.g. Fernando *et al.*, 2020; Fernando *et al.*, 2022). The ability to share information in real-time with supply chain partners is pivotal to obtaining information regarding any risk or vulnerability that can cause interruption to the supply chain. On the contrary, the relationship between operations and CSC visibility was found to be rejected. This unpredicted result could mean that many firms are still acting with little operational visibility, possibly being reactive rather than proactive in addressing operational improvements based on complaints or feedback from supply chain partners. Although surprising, there is a plausible reason that this contributed to the failure to address process bottlenecks. The concept of operation bottlenecks which was introduced by Cotteleer and Bendoly (2006), suggests that these bottlenecks hinder higher process performance due to physical or managerial constraints. Therefore, firms intending to improve CSC performance need to realise that only deploying tools or processes for application monitoring is inadequate to create CSC visibility. Instead, they must build processes and procedures to go beyond tracking inventories to obtaining actionable information and making it accessible to all stakeholders appropriately.

The result further proves that CSC visibility does contribute to achieving supply chain security. This finding is in line with past studies that have reported the importance of visibility in improving a firm's performance (Finkenstadt and Handfield, 2021). Similarly, the mediating effect of CSV between governance and systems integration is also proven to be statistically significant, implying the effort that firms make to enhance their CSC's visibility is proven to improve their CSC security and integrity. Similarly, H2b examined the mediating effect of CSC visibility between systems integration and CSC performance, and the result was found to be positive and significant as predicted. This proves that having an excellent technology infrastructure to back and integrate the dynamic CSC is the enabler for achieving visibility and attaining performance improvements; thus, it is inseparable for any CSC.

In contrast, the mediating effect of CSC visibility between operations and CSC performance was found insignificant. This negative relationship is possible if firm's operations are limited to its own and focal or first-tier suppliers but not second-tier or beyond. Studies like Hosseini and Ivanov (2019) have reported that the visibility of first-tier suppliers is more critical to a firm than second or third suppliers. The whole intent of requiring visibility can only be fully realised once the firm includes its suppliers within its supply chain's operations and makes them accountable for cyber security regardless of their tier.

5.1 Theoretical implications

This study contributes to the enrichment of the topic of CSC visibility in the CSCRM context. CSC visibility has been touted in the literature as an enabler for firms to respond to and recover from malicious intrusions. The performance impact of visibility is intensively studied in SCM. Despite that, CSC visibility relationship and effect on CSC performance have not been empirically tested; visibility is still mainly theoretical. Thus, by including CSC visibility as an enabler for CSC performance, this study has empirically proved the direct relationship of CSC visibility on performance which was proved to be positively significant. In addition, CSC visibility's role as a mediator between CSCRM practices and CSC performance was also proven via this study, which has not been examined previously. The type of CSCRM Practices affecting CSC visibility provides an important indicator on other practices that can influence CSC visibility besides having the information-sharing capability.

Next, this study offers a dual contribution to undertaking CSCRM study empirically and from a management perspective. Many studies have voiced the need for more empirical data in CSCRM and management, as the existing studies were conducted from a technical perspective instead. The present study has filled this void.

Finally, this study adds to the growing body of evidence supporting the use of the partial least square method structural equation model (PLS-SEM) as a reliable statistical tool for modelling multiple variables simultaneously. It includes a necessary goodness model analysis to assess construct validity and reliability before defining the path direction between latent variables involving mediation.

5.2 Practical implications

This study has proven that the way to achieve CSC performance is by having CSC visibility. Thus, practitioners should view their supply chain security technically and from a management perspective, with both tools and processes working in concert and with equal priority to help them achieve CSC visibility within their network. It is also imperative that the direction for pursuing CSC visibility as a priority come from the firm's governance team to implant a security culture vertically and horizontally within its supply chain, including suppliers beyond the first tier. Finally, firms must understand that CSCRM is a journey that involves multiple business processes and functions within and across the network; without ensuring they have visibility over their Tier 1 and Tier 2 suppliers, the firms would not have full visibility over their supply chain. Therefore, any safety and security program devised by the firm should facilitate information sharing, disruption alerts and coordinated responses among its supply chain partners.

