

The mediating and moderating Roles of Digital Ecosystem and Sustainable Resilience in the relationship between Green Supply Chain Cybersecurity Readiness and Supply Chain Visibility

Abdul Ganiw Hussein

aghussein@tatu.edu.gh

Tamale Technical University

Mohammed Majeed

Tamale Technical University

Mohammed Awal Zingnaa

Tamale Technical University

Research Article

Keywords: Green Supply chain cybersecurity readiness, digital ecosystem, supply chain visibility, sustainable resilience

Posted Date: September 7th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10438676/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Purpose

This research examines how information processing capability and digital supply chain capability affect supply chain resilience through their mediating effect on supply chain risk management. Based on the theory of information processing, information processing capability is considered a higher-order construct that comprises disruption orientation and supply chain visibility.

Design/methodology/approach:

A quantitative cross-sectional research methodology was followed. Data were gathered from 251 supply chain managers in manufacturing organisations located in Pakistan. Partial Least Squares Structural Equation Modelling (PLS-SEM) was applied to analyse and validate the proposed hypotheses.

Findings:

The study's results show that information processing ability and digital supply chain ability positively affect supply chain risk management. Supply chain risk management, in turn, positively affects the level of resilience within the supply chain. In addition, the study finds that supply chain risk management mediates the relationship between information processing ability and resilience, and between digital supply chain ability and resilience.

Practical implications:

The study emphasises the need for improvements in supply chain visibility, disruption orientation, and digitalisation efforts to enhance capability in managing risks and building resilience to disruptions. The managers must develop the necessary skills for real-time information processing and effective risk management practices.

Originality/value:

This research contributes to Information Processing Theory by incorporating disruption orientation, visibility, digital supply chain capability, supply chain risk management, and supply chain resilience into one comprehensive theoretical model. The empirical analysis is based on the manufacturing industry following the pandemic period, and shows the important part that visibility plays as an information processing tool in relation to supply chain risk management and resilience.

Introduction

The advent of the digital era in global supply chains has completely redefined how organisations generate, deliver and sustain value. Advanced digital technologies such as artificial intelligence, Internet of Things (IoT), blockchain, cloud computing and data analytics are used in modern supply chains to enhance efficiency, visibility, and transparency, and facilitate sustainable supply chain performance (Tsolakis et al., 2023). Digital technologies allow organisations to build industrial digital ecosystems where manufacturers interact with suppliers, customers, distributors, software providers, connectivity providers and other parties to co-create, deliver and capture value via digital solutions (Sjödin et al., 2022). Although digitalisation facilitates sustainability goals, it also makes organisations vulnerable to cyber threats, data breaches, supply chain vulnerabilities, privacy risks, and technological challenges that could disrupt sustainability efforts and lead to economic and social implications (Goswami et al., 2023). This is why organisations strive to find ways to ensure sustainable operations in the age of digital transformation.

Disruptions of recent years, including the outbreak of the COVID-19 pandemic, Brexit, the US-China trade war and the Russian invasion of Ukraine, have demonstrated the vulnerability of globally interconnected supply chains, prompting organisations to rethink their supply chain strategies (Bednarski et al., 2025). These events show that efficiency alone cannot ensure the survival of organisations in a turbulent environment. As a result, sustainable resilience has gained popularity both among academic researchers and practitioners. Sustainable resilience is defined as the ability of an organisation to resist, absorb, adapt to and recover from disruptions without compromising its ability to grow and achieve sustainability goals (Miceli et al., 2021). Increased pressure from regulators, investors and other stakeholders forces organisations to develop the necessary adaptive capabilities to deal with regulatory uncertainty, climate change risks, and increase organisational resilience (Park, 2021).

In this regard, cybersecurity is one aspect of sustainable resilience. The growing reliance of organisations on digital infrastructure, cloud computing, interconnected information systems and operational technologies expands the cyber-attack surface and increases organizational susceptibility to cyber risks (George et al., 2024). Cyber-attacks may disrupt production processes, compromise confidential information, disturb supply chain operations, and damage stakeholder trust, potentially undermining sustainable resilience and the ability to pursue sustainability goals (George et al., 2024). For this reason, organisations should possess cybersecurity capabilities that go beyond information security measures. Cybersecurity readiness emerges as an important capability for organisations aiming at digital transformation and sustainable supply chain performance in the Industry 5.0 environment (Tyagi & Tyagi, 2025). GSCCR is the term that describes the organisation's preparedness to protect digital supply chain infrastructures, environmental information systems, and sustainability-related operations against cyber-attacks and to encourage environmentally and socially responsible practices.

In addition to cybersecurity, Supply Chain Visibility (SCV) emerges as a valuable capability for organisations seeking to increase their resilience. SCV is defined as the level of access to timely, accurate, and complete demand and supply information that helps organisations manage their supply chain operations (Kalaizarasan et al., 2022). Higher levels of supply chain visibility, enabled by real-time

information sharing and analysis, help organisations identify risks, monitor and respond to disruptions, coordinate responses from supply chain partners, and make timely decisions to increase their resilience to disruptive events (Dey, 2023). Hence, the supply chain visibility, facilitated by real-time monitoring, information transparency, and digital technologies, becomes an important capability to enhance supply chain resilience, agility and risk anticipation in increasingly complex and disruption-prone environments (Padovano & Ivanov, 2025).

The relationship between Green Supply Chain Cybersecurity Readiness and Supply Chain Visibility can be explained using Information Processing Theory (IPT) (Galbraith, 1973). IPT can be considered as the theoretical foundation of this research. According to the Organizational Information Processing Theory (OIPT), organizations operating in uncertain and volatile environments need adequate information-processing capabilities to gather, interpret, and process relevant information in order to reduce uncertainty and make effective decisions (Yu et al., 2022). As environmental complexity grows, organizations have to improve their information gathering, processing, exchanging and using capabilities. In this respect, cybersecurity readiness can be considered as the information-processing capability since it depends on digital systems, communication channels, and team coordination that enable information exchange, threat identification, and collaborative decision-making (Zolkafli & AlArabi, 2025). Similarly, supply chain visibility provides organizations with the necessary information to track, respond to and recover from disruptions and enhance supply chain resilience (Rashid et al., 2024). Thus, organizations with high level of cybersecurity readiness are expected to have a high level of visibility that leads to sustainable resilience.

Alongside with cybersecurity readiness and visibility, the growing complexity of the digital environment brings new opportunities and challenges for organizations. Digital supply chain ecosystems are characterized by interactions and interconnections of various stakeholders, platform-based collaboration, information sharing, resource integration, and ecosystem development through the use of technologies (Chi et al., 2024). Although the digital connectivity and global digital ecosystems foster innovation, information sharing, and global cooperation, they also increase organizational complexity, coordination challenges, cybersecurity risks, and information-processing needs (Luo, 2022). This implies that the effectiveness of cybersecurity readiness and visibility capabilities depends on the level of digital ecosystem complexity. Organizations functioning in complex digital ecosystems face cybersecurity challenges due to interconnected systems, cloud services, third party dependencies, and IoT devices, making proactive cybersecurity and resilience-building measures essential for ensuring business continuity and growth (Kanaan et al., 2025). The motivation behind choosing this research topic is driven by several practical and theoretical considerations. First, the transition towards digitally interconnected supply chain ecosystems brings substantial cybersecurity risks for organizations that may undermine business continuity, resilience, and sustainability goals if not properly managed (Kanaan et al., 2025). Second, organizations seek capabilities that would enable them to digitalize, sustain and be resilient. Third, despite the growing interest in research on resilience, sustainability and digital transformation, there is a lack of studies that consider the impact of Green Supply Chain Cybersecurity Readiness on

Sustainable Resilience via Supply Chain Visibility in different levels of Digital Ecosystem Complexity (Tran et al., 2026).

However, there still exist a number of gaps in the literature. Despite the growing interest to supply chain resilience, there is a scarcity of research on cyber-resilience. According to existing studies, many digitally transformed supply chains lack cybersecurity that is embedded in core management practices, while the capabilities needed to build cyber resilience are poorly studied. This implies that cybersecurity readiness can be considered as a strategic capability that contributes to resilient operations of digitally connected supply chains (Mahim et al., 2025). Although cyber risks become more and more common and costly, there is little empirical evidence of Green Supply Chain Cybersecurity Readiness as an antecedent of Sustainable Resilience. Furthermore, while prior studies emphasize the importance of supply chain visibility for resilience and increasingly call for integrating cybersecurity into the research on supply chain resilience, there is little empirical research about the mechanisms through which cybersecurity-related capabilities affect resilience outcomes via supply chain visibility. (Ahmadi et al., 2025). Another issue is associated with the Digital Ecosystem Complexity. Although environmental heterogeneity and complexity have been recognized as the key factors, there is a lack of empirical studies investigating digital ecosystem complexity as a moderator of the relationship between organizational capabilities and organizational performance (Mikalef et al., 2021). Previous researches pay much attention to operational complexity, ignoring digital ecosystem complexity as the contextual factor that influences the effectiveness of organizational capabilities. This means that it is unclear how the digital ecosystem complexity affects the influence of cybersecurity readiness on visibility and visibility on sustainable resilience.

