TELAAH BISNIS

Volume 25, Issue 1, 15-25
http://journal.stimykpn.ac.id/index.php/tb

ISSN 1411-6375 (Print)
ISSN 2541-6790 (Electronic)

The Influence of Governance on Cyber Supply Chain Performance with Mediating Effect from Cyber Supply Chain Visibility

Wong Norissa Leticia Atmajaya[1]✉, **Yonathan Palumian**[2]
Petra Christian University, Indonesia[1,2]

Correspondence
norissa.atmajaya@gmail.com

Received Jan 16, 2024
Revised Aug 1, 2024
Accepted Aug 5, 2024
Published Aug 6, 2024

DOI 10.35917/tb.v25i1.466

Abstract
This research aims to analyze the influence of governance on Cyber Supply Chain (CSC) Performance, which is mediated by Cyber Supply Chain (CSC) Visibility to achieve effective and efficient cyber supply chain risk management (CSCRM) practices for the supply chain management (SCM) process. The population of this research is all manufacturing companies on the island of Java, Indonesia, that have used computerized systems in their supply chain processes with qualifications or certifications ISO 27001, ISO 28000, ISO 28001, or other certifications that are management information system standards. This research will reveal the strengths or weaknesses of the mediating role of CSC Visibility on CSC Performance in manufacturing companies. This study also found empirical evidence that having a dedicated governance team consisting of technical and non-technical personnel is important in CSCRM in the manufacturing industry, especially Java Island in Indonesia.
Keywords: SCM, CSCRM, CSC Performance, CSC Visibility, Governance

Introduction

Utilization of concepts Supply Chain Management (SCM) with a combination of Industry 4.0 by a company can make more optimal use of opportunities and prevent risks that can impact results performance (Erboz et al., 2021; Hong et al., 2018; Serkan et al., 2022). SCM that utilizes Industry 4.0 makes more optimal use of opportunities, and risk prevention can occur due to the benefits of establishing an Industry 4.0 system that can improve the quality and efficiency of business processes using technology (Serkan et al., 2022). There are changes in the supply chain process after the Coronavirus disease (COVID-19) pandemic, creating a business process in which the company monitors supply chain processes remotely, which can be carried out flexibly by the company with the condition that there is a systematized supply chain system. This was created because of the COVID-19 pandemic that occurred throughout the world, which required all people to stay at home and not do activities outside the home (Chong & Duan, 2022).

Changes in the business world that are changing rapidly and being adapted to environmental conditions have resulted in supply chain services becoming more efficient in bridging between producers and distributors as well as physical stores and consumers. However, with all the benefits of combining SCM and Industry 4.0, which are closely related to information technology, there is a risk of losing data or being infiltrated by irresponsible individuals (Ahmadi et al., 2021; Ghadge et al., 2019; Serkan et al., 2022).

Table 1. Number of cyber-attack cases in Indonesia 2019-2022

Year	Number of Cases
2019	220 million
2020	495 million
2021	1.6 billion
2022	976 million

Source: Katadata Insight Center, PwC Indonesia (2023)

From Table 1, it can be seen that the number of cyber-attack cases that occurred in Indonesia reached 976 million in 2022. This number decreased significantly from the cases in 2021, which reached 1.6 billion cases of cyber-attacks in Indonesia. Because of this problem in SCM, a solution emerged, which is called Supply Chain Risk Management (CSCRM). CSCRM is a company management strategy that focuses on assessing and preventing attack risks in the whole process supply chain, which combines processes, human resources, and technology into an integrated system between actors in the supply chain concerned (Creazza et al., 2021).

Good SCM distribution requires a good supply chain governance system with good visibility so stakeholders, such as producers, supply chain partners, and consumers, can easily track it. The previous statement is supported by previous research by Gani et al. (2022), with a good level of visibility in accessing the supply chain process will influence the performance of cyber security levels, which are increasingly coordinated and can reduce the impact of hacking losses by irresponsible individuals or hackers and can improve performance in decision making and competitive advantage of a company. Company. Improved performance in this company can be assessed from a company's internal and external security management system, such as implementing preventive measures and handling if a cyber-attack occurs (Gani et al., 2022).