6. Conclusion

This study examines how effective a manufacturing firm's CSCRM practices are in achieving CSC performance. The role of supply chain visibility as mediator between CSCRM practices and CSC performance was also investigated. This study has empirically proven that having a dedicated governance team comprising both technical and non-technical expertise personnel is crucial in defining the security tone inside a CSC within the E&E industry. Security incidents cannot be managed with the technical forefront alone. It requires an amalgam of people, processes and technology. The findings further highlight the importance of CSC visibility in achieving CSC performance. Manufacturing firms need to fully evaluate their network perimeter and prioritise integration efforts and governance of standards and policies that would improve their visibility among their supply chain partners, both internally and externally. Inherently, this implies assessing the cybersecurity maturity level of its supply chain partners, beyond first-tier suppliers, in their ability to protect integrated devices and

remote-access connections from being exploited. It is paramount that all CSC partners perceive cybersecurity as a priority and work in tandem to secure their respective networks from unwanted intrusions. This entails forming a dedicated governance team and creating integrated systems to improve network visibility to make the CSC more secure.

There are some limitations in this study that ought to be acknowledged. First, the population of this study is purely dependent on registered firms with an FMM directory which does not provide information on the security maturity level of every E&E manufacturer in Malaysia. Next, limited empirical evidence is presented in this study, which mainly aims to validate the proposed framework. A wider application of the model could offer an interesting outcome in CSCRM practices and provide a more extensive basis for benchmarking CSC visibility as a CSC performance enabler. Finally, this study was undertaken from the focal firm's perspective; future studies could approach CSCRM from the perspective of customers and suppliers, who could operate with different expectations and perceptions affected by the different rule of law environments.

References

Abedin, B. (2021), "Managing the tension between opposing effects of explainability of artificial intelligence: a contingency theory perspective", *Internet Research*, ahead-of-print (in press).

Afum, E., Agyabeng-Mensah, Y., Sun, Z., Frimpong, B., Kusi, L.Y. and Acquah, I.S.K. (2020), "Exploring the link between green manufacturing, operational competitiveness, firm reputation and sustainable performance dimensions: a mediated approach", *Journal of Manufacturing Technology Management*, Vol. 31 No. 7, pp. 1417-1438, doi: 10.1108/JMTM-02-2020-0036.

Aminaimu, Z. and Fernando, Y. (2021), "Psychometric instrument development of the sustainable balanced scorecard for the success of a new product development", *International Journal of Productivity and Quality Management*, Vol. 34 No. 1, pp. 33-63.

Angst, C.M., Block, E.S., D'arcy, J. and Kelley, K. (2017), "When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches", *MIS quarterly*, Vol. 41 No. 3, pp. 893-916, doi: 10.25300/MISQ/2017/41.3.10.

Barratt, M. and Oke, A. (2007), "Antecedents of supply chain visibility in retail supply chains: a resource-based theory perspective", *Journal of Operations Management*, Vol. 25, pp. 1217-1233.

Brun, A., Karaosman, H. and Barresi, T. (2020), "Supply chain collaboration for transparency", *Sustainability*, Vol. 12 No. 11, p. 4429.

Caridi, M., Crippa, L., Perego, A., Sianesi, A. and Tumino, A. (2010), "Do virtuality and complexity affect supply chain visibility?", *International Journal of Production Economics*, Vol. 127 No. 2, pp. 372-383.

Cheung, K.F., Bell, M.G. and Bhattacharjya, J. (2021), "Cybersecurity in logistics and supply chain management: an overview and future research directions", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 146, 102217.

Colicchia, C., Creazza, A. and Menachof, D.A. (2018), "Managing cyber and information risks in supply chains: insights from an exploratory analysis", *Supply Chain Management: An International Journal*, Vol. 24 No. 2, pp. 215-240.