To address these limitations, the present study endeavors to explore the influence of Green Supply Chain Cybersecurity Readiness (GSCCR) on Sustainable Resilience mediated by Supply Chain Visibility and moderated by Digital Ecosystem Complexity. The study intends to answer the following questions: (1) what are the effects of GSCCR on Supply Chain Visibility and Sustainable Resilience? (2) What is the effect of Supply Chain Visibility on Sustainable Resilience and does it serve as mediator in the link between GSCCR and Sustainable Resilience? And (3) what is the moderating effect of Digital Ecosystem Complexity on GSCCR and Supply Chain Visibility and on the relationship between Supply Chain Visibility and Sustainable Resilience? There are three primary contributions of this study to literature. First, a theoretical contribution where this study extends Information Processing Theory to view Green Supply Chain Cybersecurity Readiness as an information processing capability. Second, an empirical contribution, which addresses the current variable, mediation, moderation, context, and methodological gaps through developing a moderated-mediation framework that relates GSCCR, SCV, DEC, and Sustainable Resilience. Third, practical contributions where managers and policymakers get evidence-based suggestions on how to make use of cyber security readiness and visibility capabilities to improve sustainable resilience in digital ecosystems becoming ever more complicated. Hence, this study advances the emerging field of sustainable digital supply chain management by integrating cyber security readiness, visibility, and ecosystem complexity in one framework. The rest of this paper is

structured as follows: Literature Review and Hypotheses Development, Methodology, Results and Discussion, Implications for Theory and Practice, Conclusion, Limitations and Future Research.

Literature Review and Theoretical Support

Research literature on digital supply chain management highlights the importance of effective integration of such factors as cybersecurity, information visibility and digital technologies for developing organizational resilience and sustainability. Based on IPT, organizations operating in volatile and unpredictable conditions should possess more advanced information processing abilities in order to decrease uncertainty, make good decisions and cope with disruptions. Green Supply Chain Cybersecurity Readiness (GSCCR) refers to the strategic competence that allows businesses to protect their digital infrastructure, environmental information system and sustainability-oriented operations from cyber-attacks and facilitate smooth information exchange in supply chain networks. Research reveals that cyber resilience capabilities play an important role in developing supply chain resilience since they help supply chains to sense, seize and transform themselves in order to cope with cyber threats and thus protect their critical assets and flows of material, information and money from cyberattacks (Herburger et al., 2024). Moreover, digital supply chain capabilities and information processing processes increase the supply chain resilience through improved supply chain risk management capabilities, greater visibility, disruption orientation and effectiveness of responses to supply chain disruptions (Rashid et al., 2024). Since businesses are currently implementing digital transformation in pursuit of sustainability, the importance of cybersecurity readiness becomes crucial for ensuring protection of environmental and operational data and digital systems used for sustainable and circular operations (Seyi-Lande et al., 2024). Based on these considerations, one can say that GSCCR can be seen as an important factor which influences supply chain effectiveness and sustainable resilience because cybersecurity practices ensure protection of critical information assets, secure information exchange, decrease disruption risks and increase supply chain resilience and sustainability (Layode et al., 2024).

Increasing body of literature also highlights the critical importance of such factors as Supply Chain Visibility (SCV) and Digital Ecosystem Complexity (DEC) for enhancing Sustainable Resilience (SR). Supply chain visibility provides businesses with the possibility to get timely and reliable information about inventory levels, supplier activities, logistics activities and market demand in order to identify risks proactively, collaborate and make decisions. Evidence shows that the companies possessing higher supply chain visibility will be able to adapt to disruptions and will have better resilience outcomes due to greater visibility, information exchange in real time and improved collaboration between supply chain partners (Razak et al., 2023). On the other hand, the growth of digital ecosystems increases the complexity of organizational network leading to new opportunities and challenges for resilience. Digital Ecosystem Complexity represents the level of technological connectivity, interdependence of stakeholders and information exchange within digital supply chains. Research suggests that in the case of complex regional innovation ecosystems digital transformation increases resilience and sustainable development by means of information exchange, knowledge sharing, collaboration and coordination which leads to increased adaptability and resource reconfiguration in ecosystem (Wang et al., 2025).

Likewise, research reveals that resilient and digitally-enabled supply chains increase sustainability performance through improved operational continuity, resource efficiency, environmental performance and adaptiveness in the context of disruptions and crisis situations (Setyadi et al., 2025). At the same time, current research recognizes the importance of cyber resilience, SCV provided by digital technologies and growing DEC in supply chain ecosystem but fails to integrate all these dimensions.

Underpinning Theory

This research work is based on the Information Processing Theory (IPT), introduced by Galbraith (1973). According to IPT, organizations functioning in uncertain and complex environment should have effective information processing skills to gather, interpret, exchange and use information to make decisions and improve their performance. According to IPT, environmental uncertainty causes information needs to increase, and organizations should develop mechanisms that will improve information gathering and information processing to decrease uncertainty and increase organizational effectiveness. Concerning this study, Green Supply Chain Cybersecurity Readiness (GSCCR) is an information processing capability that helps organizations to securely gather, exchange and process information in digital supply chain networks and Supply Chain Visibility (SCV) is a capability that allows organizations to have access to relevant and reliable information at the right time during the entire supply chain. Thus, according to the theory, organizations with high cybersecurity readiness and visibility capabilities can better cope with risks, coordinate their supply chain activities, be ready to deal with disturbances and achieve Sustainable Resilience. In addition, Digital Ecosystem Complexity increases information processing demands on organizations, thus making their cybersecurity readiness and visibility capabilities essential to adapt and become resilient. It is logical to choose IPT as the basis of this research as it analyzes the effect of information capabilities on sustainable resilience in digital supply chain networks. Moreover, previous studies had already used Information Processing Theory to examine the effect of digital technologies, visibility and information capabilities on supply chain resilience and organizational performance.

Hypotheses Development and Literature Support

Green Supply Chain Management and Sustainability Resilience

Green Supply Chain Management (GSCM) has been developed as a strategy that allows organizations to incorporate environmental factors into supply chain activities while at the same time increasing their capacity to withstand and recover from disruption. Sustainability resilience can be defined as an organization's ability to preserve economic viability, environmental performance, and social responsibility under unexpected disruptions. During the last few years, research shows that green practices in the field of procurement, design, manufacturing, waste management, reverse logistics, and environmental collaboration significantly increase resilience by promoting resources efficiency and reducing environmental risks and enhancing relationships with stakeholders. Organizations that practice Green Supply Chain Management (GSCM) are well-positioned to respond to environmental risks, to deal with

new expectations regarding sustainability and thus achieve sustainability and competitive advantage (Feng et al., 2024).

Under the framework of Information Processing Theory (IPT), green practices in the supply chain make it possible to process environmental information more effectively, thereby increasing organizational adaptability and sustainability. Sustainable supply chain management allows creating a collaborative environment in which stakeholders share information and knowledge. Empirical evidence proves that companies practicing green supply chain management (GSCM) show higher organizational resilience and recover faster from supply chain disruption and external shocks than organizations that do not implement green practices (Ullah et al., 2022). In addition, organizations that use sustainable and green supply chain management can create proactive resilience and integrated risk management which can enhance organizational continuity, adaptation to disruption and sustain performance during the period of crisis (Setyadi et al., 2025). Thus, the following hypothesis is generated:

H1: Green Supply Chain Management has a direct positive impact on Sustainability Resilience.

Green Supply Chain Management and Supply Chain Visibility

Supply Chain Visibility (SCV) represents the ability of organizations to obtain, monitor, and communicate timely, accurate, and relevant information during supply chain operations. Modern GSCM practices utilize digital tools, environmental monitoring, supplier collaboration, and sustainability reporting techniques that contribute to improved information transparency along supply chains. When organizations implement environmental management techniques and systems, information sharing systems are developed, which make it possible to gather and share information about emissions, energy consumption, water usage, resource efficiency, and waste along supply chain participants and therefore improve SCV and environmental impacts awareness (Bellamy et al., 2020).

Information Processing Theory suggests that organizations with more complex and uncertain environment need better information processing capacity. GSCM contributes to information exchange and environmental transparency, which results in improved visibility along the whole supply chain network. Recent researches revealed that supply chains oriented on sustainability have increased visibility because of their enhanced collaboration, digital integration, and information exchange. Green supply chain practices foster transparency, collaboration, and information exchange between stakeholders in the supply chain, making it possible for organizations to gather full information about energy usage, emissions, waste production, and other activities (Onukwulu et al., 2021). Therefore, GSCM is likely to increase visibility that will help organizations make better decisions and manage disruptions. Accordingly, the following hypothesis is proposed:

H2: Green Supply Chain Management has a significant positive impact on Supply Chain Visibility.

Supply Chain Visibility and Sustainability Resilience

Supply Chain Visibility has been acknowledged widely as an important mechanism in increasing resilience in today's complex and uncertain business environment. With the help of supply chain visibility, companies have access to information on inventory status, supplier activity, logistics processes, demand, and disruptions that occur. In other words, access to real-time information contributes to better decision-making, better cooperation between supply chain members, and more efficient response to unexpected events. Higher supply chain visibility helps firms to recognize potential disruptions in advance, proactively manage risks, and perform some preventive measures, such as reallocation of resources, changes in production, or replacement of suppliers prior to disruptions influencing operations negatively (Aljohani, 2023).