This research aims to analyze the influence of governance mediated by Cyber Supply Chain (CSC) Visibility with Cyber Supply Chain (CSC) Performance in effective and efficient CSCRM practices for the SCM process especially if the firms have good governance. This research will reveal the strength or weakness of the influence of CSC Visibility on CSC Performance in manufacturing companies that focus on manufacturing companies on Java in Indonesia through management practices by the executive manager, the one decision maker of implementation in the business world. This research on CSCRM argues that CSC Visibility influences CSC Performance. This study was researched to fill the research gap empirically in the research of Pandey et al. (2020), which does not directly show the influence of CSC Visibility on CSC Performance that affect of CSC Visibility on CSC Performance especially in Java Island. Specifically, it examines how having a structured, efficient, and effective Internal Supply Chain Management (ISCM) within the broader Supply Chain Management (SCM) framework can mitigate the impacts of cyber-attacks or operational disruptions. By establishing comprehensive and detailed Standard Operating Procedures (SOPs) and structured guidelines, the study seeks to provide a clear roadmap for companies to navigate and resolve operational challenges effectively.

Literature Review and Hypotheses

Implementing Cyber Supply Chain Risk Management (CSCRM) in today's business conditions, which are all digital and vulnerable to cyber-attacks, is crucial, especially if it is a large-scale manufacturing company (Pandey et al., 2020). CSCRM practices are a strategy and initiative that focuses on assessing and preventing the risk of cyber-attacks in the whole process supply chain, which combines processes, human resources, and technology into an integrated system between the actors in the supply chain concerned (Creazza et al., 2021). The previous

research by Pandey et al. (2020) stated that CSCRM can be a risk assessment of all company management processes related to Supply Chain (SC) processes in the field of Information Systems (IT) contained in networks, software, and so on. Therefore, efficient CSCRM is closely related to security in the governance of a system in the distribution of information channeled through communication networks, so supporting the smooth and secure distribution of information is necessary (Gani et al., 2022).

CSCRM is powered by good governance that can create various positive impacts which have excellent benefits for achievement Cyber Supply Chain (CSC) Performance has not only increased in a short period but has become a habit and culture of the company (Creazza et al., 2021; Gani et al., 2022). The proactive CSCRM is apart from a good supply chain governance system with good visibility for stakeholders, such as producers, supply chain partners, and consumers. This can create a good SCM distribution, as claimed by the previous research by Gani et al. (2022), that better visibility in accessing the supply chain process will influence the performance of cyber security levels, which are increasingly coordinated and can reduce the impact of hacking losses by irresponsible individuals or hackers and improve performance in decision-making and the competitive advantage of a firm.

Governance is defined as a company management arrangement for the proper decision-making process by adjusting the company's processes, methods, policies, and structures to coordinate with individuals, operational processes, and technology used to optimize business processes (Ahmadi et al., 2021). According to previous research by Gani et al. (2022), governance means managing in harmony and unison with all company members related to supply chain management decision-making. According to Maleh et al. (2021), governance means the excellent management of organizational information assets. These assets can be information data in the form of considerations for managing business operational risks, business data, and costs in business operations. Based on several meanings explained, governance is company management used to make decisions in business processes so that they can run effectively and efficiently in terms of costs and time.

