Print ISSN: 1738-3110 / Online ISSN 2093-7717
JDS website: http://www.accesson.kr/jds
http://doi.org/10.15722/jds.23.01.202501.1

Examining the influence of Organizational Security Culture on Supply Chain Disruption Occurrence: The Mediating Role of Supply Chain Security Practices

James Peprah ADU[1], Nirmala DORASAMY[2]

Received: August 20, 2024. Revised: November 01, 2024. Accepted: January 05, 2025.

Abstract

Purpose: This study investigates the relationship between organizational security culture and supply chain disruptions, and examines the mediating role of supply chain security practices in mitigating disruptions. **Methodology:** A quantitative approach was employed, surveying 350 managers from Ghana's manufacturing and service sectors. Structural Equation Modeling (SEM) analyzed the relationships between organizational security culture, supply chain security practices (information management security, facility management security, and human resource security), and supply chain disruptions. **Results:** The study reveals that a robust organizational security culture has a profound impact on supply chain security practices, resulting in a substantial reduction in supply chain disruptions. Specifically, facility management security and information management security emerge as critical mediators, significantly influencing this relationship. Conversely, human resource security does not have a statistically significant impact. **Conclusion:** This study contributes to the supply chain security management literature, highlighting the importance of organizational security culture in mitigating supply chain disruptions. The findings provide valuable insights for managers and policymakers seeking to enhance supply chain resilience in emerging economies. The study emphasizes the need to integrate organizational security culture and supply chain security practices. Managers should prioritize building a strong security culture, allocate resources for effective supply chain security practices, and promote employee awareness.

Keywords: Human Resource Security#1, Information Management Security#2, Organizational Security Culture#3, Supply Chain Disruptions#4, Supply Chain Security Practices#5

JEL Classification Code: D23, R31, L15, O15

1. Introduction

Supply chain (SC) disruptions have increasingly affected organizations, leading to financial losses and operational challenges (Scholten & Fynes, 2016; Hendriks & Singhal, 2016). Factors such as natural disasters, cyberattacks, political instability, and supplier failures have heightened the complexity and global nature of SCs, raising the likelihood of interruptions (Hallin & Höök, 2023; Wieteska, 2018). As a result, businesses face significant pressure to enhance their SC resilience and develop strategies to mitigate these risks (Ali et al., 2021). Despite

1 Corresponding Author Department of Management Science, Faculty of Management Science, Durban University of Technology, Greyville, Durban, 4001, South Africa. Email: jamespeprah2000@gmail.com
2 Department of Public Management and Economics, Faculty of Management Science, Durban University of Technology, Greyville, Durban, 4001, South Africa. Email: nirmala@dut.ac.za

ⓒ Copyright: The Author(s)
This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://Creativecommons.org/licenses/by-nc/4.0/) which permits unrestricted noncommercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

widespread research on SC resilience, the effect of structural security culture on mitigating SC disruptions remains underexplored. This culture, which includes collective values and attitudes toward information security, plays a critical role in promoting effective safety practices and enhancing resilience (Asamoah et al., 2021; Al Izki, 2019). Given that SCs require the exchange of sensitive information among various stakeholders, a strong security culture is vital. Weaknesses in security culture can increase risks, such as data breaches and cyberattacks, potentially disrupting SC operations (Ghadge et al., 2019).

In addition, supply chain security practices are critical to minimizing the risks associated with disruptions. Within the SC there are numerous acts of surveillance designed to maintain the capacity, privacy, and ability to obtain data and physical assets. The effectiveness of these practices is determined by the culture of institutional security, which can promote compliance with protocols and the rapid communication of possible incidents. Though, new studies look at the association amid structural safety philosophy and CS disruptions, chiefly through the lens of CS care practices, are incomplete. The existing works has engrossed, above all, the straight effects of safety does on the performance of C, as well as the role of organizational culture in determining these practices (Tolah et al., 2021). This blows tourist attractions the need for additional investigate into how a strong safety culture can improve the efficiency of SC safety does and alleviate disturbances.