The Information Processing Theory assumes that higher visibility increases certainty by increasing information availability and improving its quality needed for adaptation. Improved transparency and access to information allows organizations not only to improve their resilience but also to increase sustainability resilience by sustaining their environmental and social performance through disruptions. As it has been shown recently, higher supply chain visibility helps organizations to become more resilient through increasing agility, facilitating collaborative decision-making, and better ability of organizations to recognize and react to disruptions that take place in their supply chains (Kumar & Anbanandam, 2020). Moreover, higher visibility of supply chains is beneficial for sustainability by allowing to use real-time information and control abilities to improve environmental performance of organizations and facilitate environmental collaboration between organizations in the network. Therefore, the following hypothesis is made:

H3: Supply Chain Visibility has a significant positive impact on Sustainability Resilience.

The Mediating Role of Supply Chain Visibility between Green Supply Chain Management and Sustainability Resilience

While Green Supply Chain Management contributes to Sustainability Resilience, the exact mechanism that drives this contribution calls for exploration. One such possible mechanism may be Supply Chain Visibility. The use of GSCM implies the application of principles such as transparency of information, environmental reporting, collaboration between different stakeholders, and digitization, all of which contribute to increased supply chain visibility. Increased supply chain visibility allows organizations to better anticipate disruptions, allocate resources, coordinate their mitigation efforts, and achieve their sustainability and ESG goals in volatile environments (Nnabueze et al., 2021).

Within the framework of Information Processing Theory, increased information-processing capabilities of an organization can be seen in increased visibility within supply chains. With greater visibility in the operation of supply chains, organizations are able to react more efficiently to disruptions related to environment, operation, and market. Recent research has proven that supply chain visibility is a critical component of resilience and through which various organizational mechanisms such as risk management, collaboration, and information exchange improve preparedness and response to

disruptions and increase resilience of the entire supply chain network (Statsenko et al., 2024). Therefore, visibility can serve as a key mechanism through which GSCM builds sustainability resilience. Thus, the following hypothesis is offered:

H4: Supply Chain Visibility has a positive mediating role between Green Supply Chain Management and Sustainability Resilience.

The Moderating Role of Digital Ecosystem Complexity on the Relationship between Green Supply Chain Management and Supply Chain Visibility

The Digital Ecosystem Complexity (DEC) concept is understood as a level of interconnectedness, diversity of technologies used, information exchange intensity, stakeholder interdependence, and platform integration in digitally-enabled supply chains. The increasing digitalization of operations has resulted in the development of complex ecosystems that include many stakeholders, technologies, and information systems within digitally-enabled supply chains. In such ecosystems, GSCM visibility capabilities' effects are dependent on contextual complexity variables where the product complexity acts as a moderator between supply chain visibility and sustainability performance (Emon & Khan, 2024).

According to the Information Processing Theory, organizations functioning in very complex environments have to possess greater information-processing abilities. In case the digital ecosystem complexity is very high, the organizations that implement GSCM practices should be engaged in higher levels of information exchange, cooperation, and environmental scanning processes. Consequently, the positive connection between GSCM and visibility will be strengthened since the value of the information openness and stakeholder coordination becomes even more critical in the context of complexity. Research conducted earlier showed that supply chain complexity increases the need for information processing abilities and, thus, makes digital technologies and organizational competencies such as visibility and collaboration especially important in achieving resilient outcomes (Li & Sukhotu, 2025). Hence, digital ecosystem complexity can positively influence the relationship between GSCM and supply chain visibility. Thus, the following hypothesis is formed:

H5: Digital Ecosystem Complexity has a positive moderating role on the relationship between Green Supply Chain Management and Supply Chain Visibility.

The Moderating Role of Digital Ecosystem Complexity on the Relationship between Supply Chain Visibility and Sustainability Resilience

However, the advantages of Supply Chain Visibility may be conditional on the level of digital ecosystem complexity that companies work in. In digital transformation ecosystems characterized by a high level of interconnectivity, enhanced visibility allows organizations to handle complex information streams, coordinate stakeholder activities, detect disturbances, and preserve business continuity. With the increasing complexity of digital transformation environments, companies utilize more decision-making based on data analysis, knowledge management, and information (Tarigan et al., 2025).

According to Information Processing Theory, organizations operating in a more complex environment are capable of deriving higher value from their information processing ability because uncertainty and coordination needs are growing considerably. Increased visibility is especially relevant for complex digital ecosystems in which several stakeholders, technologies, and processes are involved at the same time. Modern research reveals that in such complex socio-technical ecosystems, sustainability resilience grows dependent on digital and informational competencies that promote transparency, coordination, accountability, and information sharing among distributed actors (Oyebode, 2025). Thus, the positive impact of Supply Chain Visibility on Sustainability Resilience will be even more significant in cases of high Digital Ecosystem Complexity. Based on the abovementioned, the following hypothesis can be developed:

H6: Digital Ecosystem Complexity has a positive moderating role on the relationship between Supply Chain Visibility and Sustainability Resilience.

Methodology

The research design used in this study is the cross-sectional survey design in order to investigate the links between Green Supply Chain Cybersecurity Readiness (GSCCR), Supply Chain Visibility (SCV), Digital Ecosystem Complexity (DEC), and Sustainability Resilience (SR). Quantitative research design was chosen because it makes possible to empirically test relationships between latent constructs and use more advanced statistical tools for the hypotheses verification. The theoretical foundation of the research is the Information Processing Theory (IPT). According to IPT, organizations functioning in complex and uncertain environment need to have better information processing capabilities in order to deal with the complexity and enhance organizational outcomes. Within the framework of this study, GSCCR is seen as the information processing capability that enables secure information exchange, SCV refers to the information accessibility and transparency, DEC represents complexity of the digital environment, and SR is the strategic outcome resulting from the organizational adaptation and sustainability resilience.

The population of the study includes managers and senior executives responsible for supply chain management, logistics, procurement, information technology, sustainability management, and operations management. They have been selected due to their involvement in the digital transformation processes, cybersecurity implementation, supply chain coordination, and organizational resilience programs. The unit of analysis is the firm while managers serve as key informants since of their knowledge and experience with the studied constructs. A purposive sampling technique has been used to identify firms that have digitalized their supply chains and have implemented sustainable practices. The choice of this sampling method guarantees that respondents have adequate knowledge about cybersecurity readiness, visibility capabilities, digital ecosystems, and resilience practices making data collection more accurate and reliable.

The data were collected using the structured questionnaire developed based on the validated scales adopted from previous research in the domains of supply chain management, cybersecurity, digital transformation, and organizational resilience. All items of the questionnaire were measured using a five-point Likert scale from 1 (Strongly Disagree) to 5 (Strongly Agree). The questionnaire included four major constructs. Green Supply Chain Cybersecurity Readiness (GSCCR) was measured using five items measuring the degree of the cybersecurity readiness in the supply chain processes. Supply Chain Visibility (SCV) was measured using four items measuring information accessibility, transparency and visibility. Digital Ecosystem Complexity (DEC) was measured using four items representing the complexity and interconnections of digital technologies, stakeholders and digital platforms within the supply chain environment. Sustainability Resilience (SR) was measured using five items measuring the ability of the firm to cope with disruptions, adapt, and recover maintaining sustainability. Prior to the main survey, the pilot study was conducted in order to check the clarity, content validity and reliability of the measurement items.

The data were analyzed using Structural Equation Modeling (SEM). Prior to testing the structural relationships, the measurement model has been assessed in order to ensure reliability and validity. A number of statistical procedures has been carried out in order to measure factor loadings, Cronbach's alpha, composite reliability (CR), average variance extracted (AVE) and discriminant validity. Also the procedures of the data screening have been conducted in order to find missing values, outliers and inconsistencies. Then the Confirmatory Factor Analysis (CFA) was conducted in order to test the adequacy of the measurement model. The results of CFA revealed adequate fit of the model with $\chi^2/df = 2.18$, Comparative Fit Index (CFI) = 0.963, Tucker-Lewis Index (TLI) = 0.956, Normed Fit Index (NFI) = 0.941, Incremental Fit Index (IFI) = 0.964, Goodness-of-Fit Index (GFI) = 0.927, Standardized Root Mean Square Residual (SRMR) = 0.041 and Root Mean Square Error of Approximation (RMSEA) = 0.058. All these indices exceeded the threshold values indicating the adequate representation of the observed data by the measurement model.

After the measurement model assessment, the structural model was evaluated using the hierarchical stepwise regression analysis. The direct effects of GSCCR on SCV and SR, as well as the direct effect of SCV on SR were tested while controlling for the firm age, firm size, environmental dynamism and environmental munificence. The moderating effect of Digital Ecosystem Complexity was tested by adding into the structural model interaction terms including $GSCCR \times DEC$ and $SCV \times DEC$. Also the bootstrapping procedures were carried out in order to test the mediating effect of Supply Chain Visibility in the link between GSCCR and Sustainability Resilience. It made possible to estimate the indirect effects and calculate mediation strength. Lastly, the Importance-Performance Map Analysis (IPMA) was conducted in order to identify the relative importance and performance of the predictor constructs in explaining Sustainability Resilience.