Cotteleer, M.J. and Bendoly, E. (2006), "Order lead-time improvement following enterprise information technology implementation: an empirical study", *Management Information Systems Quarterly*, Vol. 30 No. 3, pp. 643-660.

Creazza, A., Colicchia, C., Spiezia, S. and Dallari, F. (2021), "Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era", *Supply Chain Management: An International Journal*, Vol. 27 No. 1, pp. 30-53.

Csaszar, F.A. and Ostler, J. (2020), "A contingency theory of representational complexity in organisations", *Organization Science*, Vol. 31 No. 5, pp. 1053-1312.

Dubey, R., Gunasekaran, A., Childe, S.J., Papadopoulos, T., Luo, Z. and Roubaud, D. (2020), "Upstream supply chain visibility and complexity effect on focal company's sustainable performance: Indian manufacturers' perspective", *Annals of Operations Research*, Vol. 290 No. 1, pp. 343-367.

D'Arcy, J., Adjerid, I., Angst, C.M. and Glavas, A. (2020), "Too good to be true: firm social performance and the risk of data breach", *Information Systems Research*, Vol. 31 No. 4, pp. 1200-1223.

Fernando, Y., Abideen, A.Z. and Shaharudin, M.S. (2020), "The nexus of information sharing, technology capability and inventory efficiency", *Journal of Global Operations and Strategic Sourcing*, Vol. 33 No. 4, pp. 327-351.

Fernando, Y., Tseng, M.L., Sroufe, R., Abideen, A.Z., Shaharudin, M.S. and Jose, R. (2021), "Eco-innovation impacts on recycled product performance and competitiveness: Malaysian automotive industry", *Sustainable Production and Consumption*, Vol. 28, pp. 1677-1686.

Fernando, Y., Tseng, M.L., Wahyuni-Td, I.S., Jabbour, A.B.L.D.S., Jabbour, C.J.C. and Foropon, C. (2022), "Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia", *Journal of Industrial and Production Engineering*. doi: 10.1080/21681015.2022.2116495 (in press).

Finkenstadt, D.J. and Handfield, R. (2021), "Blurry vision: supply chain visibility for personal protective equipment during COVID-19", *Journal of Purchasing and Supply Management*, Vol. 27 No. 3, 100689.

Gani, A.B.D. and Fernando, Y. (2018), "Concept and practices of cyber supply chain in manufacturing context", *Encyclopedia of Information Science and Technology*, 4th ed., pp. 5306-5316.

Gani, A.B.D. and Fernando, Y. (2021), "The cybersecurity governance in changing the security psychology and security posture: insights into e-procurement", *International Journal of Procurement Management*, Vol. 14 No. 3, pp. 308-327.

Ghadge, A., Weiß, M., Caldwell, N.D. and Wilding, R. (2019), "Managing cyber risk in supply chains: a review and research agenda", *Supply Chain Management: An International Journal*, Vol. 25 No. 2, pp. 233-240, doi: 10.1108/SCM-10-2018-0357.

Hair, J.F. Jr, Hult, G.T.M., Ringle, C. and Sarstedt, M. (2016), *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Sage Publications, Thousand Oaks, CA.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to use and how to report the results of PLS-SEM", *European Business Review*, Vol. 31 No. 1, pp. 2-24.

Hong, J., Zhang, Y. and Ding, M. (2018), "Sustainable supply chain management practices, supply chain dynamic capabilities, and enterprise performance", *Journal of Cleaner Production*, Vol. 172, pp. 3508-3519.

Hosseini, S. and Ivanov, D. (2019), "A new resilience measure for supply networks with the ripple effect considerations: a Bayesian network approach", *Annals of Operations Research*, pp. 1-27 (in press).

Hsu, C., Lee, J.-N. and Straub, D.W. (2012), "Institutional influences on information systems security innovations", *Information Systems Research: ISR*, Vol. 23 Nos (3-part-2), pp. 918-939.