Cyber Supply Chain (CSC) Visibility means the openness of a company's business processes regarding visual access to demand and supply information in real-time and accuracy, which is useful for company operations (Kalaiarasan et al., 2022). According to Baah et al. (2021), CSC Visibility means openness to information considered accurate, reliable, timely, and useful in supply chain or company operational activities. Apart from this, CSC Visibility is understood as openness in accessing relevant information elements at the level chosen by the party stakeholder supply chain (Somapa et al., 2018). Based on several definitions of CSC Visibility that are described, CSC Visibility is open access to accurate and consistent company information in real-time to help the stakeholder supply chain in business processes. Therefore, good CSC Visibility can give the company flexibility in the management supply chain because it can be easily accessed by the perpetrator's supply chain, which can increase effectiveness in operations, which has a vital role in improving supply chain performance (Kalaiarasan et al., 2022). This statement is also supported by previous research by Somapa et al. (2018), that companies that have CSC Visibility This can be seen from the capture of detailed information regarding delivery flows and stock status in several locations as well as warnings regarding essential events during the logistics journey, which includes production and delivery planning at the factory, to storage and movement by expedition companies, inspections and permits by customs authority, until land transportation to the final destination reaches the consumer. Previous research also found that having an effective company integration system and good visibility in the supply chain will improve supply chain performance (Gani et al., 2022).

Cyber Supply Chain (CSC) Performance has a sense of status output company performance using technology that can increase the efficiency and effectiveness of the entire management chain supply chain (P. N., 2021). According to Gawankar et al. (2019), CSC

Performance is a status or output value from the workings of a company's information system by evaluating the efficiency of company strategy, better company tactics, and effective operational decisions. Not only measuring efficiency and effectiveness but also combining human resources, processes, and technology to manage cyber risk effectively and help the company achieve a more robust supply chain and more resistance to cyber-attacks. Therefore, according to P. N. (2021) citing Beamon (1999), three things indicate that the company's performance is running well: management flexibility, supply chain, measurement of resources derived from suppliers, and agility in responsiveness of supply chain as output. Based on several previous statements, it can be concluded that CSC Performance is the value of the status or condition of the company with the use of information systems and technology to increase the efficiency and effectiveness of the company's operational activities. In previous research, CSC Performance Also has several measurements: internal flexibility supply chain, resource performance measurement supplier, and responsiveness supply chain output. Therefore, it is divided into two sectors in assessing this variable, namely through internal parties and external parties (Gani et al., 2022).

According to Maleh et al. (2021), who quoted from Lunardi et al. (2014), there is a statement that good ones can improve performance with governance. The increase will lead to better supply chain and financial performance. Meanwhile, research by Gani et al. (2022) stated that good governance can increase CSC Performance because it is one of the supporting factors in deciding on the best action for the interests of all shareholders. Therefore, good governance can impact the overall CSC Performance, which can be more efficient, and effective.

H1: *Governance influences CSC Performance.*

Gani et al. (2022), who quotes from Hong et al. (2018), explain that the existence of CSC Visibility in the network supply chain plays a crucial role in solving global problems in the supply chain, which is very dynamic and rapidly changing. Therefore, according to Dubey et al. (2017), companies must implement practices that increase the visibility of the supply chain through governance and information systems. In previous research, he also argued that corporate governance improves performance because it supports actions that are in the best interests of all shareholders (Wijethilake & Lama, 2018). Therefore, governance influences CSCVisibility.

H2: *Governance influences CSC Visibility.*

In previous research, with transparency, communication was accessible for the perpetrator's supply chain, which can increase effectiveness in operations, which plays a vital role in improving supply chain performance (Kalaiarasan et al., 2022). According to the assumptions of Gani et al. (2022), CSC Visibility is critical in improving CSC Performance, because this process obtained through information sharing and connectivity allows for increased resilience and a resilient supply chain. Thus, this will have a direct or indirect impact on CSC Performance. Therefore, CSC Visibility influences CSC Performance.

H3: *CSC Visibility influences CSC Performance.*

Arrangement Governance, which is suitable for the supply chain, will increase the efficiency of business operations, which will then positively impact CSC Performance. This statement is strengthened by previous research by Gani et al. (2022), the importance of governance in the CSC relationship performance and CSC Visibility, which forms the basis of practice Cyber Supply Chain Risk Management (CSCRM) in efforts to prevent and minimize the impact and preventive measures of attacks cyber in the whole process supply chain (Creazza et al., 2021). Thus, it can be concluded that CSC Visibility mediates governance influence on CSC Performance.