Measurements

Green Supply Chain Cybersecurity Readiness (GSCCR), Supply Chain Visibility (SCV), Digital Ecosystem Complexity (DEC), and Sustainability Resilience (SR) were the four major constructs tested in this research. Measurement scales were adopted from reliable scales used in the fields of supply chain, cybersecurity, digitalization, and resilience to guarantee content validity. The green supply chain cybersecurity readiness (GSCCR) construct was measured through five questions related to the readiness of the organization to deal with cyber security issues in digitally enabled supply chains. The SCV construct was measured based on four questions that addressed accessibility, transparency, and visibility of information in supply chain processes. DEC was tested through four questions regarding the complexity of digital technologies, platforms, and stakeholders' relationships in the digital ecosystem. SR was tested through five questions that assessed the organization's capability to predict, respond to, adapt to, and recover from disruptions. All measurement questions were answered by using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).

Results and Discussion

The validity and reliability of the measurement instrument were tested using Confirmatory Factor Analysis (CFA). The findings showed that the factor loading values were between 0.81 and 0.91, above the recommended value of 0.70. The Cronbach alpha values were between 0.88 and 0.94, while the CR values were between 0.92 and 0.95, hence showing high reliability in internal consistency. Also, the AVE values were between 0.73 and 0.80, above the recommended value of 0.50, hence demonstrating convergent validity. The VIF values were between 1.74 and 2.34, showing no issues of multicollinearity. Additionally, discriminant validity was proven through the use of the Fornell-Larcker criterion and HTMT approach, whereby all the values met the recommended levels, and constructs measured distinct theories.

Table 1
CFA, Reliability, Validity and Multicollinearity Assessment Measurement Model Results

Construct	Item	Mean	SD	Loading	VIF	Cronbach's α	CR	AVE
Green Supply Chain Cybersecurity Readiness (GSCCR)	GSCCR1	4.05	0.69	0.84	2.21	0.92	0.94	0.75
	GSCCR2			0.88				
	GSCCR3			0.86				
	GSCCR4			0.85				
	GSCCR5			0.89				
Supply Chain Visibility (SCV)	SCV1	4.11	0.71	0.83	2.08	0.90	0.93	0.77
	SCV2			0.89				
	SCV3			0.87				
	SCV4			0.91				
Digital Ecosystem Complexity (DEC)	DEC1	3.72	0.74	0.81	1.74	0.88	0.92	0.73
	DEC2			0.87				
	DEC3			0.85				
	DEC4			0.88				
Sustainability Resilience (SR)	SR1	4.18	0.67	0.88	2.34	0.94	0.95	0.80
	SR2			0.91				
	SR3			0.90				
	SR4			0.87				
	SR5			0.89				

Evaluation

Criterion	Threshold	Result
Factor Loading	> 0.70	Passed
Composite Reliability (CR)	> 0.70	Passed
AVE	> 0.50	Passed
VIF	< 5.00	Passed

The results of measurement model assessment, which include factor loadings, reliability, convergent validity and multicollinearity diagnostics, are presented in Table 1. From the table, it is clear that all measurement items have factor loadings above the suggested value of 0.70. The factor loadings range from 0.81 to 0.91. Thus, all measurement indicators effectively capture their latent constructs, making them reliable. More specifically, factor loadings for Green Supply Chain Cybersecurity Readiness (GSCCR) range from 0.84 to 0.89, for Supply Chain Visibility (SCV) from 0.83 to 0.91, for Digital Ecosystem Complexity (DEC) from 0.81 to 0.88 and for Sustainability Resilience (SR) from 0.87 to 0.91. The reliability analysis shows the quality of measurement model as well. Cronbach's alpha values are ranging from 0.88 to 0.94, which is above the suggested level of 0.70. Similarly, Composite Reliability (CR) values range from 0.92 to 0.95, showing good internal consistency reliability of the measurement model. Convergent validity of the measures is confirmed by Average Variance Extracted (AVE) values ranging from 0.73 to 0.80. Since AVE is above the suggested level of 0.50, each construct explains more than 50 percent of the variance of its indicators. Finally, Variance Inflation Factor (VIF) values range from 1.74 to 2.34, which is far below the critical value of 5.00, implying that there is no multicollinearity problem with the measurement model.

Table 2
Discriminant Validity (Fornell-Larcker)

Construct	GSCCR	SCV	DEC	SR
GSCCR	0.866			
SCV	0.64	0.878		
DEC	0.42	0.39	0.854	
SR	0.69	0.66	0.45	0.894

The discriminant validity of Table 2 is tested based on the Fornell-Larcker criterion. As per the Fornell-Larcker criterion, the square root of the AVE of each construct needs to exceed its correlations with other constructs. The square root of AVE of each construct, which is shown on the diagonal, is 0.866 for GSCCR, 0.878 for SCV, 0.854 for DEC, and 0.894 for SR. Each square root of AVE value is higher than the corresponding inter-construct correlations. For instance, the square root of AVE of GSCCR (0.866) is larger than its correlations with SCV (0.64), DEC (0.42), and SR (0.69). Likewise, the square root of AVE of SR (0.894) is larger than its correlations with GSCCR (0.69), SCV (0.66), and DEC (0.45). It suggests

that each construct is theoretically distinct from other constructs and measures different theoretical concepts. Thus, discriminant validity is satisfactorily achieved and constructs do not overlap with each other.

Table 3
HTMT Ratios

Constructs	HTMT
GSCCR ↔ SCV	0.74
GSCCR ↔ DEC	0.48
GSCCR ↔ SR	0.79
SCV ↔ DEC	0.44
SCV ↔ SR	0.77
DEC ↔ SR	0.51

Another approach for assessing discriminant validity is through the Heterotrait-Monotrait Ratio. All HTMT ratios are less than the threshold value of 0.85. The HTMT ratios that have the largest values are between GSCCR and SR (0.79), SCV and SR (0.77), and GSCCR and SCV (0.74). The rest are less and have values of between 0.44 and 0.51. As all the HTMT values are less than 0.85, the conclusion is drawn that discriminant validity has been successfully obtained. This means that there is sufficient difference in the constructs and that the respondents made distinctions between cybersecurity readiness, visibility, ecosystem complexity, and sustainability resilience.

Table 4
Overall Model Fitness CFA Model

Fit Index	Value	Recommended
χ^2	318.87	-
df	146	-
χ^2/df	2.18	< 3.00
CFI	0.963	> 0.90
TLI	0.956	> 0.90
NFI	0.941	> 0.90
IFI	0.964	> 0.90
GFI	0.927	> 0.90
AGFI	0.904	> 0.80
SRMR	0.041	< 0.08
RMSEA	0.058	< 0.08

Table 4 shows the goodness-of-fit measures for the Confirmatory Factor Analysis (CFA) model and proves that the suggested measurement model has fitted the observed data exceptionally well. First, the value of the chi-square (χ^2) is equal to 318.87 with 146 degrees of freedom, producing the ratio of χ^2/df equal to 2.18, which is below the recommended threshold of 3.00. Thus, the difference between the theoretical and empirical data is quite acceptable. Moreover, all the incremental fit indices exceed their respective cut-off values. In particular, the Comparative Fit Index (CFI = 0.963), Tucker-Lewis Index (TLI = 0.956), Normed Fit Index (NFI = 0.941), Incremental Fit Index (IFI = 0.964), and Goodness-of-Fit Index (GFI = 0.927) are all higher than the recommended index of 0.90. Additionally, the Adjusted Goodness-of-Fit Index (AGFI = 0.904) exceeds the minimum threshold of 0.80.

Besides, the residual-based fit indices show the very good level of fit. In particular, the Standardized Root Mean Square Residual (SRMR) is equal to 0.041 and is much lower than the maximum recommended index of 0.08, while the Root Mean Square Error of Approximation (RMSEA) equals 0.058 and is also lower than the acceptable index of 0.08. All this means that the discrepancies between the predicted covariance matrix and the observed covariance matrix are quite small. Thus, the combination of absolute fit indices, incremental fit indices, and residual-based fit indices confirms that the suggested measurement model fits the data exceptionally well. Consequently, the results of the CFA analysis prove that the latent constructs Green Supply Chain Cybersecurity Readiness (GSCCR), Supply Chain Visibility (SCV), Digital Ecosystem Complexity (DEC), and Sustainability Resilience (SR) are sufficiently measured with their items.