Kalaiarasan, R., Olhager, J., Agrawal, T.K. and Wiktorsson, M. (2022), "The ABCDE of supply chain visibility: a systematic literature review and framework", *International Journal of Production Economics*, Vol. 248, 108464.

Kraemer, S., Carayon, P. and Clem, J. (2009), "Human and organisational factors in computer and information security: pathways to vulnerabilities", *Computers and Security*, Vol. 28 No. 7, pp. 509-520.

Maghsoudi and Pazirandeh (2016), "Visibility, resource sharing and performance in supply chain relationships: insights from humanitarian practitioners", *Supply Chain Management: An International Journal*, Vol. 21 No. 1, pp. 125-139.

Malatji, M., Marnewick, A.L. and Von Solms, S. (2021), "Cybersecurity capabilities for critical infrastructure resilience", *Information and Computer Security*, Vol. 30 No. 2, pp. 255-279.

MSIA (2022), "Media release - Malaysia's E&E industry celebrates 50th Anniversary", available at: https://msia.org.my/news_updates_details/H7YFCTGRWM

Nagurney, A., Daniele, P. and Sukla, S. (2017), "A supply chain network game theory of cybersecurity investments with nonlinear budget constraints", *Annuals of Operations Research*, Vol. 248 Nos 1-2, pp. 405-427.

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

Pérez-Morón, J. (2022), "Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda", *Journal of Asia Business Studies*, Vol. 16 No. 2, pp. 371-395.

Rehman, S.U., Kraus, S., Shah, S.A., Khanin, D. and Mahto, R.V. (2021), "Analysing the relationship between green innovation and environmental performance in large manufacturing firms", *Technological Forecasting and Social Change*, Vol. 163, 120481.

Saqib, Z.A. and Zhang, Q. (2021), "Impact of sustainable practices on sustainable performance: the moderating role of supply chain visibility", *Journal of Manufacturing Technology Management*, Vol. 32 No. 7, pp. 1421-1443.

Shibin, K.T., Gunasekaran, A. and Dubey, R. (2017), "Explaining sustainable supply chain performance using a total interpretive structural modeling approach", *Sustainable Production and Consumption*, Vol. 12, pp. 104-118.

Sindhuja, P.N. (2014), "Impact of information security initiatives on supply chain performance", *Information and Computer Security*, Vol. 22 No. 5, p. 450.

Somapa, S., Cools, M. and Dullaert, W. (2018), "Characterizing supply chain visibility – a literature review", *The International Journal of Logistics Management*, Vol. 29 No. 1, pp. 308-339, doi: 10.1108/IJLM-06-2016-0150.

Swift, C., Guide, V.D.R. Jr and Muthulingam, S. (2019), "Does supply chain visibility affect operating performance? Evidence from conflict minerals disclosures", *Journal of Operations Management*, Vol. 65 No. 5, pp. 406-429.

Tan, C.L., Tei, Z., Yeo, S.F., Lai, K.H., Kumar, A. and Chung, L. (2022), "Nexus among blockchain visibility, supply chain integration and supply chain performance in the digital transformation era", *Industrial Management and Data Systems* (in press).

Tang, M., Li, M.G. and Zhang, T. (2016), "The impacts of organisational culture on information security culture: a case study", *Information Technology and Management*, Vol. 17 No. 2, pp. 179-186.

Tse, Y.K., Chung, S.H. and Pawar, K.S. (2018), "Risk perception and decision making in the supply chain: theory and practice", *Industrial Management and Data Systems*, Vol. 118 No. 7, pp. 1322-1326.

Tseng, M.L., Tran, T.P.T., Ha, H.M., Bui, T.D. and Lim, M.K. (2021), "Sustainable industrial and operation engineering trends and challenges toward Industry 4.0: a data driven analysis", *Journal of Industrial and Production Engineering*, Vol. 38 No. 8, pp. 581-598.

Wijethilake, C. and Lama, T. (2019), "Sustainability core values and sustainability risk management: moderating effects of top management commitment and stakeholder pressure", *Business Strategy and the Environment*, Vol. 28 No. 1, pp. 143-154.