H4: *Governance has an influence on CSC Performance through CSC Visibility.*

Research Method

This research uses a type of quantitative research that is explanatory causal in nature to look at the characteristics of the experiment, namely the search for cause-and-effect relationships between variables in the research (Sekaran & Bougie, 2016, p.44). The population of this research is all manufacturing companies on the island of Java in Indonesia that have used computerized systems in their supply chain processes with ISO 27001, ISO 28000, and ISO 28001 qualification or certification as an international standard for information system security management or other certifications that are standards for management information systems. The sampling technique in this research is non-probability sampling with a purposive sampling category, judgment sampling. This sampling process involves selecting subjects most advantageously placed or in the best position to provide the required information (Sekaran & Bougie, 2016, p.248). Respondents in this research were managers who held senior or executive management roles because it is assumed that they have authority in decision-making, are fluent in business operations, and can represent the firm.

The list of manufacturing companies collected for this research is obtained from certification bodies and manufacturing associations in Indonesia, such as the National Certification Body, TÜV Rheinland Indonesia, SGS Indonesia, Bureau Veritas Indonesia, Sucofindo, Indonesian Automotive Component Manufacturing Association, Indonesian Electronic Equipment Manufacturers Association, and the Association of Manufacturers and Indonesian Industry.

Table 2. Firm's Profile

Criteria		Frequency	Percentage
Having Management Information Systems Certification	No	115	48.7%
	Yes	121	51.3%
Types of ISO Certification	ISO 27001	103	85.1%
	ISO 28000	14	11.6%
	ISO 28001	4	3.3%
Type of manufacturing industry	FMCG	10	8.3%
	Food and Bevarages	13	10.7%
	Semiconductor	4	3.3%
	Information and Technology	27	22.3%
	Electronics/ Electrical	37	30.6%
	Automotive	30	24.8%
Experienced cyberattacks?	Yes	121	100%
	No	0	0%

Source: Results of Data Processing (2023)

The distribution of this research questionnaire is carried out online via email, telephone, and WhatsApp. The questionnaire survey was developed from indicator items based on several

previous studies with a Lickert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The questionnaires were distributed for six weeks, and 567 surveys were distributed via email, WhatsApp, and telephone. From the distribution of questionnaires, 236 surveys were collected. However, only 121 respondents met the criteria and were considered valid in this research. After the data is collected, it is processed using SmartPLS version 4.0 to analyze it further.

Respondents who participated in this research as firm representatives predominantly came from senior managers or middle management who played a role in decision-making in SCM business processes. Based on a survey collected from 121 respondents, 97 respondents acted as operations managers, with a percentage of 76.9%. In comparison, for IT managers, there were 25 respondents with a percentage of 20.7%, and the last was supply chain managers, with 3 respondents with a percentage of 2.5%. Survey data collected to test its validity in implementing CSCRM is explained with several questions in Table 2. According to data from Table 2 from 121 respondents, all those implementing the ISO 27001, ISO 28000, and ISO 28000 certification systems have experienced cyber-attacks. Based on Table 2, the ISO type that is most widely owned is ISO 27001, with 103 respondents, which has a percentage of 85.1% and is dominated by companies operating in the electronics/electrical industry. Table 2 also shows that companies with ISO 27001, ISO 28000, and ISO 28001 have experienced cyber-attacks.

Results and Discussion

The measurement model has two model tests: the inner and outer models. These models are useful for testing each existing indicator to assess the validity and reliability of the construct. Then, evaluate the inner model using the t-statistics test to determine the correlation between research constructs.