Table 5
Stepwise Regression for Supply Chain Visibility (H2 & H5) Dependent Variable:
SCV

Variables	Model 1	Model 2	Model 3
Firm Age	0.11 (2.01)*	0.09 (1.78)	0.08 (1.63)
Firm Size	0.05 (0.88)	0.04 (0.74)	0.03 (0.58)
Environmental Dynamism	0.14 (2.36)*	0.10 (1.89)	0.08 (1.56)
Environmental Munificence	0.11 (2.01)*	0.09 (1.75)	0.07 (1.39)
GSCCR		0.61 (10.72)***	0.55 (9.41)***
DEC			0.18 (3.22)**
GSCCR × DEC			0.17 (3.08)**
R ²	0.08	0.45	0.51
ΔR ²	-	0.37	0.06
F-value	3.12*	18.41***	20.85***

Relationship between Green Supply Chain Cybersecurity Readiness, Supply Chain Visibility, Digital Ecosystem Complexity and Sustainability Resilience

First of all, it is essential to note that GSCCR, SCV, DEC, and SR are related in the following manner. The results presented in Table 5 and Table 6 prove that there is a positive and statistically significant relationship between GSCCR and Supply Chain Visibility ($\beta = 0.61$, $p < 0.001$). In other words, organizations that have better cybersecurity readiness are in a better position to gather, process, protect, and exchange information through the supply chain network. According to Information Processing Theory (IPT), cybersecurity readiness contributes to increasing organizational information-processing capacity as it makes sure that there are secure information flows through the supply chain. The more information can be shared and integrated through the supply chain, the more visibility can be achieved due to secure information flows, which helps supply chain participants make decisions and collaborate. Thus, cybersecurity readiness should be considered as an important strategic resource rather than only a technical one.

Second, the results presented in Table 5 and Table 6 prove that Supply Chain Visibility positively affects Sustainability Resilience ($\beta = 0.41$, $p < 0.001$). In other words, the more visible the organization, the better it identifies risks, coordinates stakeholders' activities, allocates resources, and reacts to disruptions. Higher visibility allows organizations to access relevant and up-to-date information concerning operations, inventories, suppliers, and threats, which makes organizations more resilient.

The findings are consistent with previous research proving that visibility is an important factor of supply chain resilience because it increases coordination between the supply chain partners, flexibility, and

monitoring and managing disruptions because of timely information sharing and coordinated reactions (Dey, 2023; Juan et al., 2022). From IPT perspective, visibility is an instrument of reducing uncertainty and improving decision-making. Thus, the more visibility organizations have, the more capabilities they have for keeping the balance of environmental, social, and economic sustainability objectives during disruptions.

The fact that the increment of R^2 is equal to $0.51 - 0.45 = 0.06$ proves that moderating variable explains the additional 6% of variance in visibility. Therefore, H5 is supported. Organizations operating in complex digital ecosystems benefit more from cybersecurity readiness in terms of visibility enhancement.

Table 6
Stepwise Regression for Sustainability Resilience Dependent Variable: SR

Variables	Model 1	Model 2	Model 3	Model 4
Firm Age	0.12 (2.16)*	0.10 (1.92)	0.09 (1.74)	0.08 (1.59)
Firm Size	0.06 (1.01)	0.04 (0.81)	0.03 (0.69)	0.02 (0.43)
Environmental Dynamism	0.15 (2.63)**	0.11 (2.01)*	0.09 (1.76)	0.07 (1.38)
Environmental Munificence	0.13 (2.32)*	0.10 (1.85)	0.08 (1.53)	0.07 (1.31)
GSCCR		0.56 (9.84)***	0.33 (5.61)***	0.29 (4.98)***
SCV			0.41 (7.12)***	0.35 (6.29)***
DEC			0.14 (2.58)**	0.12 (2.21)*
SCV × DEC				0.18 (3.35)**
R^2	0.09	0.43	0.58	0.63
ΔR^2	-	0.34	0.15	0.05
F-value	3.58*	16.74***	23.52***	27.11***

Additionally, the results imply that GSCCR significantly impacts Sustainability Resilience ($\beta = 0.56$, $p < 0.001$). This suggests that organisations capable of maintaining cybersecurity readiness can continue their operations sustainably by absorbing disruptive effects and recovering from them. Since digitalisation exposes organisations to cyber-attacks that can disrupt production processes, environmental information systems, logistics, and sustainability goals, it is necessary to be ready for these threats to maintain resilience and sustainability. Thus, the results support Kanaan et al. (2025) that digital risk management and cybersecurity capabilities contribute to organisational resilience and sustainability. The result is consistent with IPT, which implies that organisations operating in uncertain environments need strong information-processing capabilities to reduce vulnerability and manage risks. In this case, the explanatory power of the model increases from $R^2 = 0.58$ in Model 3 to $R^2 = 0.63$ in Model 4. Therefore, H6 is supported. The benefits of visibility for resilience become stronger in highly complex digital ecosystems.

The findings also show that Supply Chain Visibility positively influences Sustainability Resilience ($\beta = 0.41, p < 0.001$). The result indicates that organisations with high visibility have more opportunities to recognise risks, coordinate stakeholder activities, manage resources, and react to disruptions proactively. Visibility gives access to accurate information about operational activities, inventories, supplier performance, and risks. This result is consistent with previous research, where visibility was identified as one of the critical determinants of resilience due to its coordination and flexibility properties (Dey, 2023; Juan et al., 2022). From the perspective of Information Processing Theory, visibility helps reduce uncertainty and improve decision-making. Thus, organisations with high visibility are capable of maintaining their environmental, social, and economic sustainability goals during periods of disruption. The explanatory power of the model increases from $R^2 = 0.58$ in Model 3 to $R^2 = 0.63$ in Model 4. Therefore, H6 is supported. The benefits of visibility for resilience become stronger in highly complex digital ecosystems.

Additionally, the moderating results indicate that Digital Ecosystem Complexity positively affects the relationship between GSCCR and Supply Chain Visibility ($\beta = 0.17, p < 0.01$). This means that cybersecurity readiness becomes more valuable when the organisation operates in a highly complex digital ecosystem. Since the organisation faces increasing interdependencies between stakeholders, information exchange, and technology integration, there is a need for advanced cybersecurity infrastructure. This result supports the arguments of Wang (2021), who claims that the complexity of the digital ecosystem increases information processing requirements, making digital capabilities valuable for coordinating actors, integrating knowledge, and managing interdependencies within the innovation ecosystem. Thus, the finding shows that organisations operating in highly complex digital ecosystems gain more visibility benefits from cybersecurity readiness than organisations operating in low-complexity environments.

Similar to the previous result, the Digital Ecosystem Complexity positively affects the relationship between Supply Chain Visibility and Sustainability Resilience ($\beta = 0.18, p < 0.01$). This result shows that visibility is more beneficial to resilience under conditions of high digital complexity. With the development of stakeholder networks and information flows, the organisations become more dependent on visibility capabilities for coordination and adaptation. The result is consistent with Information Processing Theory since organisations facing high complexity require a higher level of information accessibility and processing capabilities. This result is consistent with the previous research indicating that the complexity of the ecosystem serves as a significant contextual condition for resilience since it emerges from the interaction of various technological, organisational, and environmental factors, not from capabilities. Consequently, the value of digital capabilities depends on their configuration in the innovation ecosystem (Wang et al., 2025).

Bootstrapped Mediation Results

Table 7. Indirect Effects

Path	Indirect Effect	SE	LLCI	ULCI
GSCCR → SCV → SR	0.25***	0.05	0.15	0.37

Direct Effects

Path	Effect	SE	LLCI	ULCI
GSCCR → SR	0.33***	0.06	0.20	0.45

Mediating Role of Supply Chain Visibility

Table 7 depicts the mediated relationship between Green Supply Chain Cybersecurity Readiness and Sustainability Resilience, with Supply Chain Visibility acting as a mediating factor. The mediation analysis reveals that the indirect impact of GSCCR on Sustainability Resilience via Supply Chain Visibility is significant ($\beta = 0.25$, LLCI = 0.15, ULCI = 0.37). The results of the analysis show that, in addition to making a direct contribution to resilience, cybersecurity readiness can also contribute indirectly via increased visibility. Specifically, the indirect impact reveals that high cybersecurity readiness creates opportunities for information exchange, cooperation, and increased transparency. As a result, organisations can detect potential disruptions earlier, better coordinate their supply chain operations, and preserve their sustainability-related objectives during adverse situations. At the same time, the direct effect of GSCCR on Sustainability Resilience remains statistically significant ($\beta = 0.33$), thus proving partial mediation.

The mediation analysis provides evidence in favour of the theoretical proposition made by Information Processing Theory that organisational capabilities impact performance outcomes through mechanisms that facilitate the use of information. Similarly to Rashid et al. (2024), the role of visibility is revealed as one of the most important mechanisms that make it possible for information processing capabilities to have effects on organisational resilience since visibility makes it possible to collect information, narrow down information gaps, enhance risk management, and resilience during disruptive events. Thus, Supply Chain Visibility acts as one of the most important dynamic capabilities facilitating transformation of cybersecurity readiness into sustainable resilience outcomes.

Overall, the findings of the research demonstrate that the sustainable resilience of organisations operating in the digital supply chain cannot be achieved only through cybersecurity investments. Organisations achieve resilience when cybersecurity investments help them gain visibility and information management capabilities.