Younis, H. and Sundarakani, B. (2019), "The impact of firm size, firm age and environmental management certification on the relationship between green supply chain practices and corporate performance", *Benchmarking: An International Journal*, Vol. 27 No. 1, pp. 319-346.

Zhu, C., Guo, X. and Zou, S. (2022), "Impact of information and communications technology alignment on supply chain performance in the Industry 4.0 era: mediation effect of supply chain integration", *Journal of Industrial and Production Engineering*. doi: 10.1080/21681015.2022.2099472 (in press).

Further reading

Dash, G. and Paul, J. (2021), "CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting", *Technological Forecasting and Social Change*, Vol. 173, 121092.

Appendix

Variable		Adapted from
Governance		
GVN1	My firm has a cross-functional team that specialises in managing cybersecurity issues	Gani and Fernando (2021)
GVN2	My firm has regular sharing of cybersecurity plans with the stakeholders	
GVN3	My firm follows government or industry-initiated cybersecurity guidelines (e.g. ISO/IEC 27000)	
GVN4	My firm verifies that supply chain partners follow government or industry security guidelines	
GVN5	The operation of the overall cyber supply security structure is evaluated and adjusted to adapt to changing conditions	
Systems Integration		
SI1	My firm's security plan is coordinated with major suppliers	Gani and Fernando (2021)
SI2	My firm's security plan is coordinated with outside groups (i.e. government and suppliers)	
SI3	My firm and the supplier have jointly implemented a document retention policy on cyber supply chain risk	
SI4	My firm's suppliers provide frequent status updates on current or emerging cyber supply chain risks	
SI5	My firm's information systems provide our supply chain partners with the timely information they need to respond to contamination/security incidents	
Operations		
OPS1	My firm has processes to prevent security issues in our supply chain	Gani and Fernando (2021)
OPS2	My firm has processes to detect security issues in our supply chain	
OPS3	My firm has processes to respond to security issues in our supply chain	
OPS4	My firm uses security audits to determine whether supplier relationships should be maintained	
OPS5	My firm audits the security procedures of contract manufacturers	
Supply Chain Visibility		
VIS1	My firm has visibility on vulnerabilities originating from its supply chain partners	Caridi *et al.* (2010)
VIS2	My firm has visibility on possible intrusions before the cyber supply chain is compromised	
VIS3	My firm has visibility on the intrusion immediately after the cyber supply chain is compromised	
VIS4	My firm performs periodic vital checks to ensure the cyber supply chain runs correctly	

Table A1.
Measurement items

(*continued*)

Variable		Adapted from
External Security		
X_SEC1	My firm's supply chain partners have enforced proper physical controls (protecting physical facilities, data storage centres and premises from unauthorised entry, environmental dangers, etc.)	Sindhuja (2014)
X_SEC2	My firm's supply chain partners have enforced access controls (password mechanisms, data, backup and network security, anti-virus solutions, etc.) to protect its information assets from unauthorised access, use, disclosure, modification, or destruction	
X_SEC3	My firm has well-documented policies and procedures for ensuring a secure flow of information with our supply chain partners	
X_SEC4	My firm and supply chain partners keep each other informed of the events that may affect the other party	
Internal Security		
I_SEC1	My firm has proper access controls (password mechanisms, data, backup and network security, anti-virus solutions, etc.) to protect its information assets from unauthorised access, use, disclosure, disruption, modification, or destruction	Sindhuja (2014)
I_SEC2	My firm has proper physical controls (protecting physical facilities, data storage centres and premises from unauthorised entry, environmental dangers, etc.)	
I_SEC3	My firm maintains a good cultural information security climate (attitudes, beliefs, norms, assumptions, awareness, training programs, etc.)	
I_SEC4	My firm has consistently enforced information security policies and procedures (policy statements, policy enforcement, personnel security, etc.)	

Table A1.

Corresponding author
Ming-Lang Tseng can be contacted at: tsengminglang@gmail.com, tsengminglang@asia.edu.tw

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**