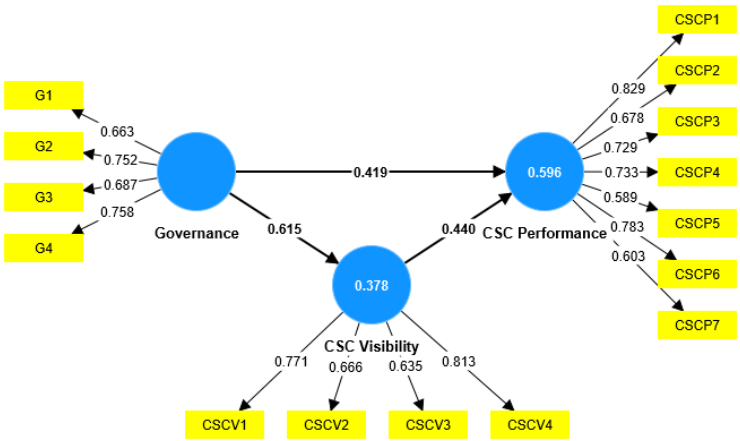

Figure 1. Research's Framework and Path Analysis Test Result
Source: Results of Data Processing (2023)

The measurement of variables that can be considered reliable and valid can be measured from the outer model if an outer model is needed that has a Loading Factor value of more than 0.50 and a Factor Loading higher than the Cross Loading Value (Hair et al., 2019). From Table 3 and Figure 1, all indicators have a factor loading value of more than 0.50 and have a cross-loading value for each indicator, which is higher than the other values. Therefore, this data shows that each indicator that measures the variables in the research is considered valid and reliable.

Table 3. Indicator's Discriminant Validity Test

Indicators	CSC Performance	CSC Visibility	Governance
G1	0.447	0.362	0.663
G2	0.577	0.567	0.752
G3	0.489	0.410	0.687
G4	0.434	0.378	0.758
CSCV1	0.514	0.771	0.363
CSCV2	0.474	0.666	0.488
CSCV3	0.378	0.635	0.253
CSCV4	0.611	0.813	0.592
CSCP1	0.829	0.613	0.560
CSCP2	0.678	0.523	0.418
CSCP3	0.729	0.440	0.521
CSCP4	0.733	0.549	0.450
CSCP5	0.589	0.419	0.518
CSCP6	0.783	0.551	0.474
CSCP7	0.603	0.331	0.490

Source: Results of Data Processing (2023)

Table 4 Reliability, R^2, Q^2 Test Result

Variables	Cronbach'sAlpha	Composite Reliability	AVE	R^2	Q^2
Governance	0.685	0.808	0.513	-	-
CSC Visibility	0.703	0.814	0.525	0.378	0.178
CSC Performance	0.833	0.876	0.505	0.596	0.279

Source: Results of Data Processing (2023)

Apart from measurements using factor loading, other measurements also measure that the indicators used can measure variables consistently. Table 4 shows each construct's reliability test in three measurements: Cronbach's Alpha, Composite Reliability, and Average Variance Extracted (AVE). According to data processed with SmartPLS 4.0, the blocks of indicators are considered reliable when the composite reliability value is > 0.70 and AVE > 0.50 (Hair et al., 2014, p.106-121). The Cronbach's Alpha value is deemed reliable and valid in measuring the blocks of indicators if it has a value of 0.60 to 0.80 (Hajjar, 2018). Table 4 shows that the lowest Cronbach's Alpha value is 0.685, which is related to governance, and the lowest composite reliability value is 0.808, which is also related to governance, with an AVE value above 0.500 for all variables. Based on this research, it was found that all the indicators were valid and reliable. This research uses the R^2 assessment category proposed by Sholihin and Ratmono (2013), which is divided into three categories: the substantial R^2 category with a value of >0.75, the moderate R^2 category with a value of 0.50-0.75, and the weak R^2 category with a value of 0.25-0.50. Table 4 shows that CSC Performance has an R^2 value of 0.596, meaning that 59.6% of CSC Performance can be explained by two other variables: governance and CSC Visibility. In this research, the CSC Visibility value has an R^2 value of 0.378, which means that the CSC R^2 value is included in the weak category because it only has an R-square value of 0.378. Although CSC Visibility has a weak R^2, in assessing whether this model framework is appropriate and suitable for research, the suitability test and prediction of research relevance can be set by having a Q^2 value of more than 0, as shown in Table 4. Therefore, this result indicates that the model of this research has a qualified predictive relevance.