Importance–Performance Map Analysis (IPMA)

Target Construct: Sustainability Resilience (SR)

Construct	Importance	Performance
GSCCR	0.56	74.8
SCV	0.41	78.1
DEC	0.14	69.4

The GSCCR has the largest importance score of 0.56, which means that it is the most important predictor of Sustainability Resilience. The SCV variable comes second in terms of importance (0.41), whereas the least important variable is the DEC (0.14). In terms of management, strengthening cybersecurity will create the biggest impact on sustainability resilience.

IPMA Matrix

High Importance	High Performance
GSCCR (0.56; 74.8)	SCV (0.41; 78.1)
Low Importance	Lower Performance
DEC (0.14; 69.4)	DEC (0.14; 69.4)

Hypothesis Summary

Hypothesis	Relationship	β	Result
H1	GSCCR $\rightarrow$ SR	0.56***	Supported
H2	GSCCR $\rightarrow$ SCV	0.61***	Supported
H3	SCV $\rightarrow$ SR	0.41***	Supported
H4	GSCCR $\rightarrow$ SCV $\rightarrow$ SR	0.25***	Supported
H5	GSCCR $\times$ DEC $\rightarrow$ SCV	0.17**	Supported
H6	SCV $\times$ DEC $\rightarrow$ SR	0.18**	Supported

The moderation graph shows that Digital Ecosystem Complexity strengthens the positive relationship between GSCCR and SCV. With low levels of DEC, there is an improvement in GSCCR and moderate levels of SCV. However, with high levels of DEC, the slope becomes very steep, signifying a stronger positive relationship. This shows that the significance of cyber security readiness increases in achieving SCV in complex digital ecosystems.

Figure 2 shows how the correlation between Supply Chain Visibility and Sustainability Resilience strengthens as DEC increases. When DEC is low, visibility adds positively to resilience but in a smaller way. When DEC is high, the correlation gets much stronger, meaning that visibility creates greater resilience value when complexity increases across information, stakeholders, and technology interactions. This supports the idea that visibility is especially important in complex digital ecosystems, as organisations need to handle massive amounts of data and many stakeholders. Therefore, DEC improves the effectiveness of visibility in constructing Sustainability Resilience, hence supporting H6.

Discussion

In this way, the results of the current research reveal that GSCCR positively influences SR and SCV. In particular, GSCCR is a vital precondition for securing information flow, promoting information exchange, and increasing supply chain network transparency. Within the framework of Information Processing Theory, cybersecurity readiness can be considered a key information processing capability necessary for the successful acquisition, protection, and distribution of information under uncertainty. Thus, the results are consistent with the theory that information processing mechanisms are important for organisations operating in a digitally connected environment, as they help organisations reduce uncertainty and achieve higher resilience performance (Galbraith, 1973; Yu et al., 2022). In addition, the findings are supported by previous research on the impact of cybersecurity capabilities and digital information processing mechanisms on improving supply chain resilience, risk management, and organisational flexibility in highly dynamic settings (Rashid et al., 2024; Herburger et al., 2024; Kanaan et al., 2025). The positive effect of GSCCR on SCV supports the hypothesis that cybersecurity-ready organisations can generate timely, reliable, and accurate information that increases visibility within supply chains and allows for more efficient coordination among supply chain partners.

In addition, the results show that SCV has a positive effect on SR and partially mediates the relationship between GSCCR and Sustainable Resilience. The results imply that not only cybersecurity readiness but also enhanced visibility contributes to the development of organisations' resilient abilities. As a result of increased visibility, organisations can detect threats, monitor disruptions, collaborate in negative situations, and sustain business operations in the face of unexpected events. In addition, the findings support previous research, which suggests that enhancing SCV helps organisations increase preparedness, responsiveness, and recovery capabilities by enabling real-time information use and collaborative decision-making (Dey, 2023; Kalaiarasan et al., 2022; Rashid et al., 2024). Moreover, the moderating effect of Digital Ecosystem Complexity shows that the positive impact of cybersecurity readiness and visibility becomes even more apparent as digital ecosystems become increasingly interconnected and technologically advanced. The result supports Information Processing Theory, which holds that increasing environmental complexity requires enhancing an organisation's information-processing ability to ensure effective organisational operation (Galbraith, 1973; Yu et al., 2022). The results show how the principles of Information Processing Theory can be applied to understand how cybersecurity readiness, visibility, and digital ecosystem complexity affect the development of

sustainable organisational resilience. In addition, the findings can contribute to existing research on digital transformation, cybersecurity, and resilience. Information-related capabilities become crucial in the context of the Industry 5.0 era (Sjödín et al., 2022; Tyagi & Tyagi, 2025; Padovano & Ivanov, 2025).

Implications for theory

These findings make several theoretical contributions to the literature of digital supply chains, cybersecurity, and organisational resilience. First, the paper advances Information Processing Theory (IPT) by showing that Green Supply Chain Cybersecurity Readiness (GSCCR) can serve as an essential information-processing capability that leads to improved Supply Chain Visibility and Sustainability Resilience. Although many IPT-related papers concentrate on information-sharing, coordination and risk-management practices, the present research adds a new dimension by considering cyber readiness as an ability to manage uncertainty and obtain sustainable organisational benefits.

Secondly, the paper contributes to the resilience literature by showing that Supply Chain Visibility acts as a crucial mediator through which the impact of GSCCR on sustainability resilience is delivered. The mediation effect shows that the value created by cybersecurity readiness capabilities becomes more apparent due to increased information accessibility, transparency, and coordination. Thirdly, the paper contributes to the nascent field of digital ecosystems by identifying the moderating effect of Digital Ecosystem Complexity. It has been shown that the influence of cybersecurity readiness and visibility is significantly amplified in highly connected and technology-advanced environments. Thus, Digital Ecosystem Complexity can be considered as a new boundary condition for the IPT model and a new moderated-mediation approach to sustainable digital supply chain management.

Implications for practice

The implications can be summarised as follows. Firstly, managers should realise that the Green Supply Chain Cybersecurity Readiness (GSCCR) is not only a technical or regulatory responsibility but also a strategic tool that improves sustainability resilience and supply chain visibility. Thus, organisations are recommended to invest in cybersecurity infrastructure development, employee education programs, threat identification systems, and information exchange platforms to protect sensitive data.

Secondly, organisations are suggested to consider Supply Chain Visibility development as one of the main tools through which cybersecurity readiness leads to sustainability resilience. Companies need to create digital monitoring systems, real-time information-sharing platforms, and collaborative technologies to increase transparency and speed of response to disruptions. Improved visibility helps to process information and coordinate stakeholders' actions to operate sustainably despite crises. Thirdly, managers working in complex digital ecosystems need to focus on cybersecurity readiness and visibility development. As the results show, these resources gain additional importance as Digital Ecosystem Complexity grows.

Conclusion

In this research paper, the focus was on the association between Green Supply Chain Cybersecurity Readiness (GSCCR), Supply Chain Visibility (SCV), Digital Ecosystem Complexity (DEC), and Sustainability Resilience (SR). Applying Information Processing Theory, the research proved that cybersecurity readiness is an important organisational resource that contributes to SCV and SR. According to the results obtained, GSCCR has a positive impact on SCV and SR. In turn, SCV positively influences SR. In addition, the results show that SCV partially mediates the relationship between GSCCR and Sustainability Resilience, meaning that organisations use information processing capabilities to convert cybersecurity resources into resilience outcomes by enhancing information availability. The study also found that DEC increases the impact of GSCCR on SCV and of SCV on SR. All in all, the results of the current research can be used by organisations to increase sustainable resilience by using cybersecurity readiness, visibility capabilities, and managing digital ecosystems.

Limitations and future directions

There are some limitations associated with this study that need to be taken into account when analysing its results. Firstly, it is not possible to determine any causal connections between GSCCR, SCV, DEC, and SR because the research was conducted using a cross-sectional approach. Further research may use a longitudinal methodology to analyse how these connections change over time. Secondly, the results obtained using the self-reporting method may be subject to perceptual and common method biases, even with the application of the measurement procedure and validated scales. Thirdly, since the study was limited to the organisations implementing digitalised supply chain systems, its findings may not be generalised to less digitally mature firms. Finally, this research was limited to the analysis of the only mediator and moderator of interest (Supply Chain Visibility and Digital Ecosystem Complexity, respectively). Further research should explore other organisational capabilities, environmental factors, and technologies affecting sustainability resilience in supply chain ecosystems.

Declarations

Conflict of Interest Statement: The authors have no potential conflicts of interest.

Ethics approval: This study was reviewed and approved by the Institutional Review Board (IRB) of Tamale Technical University under approval code TaTU/IRB/DM/2026/018. The study was conducted in accordance with the Declaration of Helsinki and the Belmont Report.

Consent to participate: Informed consent was obtained from all participants involved in the study.

Funding: Not Applicable.

Availability of Data: Data will be made available upon request.

Acknowledgements: Not Applicable.