Table 5 Direct and Indirect Effect Test Results

Hypothesis	Path	Path Coefficient	t-Values	p-Values	Decision
H1	Governance→CSC Performance	0,419	3,148	0,002	Accept
H2	Governance→CSC Visibility	0,615	12,761	0,000	Accept
H3	CSC Visibility→CSC Performance	0,440	3,381	0,001	Accept
H4	Governance→CSC Visibility→CSC Performance	0,270	3,215	0,001	Accept

Source: Results of Data Processing (2023)

The subsequent analysis of the data that has been collected is to test the hypothesis that has been determined from the research framework. The study of a hypothesis accepted in this research is based on a significance level of 5%, a critical t-value of 1.96, or a p-value of 0.05. The hypothesis is accepted when the t-value exceeds 1.96 or the p-value is less than 0.05 (Hair et al., 2014, p.106-121). Based on Table 5, the four hypotheses are accepted for both direct and indirect effects, where all hypotheses have a t-value exceeding 1.96 or a p-value less than 0.05.

The results of testing H1 show that governance influences CSC Performance. The result is shown in Table 5 that testing H1 on this direct effect has a t-value of 3,148 and if the t-value > 1.96 then the H1 statement is accepted. This statement is supported by several previous studies, such as research by Maleh et al. (2021), who quoted from Lunardi et al. (2014), there is a statement that good governance can improve performance. Improved governance will lead to better supply chain and financial performance. Meanwhile, research by Gani et al. (2022) stated that good governance can improve CSC Performance because it is one of the factors that helps decide on the best action for the interests of all stakeholders.

The results of testing H2 show that governance influences CSC Visibility. Table 5 shows that testing H2 on the direct effect has a t-value of 12,761 and if the t-value > 1.96, then the H2 statement is accepted. The statement that H2 is accepted is supported by previous research by Gani et al. (2022) who quotes from Hong et al. (2018), explained that the existence of CSC Visibility in the supply chain network plays an important role in solving global supply chain problems which are very dynamic and rapidly changing. Therefore, according to Dubey et al. (2017) firms must implement practices that increase supply chain visibility through governance of collaboration from integration and information systems. In previous research, he also argued that corporate governance improves performance because it supports actions that are in the best interests of all shareholders (Wijethilake & Lama, 2018).

The results of testing H3 show that governance influences CSC Visibility. Table 5 shows that testing H3 on the direct effect has a t-value of 3,381 and if the t-value > 1.96, then the H3 statement is accepted. The statement that H3 is accepted is supported by previous research that has a statement that transparency and communication were accessible for the perpetrator's supply chain, which can increase the effectiveness in operations, which plays a vital role in improving supply chain performance (Kalaiarasan et al., 2022). According to the assumptions of Gani et al. (2022), CSC Visibility is critical in improving CSC Performance, because this process obtained through information sharing and connectivity allows for increased resilience and a resilient supply chain. Thus, this will have a direct or indirect impact on CSC Performance.

The results of testing H4 show that governance influences CSC Performance through CSC Visibility. Table 5 shows that testing H4 on the indirect effect has a t-value of 3,215 and

if the t-value > 1.96 then the H4 statement is accepted. The statement that H4 is accepted is supported by the previous research by Gani et al. (2022) and Pandey et al. (2020), good firms will have structured governance suitable for the supply chain and increase the efficiency of business operations, which will then positively impact CSC Performance. This statement is strengthened by previous research by Gani et al. (2022), the importance of governance in the CSC relationship performance and CSC Visibility, which forms the basis of practice Cyber Supply Chain Risk Management (CSCRM) in efforts to prevent and minimize the impact and preventive measures of attacks cyber in the whole process supply chain (Creazza et al., 2021).