Consent to Publish: Not Applicable

Author Contribution

M. M conceptualized the idea of the research.A. G.H wrote the main manuscript text and collect dataM.
A. Z prepared figures and tablesAll authors reviewed the manuscript

References

1. Ahmadi T, Hesarakı AF, Morsch JPM. Exploring IT-driven supply chain capabilities and resilience: The roles of supply chain risk management and complexity. *Supply Chain Management: Int J*. 2025;30(1):50–66. <https://doi.org/10.1108/SCM-11-2023-0561>.
2. Aljohani A. Predictive analytics and machine learning for real-time supply chain risk mitigation and agility. *Sustainability*. 2023;15(20):15088. <https://doi.org/10.3390/su152015088>.
3. Al-Khatib AW. The impact of industrial Internet of Things on sustainable performance: The indirect effect of supply chain visibility. *Bus Process Manage J*. 2023;29(5):1607–29. <https://doi.org/10.1108/BPMJ-03-2023-0198>.
4. Bednarski L, Roscoe S, Blome C, Schleper MC. Geopolitical disruptions in global supply chains: A state-of-the-art literature review. *Prod Plann Control*. 2025;36(4):536–62. <https://doi.org/10.1080/09537287.2023.2286283>.
5. Bellamy MA, Dhanorkar S, Subramanian R. Administrative environmental innovations, supply network structure, and environmental disclosure. *J Oper Manag*. 2020;66(7–8):895–932. <https://doi.org/10.1002/joom.1114>.
6. Chi K, Yan F, Zhang C, Wang J. Research on the construction process of supply chain ecosystem led by digital platform enterprises from the perspective of dynamic capability. *Supply Chain Management: Int J*. 2024;29(6):1019–41. <https://doi.org/10.1108/SCM-03-2024-0208>.
7. Dey S. Surviving major disruptions: Building supply chain resilience and visibility through rapid information flow and real-time insights at the edge. *Sustainable Manuf Service Econ*. 2023;2:100008. <https://doi.org/10.1016/j.smse.2022.100008>.
8. Emon MMH, Khan T. Unlocking sustainability through supply chain visibility: Insights from the manufacturing sector of Bangladesh. *Brazilian J Oper Prod Manage*. 2024;21(4):e20242194. <https://doi.org/10.14488/BJOPM.2194.2024>.
9. Feng T, Qamruzzaman M, Sharmin SS, Karim S. Bridging environmental sustainability and organisational performance: The role of green supply chain management in the manufacturing industry. *Sustainability*. 2024;16(14):5918. <https://doi.org/10.3390/su16145918>.
10. George AS, Baskar T, Balaji Srikanth P. Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. *Partners Univers Int Innov J*. 2024;2(1):51–75. <https://doi.org/10.5281/zenodo.10639463>.
11. Goswami SS, Sarkar S, Gupta KK, Mondal S. The role of cyber security in advancing sustainable digitalisation: Opportunities and challenges. *J Decis Analytics Intell Comput*. 2023;3(1):270–85. <https://doi.org/10.31181/jdaic10018122023g>.

12. Herburger M, Wieland A, Hochstrasser C. Building supply chain resilience to cyber risks: A dynamic capabilities perspective. *Supply Chain Management: Int J.* 2024;29(7):28–50.
<https://doi.org/10.1108/SCM-01-2023-0016>.
13. Joussen TP, Kanbach DK, Kraus S. Enabling strategic change toward resilience: A systematic review from a dynamic capabilities perspective. *Strategic Change.* 2025;34(3):373–405.
<https://doi.org/10.1002/jsc.2626>.
14. Juan S-J, Li EY, Hung W-H. An integrated model of supply chain resilience and its impact on supply chain performance under disruption. *Int J Logistics Manage.* 2022;33(5):1535–64.
<https://doi.org/10.1108/IJLM-03-2021-0174>.
15. Kalaiarasan R, Olhager J, Agrawal TK, Wiktorsson M. The ABCDE of supply chain visibility: A systematic literature review and framework. *Int J Prod Econ.* 2022;248:108464.
<https://doi.org/10.1016/j.ijpe.2022.108464>.
16. Kanaan A, Al-Hawamleh A, Aloun M, Alorfi A, Alrawashdeh MA. Fortifying organisational cyber resilience: An integrated framework for business continuity and growth amidst an escalating threat landscape. *Int J Comput Digit Syst.* 2025;17(1):1–14. <https://doi.org/10.12785/ijcds/1571023809>.
17. Kumar S, Anbanandam R. (2020). Impact of risk management culture on supply chain resilience: An empirical study from Indian manufacturing industry. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 234(2), 246–259.
<https://doi.org/10.1177/1748006X19886718>
18. Layode O, Naiho HNN, Labake TT, Adeleke GS, Udeh EO, Johnson E. Addressing cybersecurity challenges in sustainable supply chain management: A review of current practices and future directions. *Int J Manage Entrepreneurship Res.* 2024;6(6):1954–81.
<https://doi.org/10.51594/ijmer.v6i6.1208>.
19. Li Y, Sukhotu V. Enhanced digital capabilities for building resilient supply chains: Exploring visibility, collaboration, and resilience in China's electric vehicle industry. *World Electr Veh J.* 2025;16(2):63.
<https://doi.org/10.3390/wevj16020063>.
20. Luo Y. A general framework of digitisation risks in international business. *J Int Bus Stud.* 2022;53(2):344–61. <https://doi.org/10.1057/s41267-021-00448-9>.
21. Mahim MMH, Mallik SK, Mahadi SKMI. Dynamic capabilities and cyber resilience in supply chain management: Insights from case studies across Asia. *Am J Social Dev Entrepreneurship.* 2025;4(1):111–21. <https://doi.org/10.54536/ajsde.v4i1.5037>.
22. Metwally ABM, Ali HAA, Aly SAS, Ali MAS. The interplay between digital technologies, supply chain resilience, robustness and sustainable environmental performance: Does supply chain complexity matter? *Sustainability.* 2024;16(14):6175. <https://doi.org/10.3390/su16146175>.
23. Miceli A, Hagen B, Riccardi MP, Sotti F, Settembre-Blundo D. (2021). Thriving, not just surviving in changing times: How sustainability, agility and digitalisation intertwine with organisational resilience. *Sustainability*, 13(4), 2052. <https://doi.org/10.3390/su13042052>

24. Mikalef P, Pateli A, van de Wetering R. IT architecture flexibility and IT governance decentralisation as drivers of IT-enabled dynamic capabilities and competitive performance: The moderating effect of the external environment. *Eur J Inform Syst.* 2021;30(5):512–40.
<https://doi.org/10.1080/0960085X.2020.1808541>.
25. Nnabueze SB, Ike PN, Olatunde-Thorpe J, Aifuwa SE, Oshoba TO, Ogbuefi E, Akokodaripon D. End-to-end visibility frameworks: Improving transparency, compliance, and traceability across complex global supply chain operations. *Int J Multidisciplinary Futuristic Dev.* 2021;2(2):50–60.
<https://doi.org/10.54660/IJMFD.2021.2.2.50-60>.
26. Okolo FC, Etukudoh EA, Ogunwole O, Osho GO, Basiru JO. Systematic review of cyber threats and resilience strategies across global supply chains and transportation networks. *Iconic Res Eng Journals.* 2021;4(9):204–17.
27. Onukwulu EC, Agho MO, Eyo-Udo NL. Framework for sustainable supply chain practices to reduce carbon footprint in energy. *Open Access Res J Sci Technol.* 2021;1(2):12–34.
<https://doi.org/10.53022/oarjst.2021.1.2.0032>.
28. Oyeboode O. Blockchain-anchored reinforcement learning collectives with tokenised ecosystem optimisation for trustless, bias-free adaptation of complex systems. *Int J Adv Res Publication Reviews.* 2025;2(8):698–720.
29. Padovano A, Ivanov D. Towards resilient and viable supply chains: A multidimensional model and empirical analysis. *Int J Prod Res.* 2025;63(17):6252–90.
<https://doi.org/10.1080/00207543.2025.2470350>.
30. Park SK. Legal strategy disrupted: Managing climate change and regulatory transformation. *Am Bus Law J.* 2021;58(4):711–49. <https://doi.org/10.1111/ablj.12199>.
31. Rashid A, Rasheed R, Ngah AH, Jayaratne MDRP, Rahi S, Tunio MN. (2024). Role of information processing and digital supply chain in supply chain resilience through supply chain risk management—Journal of Global Operations and Strategic Sourcing. Advance online publication. <https://doi.org/10.1108/JGOSS-12-2023-0106>
32. Razak GM, Hendry LC, Stevenson M. Supply chain traceability: A review of the benefits and its relationship with supply chain resilience. *Prod Plann Control.* 2023;34(11):1114–34.
<https://doi.org/10.1080/09537287.2021.1983661>.
33. Setyadi A, Pawirosumarto S, Damaris A. Toward a resilient and sustainable supply chain: Operational responses to global disruptions in the post-COVID-19 era. *Sustainability.* 2025;17(13):6167. <https://doi.org/10.3390/su17136167>.
34. Seyi-Lande OB, Layode O, Naiho HNN, Adeleke GS, Udeh EO, Labake TT, Johnson E. Circular economy and cybersecurity: Safeguarding information and resources in sustainable business models. *Finance Acc Res J.* 2024;6(6):953–77. <https://doi.org/10.51594/farj.v6i6.1214>.
35. Sjödin D, Parida V, Visnjic I. How can large manufacturers digitalise their business models? A framework for orchestrating industrial ecosystems. *Calif Manag Rev.* 2022;64(3):49–77.
<https://doi.org/10.1177/00081256211059140>.