Table 5 shows the indirect relationship between governance and CSC Performance through CSC Visibility, the lowest path coefficient value. The ones with the highest value in path coefficient, t-values, and lowest p-values directly influence governance and CSC Visibility. Even though this finding has R^2 included in the low category, this can be caused by various factors, such as the influence of other variances from the firm's operational side, the system integration side, the supply chain flexibility side, and many more (Gani et al., 2022; Siagian et al., 2021). To ensure a mediation relationship through CSC Visibility, this study used the Variance Accounted For (VAF) method to check the mediating role of CSC Visibility in this research. The VAF calculation found that there was 39.24% mediation. These indicate a partial mediation relationship quoted from Hair et al. (2014), where VAF greater than 20% and less than 80% can be categorized as typical partial mediation.

Conclusion

This research investigates the influence of Governance on CSC Performance with the mediating role of CSC Visibility. The mediating role of CSC Visibility significantly influences CSC Performance, as shown in Table 5. This study also found empirical evidence that having a dedicated governance team consisting of technical and non-technical personnel is important in defining security problems and solutions in CSC in the manufacturing industry, especially Java Island in Indonesia. Apart from that, accessing all supply chain business processes, namely CSC Visibility, requires good governance from the company. Security incidents cannot be handled only with technical support. Hence, good governance management can manifest company actions in creating coordinated conditions that have coherent coherence between all company members regarding decision-making in supply chain management to create effective CSC Performance efficiency in business implications, especially in the supply chain process.

This research is expected to contribute to practical business practices for manufacturing companies to evaluate their networks thoroughly and prioritize governance standards and policies that will increase their visibility among their supply chain partners, both internally and externally. Because of the maturity level of cyber security, supply chain partners, internally and externally, protect remote access to cyber systems from exploitation. All CSC partners must prioritize cyber security and work together to secure their networks from unwanted intrusions. Implementing ISO 27001, ISO 28000, ISO 28001, and other ISO certifications can also help prevent and solutions cyber-attacks on management information systems. This implementation requires establishing a dedicated governance team and creating an integrated system to increase network visibility to make CSC more secure. It will impact CSC's performance, which will be effective and efficient in implementing the supply chain process.

The limitation of this research is that it only examines it from the perspective of manufacturing companies on the island of Java in Indonesia. Hence, there are some suggestion for the future research that can expand be take other population distribution to Indonesia or other Indonesian islands. Apart from that, the future research can also employ qualitative methods, such as interviews with business practitioners, to examine the CSCRM approach from the perspective of end-users or distributors. This qualitative approach would complement the

quantitative methods used in this study, which provided a broader picture based on the samples participating through questionnaires. Qualitative methods would offer deeper insights into the different perceptions and expectations of legal regulations and the business environment.

References

Ahmadi, S., Tavana, M. M., Shokouhyar, S., & Dortaj, M. (2021). A new fuzzy approach for managing data governance implementation relevant activities. *The TQM Journal*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/tqm-01-2021-0015

Baah, C., Opoku Agyeman, D., Acquah, I. S. K., Agyabeng-Mensah, Y., Afum, E., Issau, K., Ofori, D., & Faibil, D. (2021). Effect of information sharing in supply chains: Understanding the roles of supply chain visibility, agility, collaboration on supply chain performance. *Benchmarking: An International Journal*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/bij-08-2020-0453

Chong, J., & Duan, S. X. (2022). Riding on the waves of the COVID-19 pandemic in re-thinking organizational design: A contingency-based approach. *Journal of Strategy and Management*, *15*(4). https://doi.org/10.1108/jsma-07-2021-0142

Creazza, A., Colicchia, C., Spiezia, S., & 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*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/scm-02-2020-0073

Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Luo, Z., & Roubaud, D. (2017). Upstream supply chain visibility and complexity effect on focal company's sustainable performance: Indian manufacturers' perspective. *Annals of Operations Research*, *290*, 343–367. https://doi.org/10.1007/s10479-017-2544-x

Erboz, G., Yumurtacı Hüseyinoğlu, I. Ö., & Szegedi, Z. (2021). The partial mediating role of supply chain integration between Industry 4.0 and supply chain performance. *Supply Chain Management: An International Journal*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/scm-09-2020-0485

Gani, A. B. D., Fernando, Y., Lan, S., Lim, M. K., & Tseng, M.-L. (2022). Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management & Data Systems*, *123*(3). https://doi.org/10.1108/imds-05-2022-0313

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223–240. https://doi.org/10.1108/scm-10-2018-0357

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J. F., 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.

Hajjar, S. T. (2018). Statistical analysis: Internal-consistency reliability and construct validity. *International Journal of Quantitative and Qualitative Research Methods* , *6*(1), 46–57.

Hong, J., Zhang, Y., & Ding, M. (2018). Sustainable supply chain management practices, supply chain dynamic capabilities, and enterprise performance. *Journal of Cleaner Production*, *172*(1), 3508–3519. https://doi.org/10.1016/j.jclepro.2017.06.093

Kalaiarasan, R., Olhager, J., Agrawal, T. K., & Wiktorsson, M. (2022). The abcde of supply chain visibility: A systematic literature review and framework. *International Journal of Production Economics*, *248*, 108464. https://doi.org/10.1016/j.ijpe.2022.108464

Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of adopting IT governance on financial performance: An empirical analysis among brazilian firms. *International Journal of Accounting Information Systems*, *15*(1), 66–81. https://doi.org/10.1016/j.accinf.2013.02.001

Mahfud, S., & Ratmono, D. (2013). Analisis SEM-PLS Dengan WarpPLS 3.0. *Penerbit Andi Yogyakarta*

Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. *EDPACS*, *63*(6), 1–22. https://doi.org/10.1080/07366981.2020.1815354

Number of cyber-attack cases in Indonesia from 2019 to 2022 (in million). (2023, September 15). Katadata Insight Center; East Ventures; Statista Research Department. https://www-statista-com.ezproxy.dewey.petra.ac.id:2443/statistics/1412527/indonesia-number-of-cyber-attacks/

P. N., S. (2021). The impact of information security initiatives on supply chain robustness and performance: An empirical study. *Information & Computer Security*, *29*(2), 365–391. https://doi.org/10.1108/ics-07-2020-0128

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: Conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103–128. https://doi.org/10.1108/jgoss-05-2019-0042

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). John Wiley & Sons.

Serkan K., S., & Baygin, M. (2022). *Supply chain management reshaped with industry 4.0: A review: Vols. 108 A*. Emerald Publishing Limited. https://www.emerald.com-/insight/content/doi/10.1108/S1569-37592022000108A033/full/html

Siagian, H., Tarigan, Z. J. H., & Jie, F. (2021). Supply chain integration enables resilience, flexibility, and innovation to improve business performance in covid-19 era. *Sustainability*, *13*(9), 4669. MDPI. https://doi.org/10.3390/su13094669

Somapa, S., Cools, M., & Dullaert, W. (2018). Characterizing supply chain visibility: A literature review. *The International Journal of Logistics Management*, *29*(1), 308–339. https://doi.org/10.1108/ijlm-06-2016-0150

Wijethilake, C., & Lama, T. (2018). Sustainability core values and sustainability risk management: Moderating effects of top management commitment and stakeholder pressure. *Business Strategy and the Environment*, *28*(1), 143–154. https://doi.org/10.1002/bse.2245