36. Statsenko L, Jayasinghe RS, Soosay C. Supply network resilience capabilities: A social–ecological perspective. *Supply Chain Management: Int J.* 2024;29(1):1–26. <https://doi.org/10.1108/SCM-11-2022-0438>.
37. Tarigan MK, Simatupang TM, Bangun YR. Building resilience through digital transformation: A systematic literature review and comprehensive framework for large enterprises. *Int J Bus Innov Res.* 2025;36(5):1–28. <https://doi.org/10.1504/IJBIR.2025.10070413>.
38. Tran TTN, Do AD, Nguyen MN. Supply chain digitalisation and performance: The serial mediation of visibility and resilience. *Emerg Sci J.* 2026;10(2):742–59. <https://doi.org/10.28991/ESJ-2026-010-02-08>.
39. Tsolakis N, Schumacher R, Dora M, Kumar M. Artificial intelligence and blockchain implementation in supply chains: A pathway to sustainability and data monetisation? *Ann Oper Res.* 2023;327:157–210. <https://doi.org/10.1007/s10479-022-04785-2>.
40. Tyagi M, Tyagi K. Industry 5.0 readiness factors for implementing digital twins in sustainable supply chains: A pathway to circularity. *J Clean Prod.* 2025;529:146795. <https://doi.org/10.1016/j.jclepro.2025.146795>.
41. Ullah M, Zahid M, Rizvi SMA-R, Qureshi QGM, Ali F. (2022). Do green supply chain management practices improve organisational resilience during the COVID-19 crisis? A survival analysis of global firms.
42. Wang P. Connecting the parts with the whole: Toward an information ecology theory of digital innovation ecosystems. *MIS Q.* 2021;45(1):397–422. <https://doi.org/10.25300/MISQ/2021/15864>.
43. Wang Y, Xiao J, Xu Z. Digital transformation drives regional innovation ecosystem resilience: A study based on the dynamic QCA method. *Sustainability.* 2025;17(18):8148. <https://doi.org/10.3390/su17188148>.
44. Xu H, Zheng H, Sun D, Wang M, Ye C. An integrated framework for enablers in supply chain resilience: Model development and analysis. *IEEE Access.* 2024;12:42490–508. <https://doi.org/10.1109/ACCESS.2024.3379212>.
45. Yu W, Chavez R, Jacobs MA, Wong CY. Openness to technological innovation, supply chain resilience and operational performance: Exploring the role of information processing capabilities. *IEEE Trans Eng Manage.* 2022;71:1258–70. <https://doi.org/10.1109/TEM.2022.3156531>.
46. Zolkafli UK, AlArabi A. Enhancing cybersecurity readiness in express logistics: The role of cyber-attack features and project team skills. *Acta Logistica.* 2025;12(3):571–94. <https://doi.org/10.22306/al.v12i3.691>.

Figures

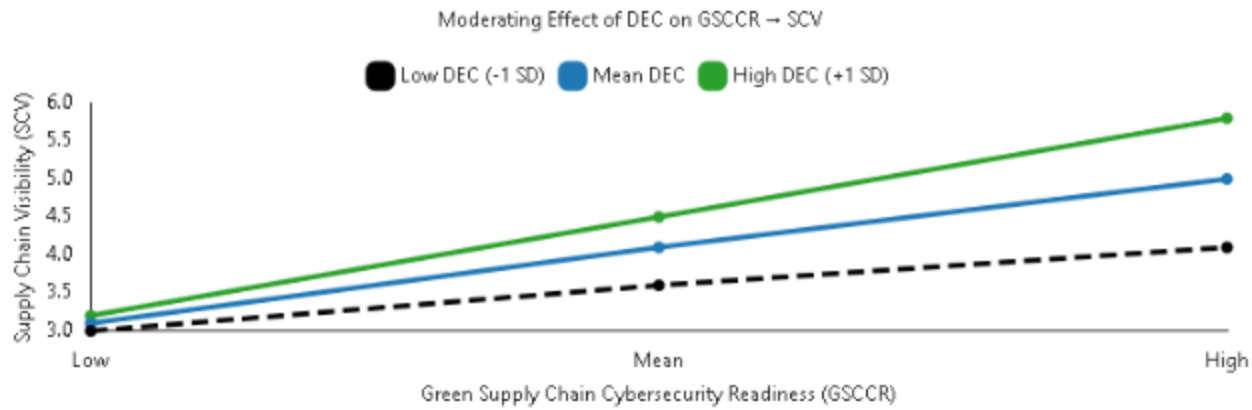


Figure 1

H5: Moderating Effect of Digital Ecosystem Complexity (DEC) on the GSCCR → SCV Relationship

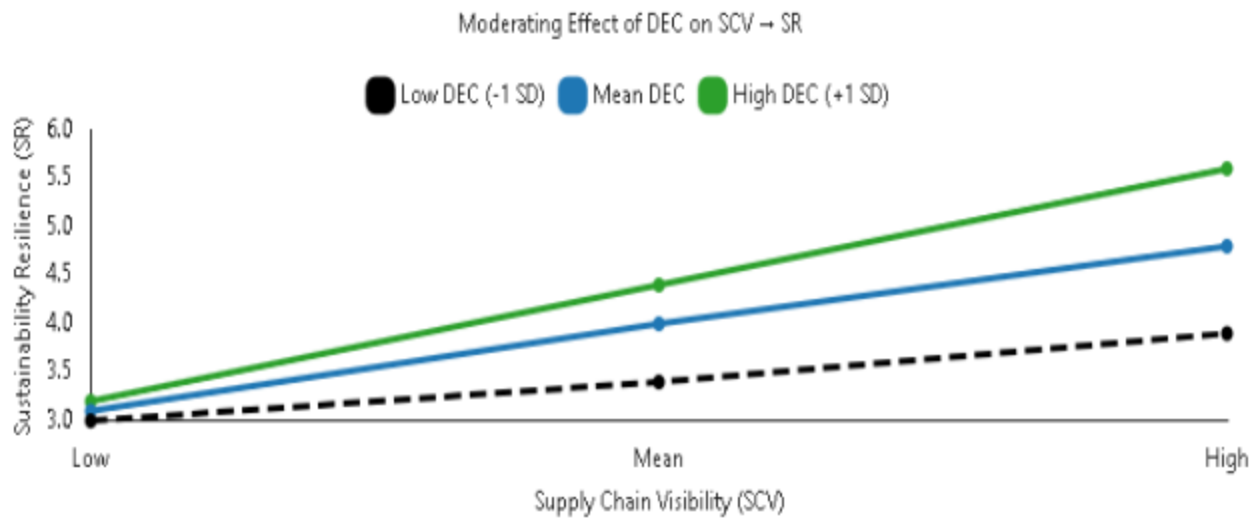


Figure 2

H6: Moderating Effect of Digital Ecosystem Complexity (DEC) on the SCV → SR Relationship

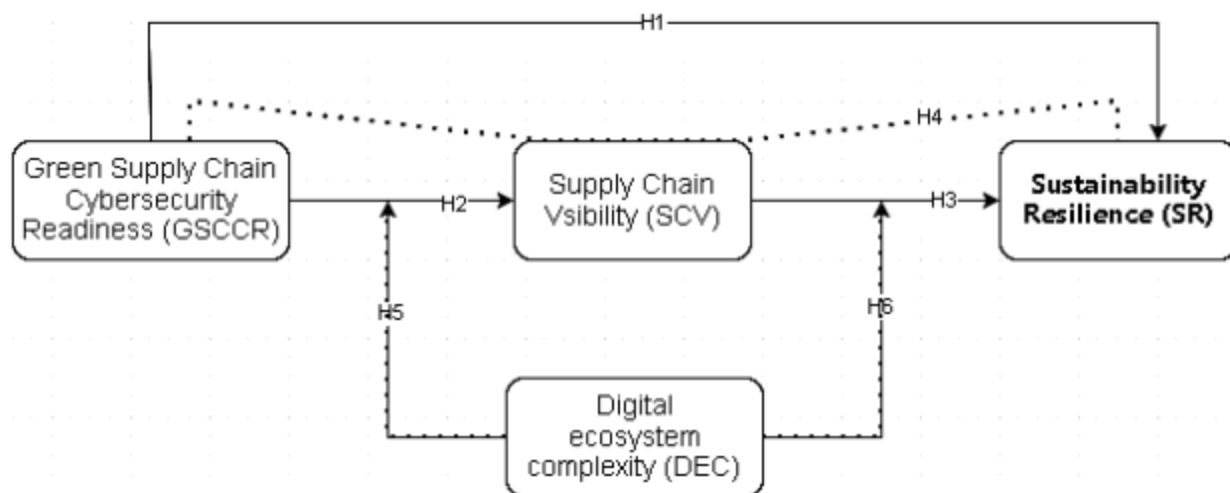


Figure 3

Unnumbered image in the Literature Review and Theoretical Support section.

Conceptual Framework