Supply chain security does (SC Security Practices) are critical to minimalizing the risks related with SC disturbances (Park et al., 2016). These practices include a wide range of security measures and protocols designed to protect the ability to obtain data and physical assets, strict access control mechanisms, specific risk assessment procedures, specific incident response plans, and extensive personnel training programs (DuHadway et al., 2017). The effectiveness of the SC's security practices has a major impact on the institution's overall security culture. A strong safety culture promotes an environment where workers adhere to safety protocols and report safety incidents, improving the overall effectiveness of these practices. Equally, a poor care ethos deteriorates the application and efficiency of SC safety does, cumulative the risk of outages.

Despite the importance of organizational security culture, there are no concrete empirical studies to analyze the impact of disruptions on CS, particularly through the lens of CS security practices (Autry & Bobbitt, 2008). Previous studies are based, above all, on the direct impact of security practices on the performance or resilience of CS security practices (Yang and Hsu, 2018; Nissen et al., 2018; Jonsen, 2016), often forgetting the role of organizational culture in shaping these practices. In addition, the existing literature tends to concentrate on specific security practices, such as information security, physical security, or human security, without taking into account the holistic impact of an organization's security culture on CS security practices (Zailani et al., 2015; Yang & Wei, 2013; Li, 2013). This fragmented approach fails to achieve the relationships and interdependencies between security practices in the context of CS.

In addition, the mechanisms influencing the idea of CS pauses are understood in a limited way. While some studies have examined how SC security practices influence the relationship between risk-taking propensity and SC disruption occurrence, empirical evidence exploring the arbitrating role of SC security practices in the context of SC disruptions is scarce. To address these gaps, this study employs both dynamic capability and contingency perspectives to examine the influence of organizational security culture on SC disruption occurrence, focusing particularly on the mediating role of SC security practices. By integrating these theoretical perspectives, the research aims to provide a comprehensive understanding of in what way a robust structural safety philosophy can enhance the effectiveness of SC security practices, thereby mitigating SC disruptions. To achieve these objectives, the study aims to answer the following research questions:

RQ1: What is the influence of organizational security culture on the occurrence of SC disruptions?

RQ2: To what extent do SC security practices mediate the relationship between organizational security culture and SC disruption occurrence?

This research attempts to give empirical evidence on the relationship among supply chain security practices, organisational security culture, and supply chain disruption occurrence by addressing these research questions. The results have the potential to improve supply chain resilience and reduce disruption risks through the development of policies, resource allocation decisions, and organisational initiatives. The rest of the paper is organised as follows: A survey of the pertinent theories and concepts is given in Section 2 of the literature. The study's methodology, which includes information on data collection, measurements, and analytical methods, is described in Section 3. The empirical findings derived from the data analysis are then presented in Section 4. Lastly, the conclusion section addresses the results, theoretical and practical ramifications, study limitations, and recommendations for additional study in this domain.

1.1. Research Gap

The existing literature on organizational safety culture and supply chain disruptions reveals significant findings but also highlights critical research gaps. Notably, there is a

scarcity of empirical studies investigating the relationship between organizational safety culture and the mitigation of supply chain disruptions. Furthermore, few studies have explored the mediating role of supply chain security practices within this context. These gaps emphasize the necessity for further exploration.

Building on this foundation, this study aims to address these research gaps by examining two primary research questions:

i. What impact does organizational safety culture have on supply chain disruptions?
ii. To what extent do supply chain safety practices mediate the relationship between organizational safety culture and the occurrence of supply chain disruptions?

The goal of this research is to understand how a strong safety culture can improve resilience to supply chain disruptions, ultimately improving operational efficiency and risk management.

1.2. The importance of organizational security culture in mitigating supply chain disruptions

The importance of organizational security culture in mitigating supply chain disruptions cannot be overstated. A strong security culture protects against cyberattacks, data breaches, and intellectual property theft, while ensuring obedience with manufacturing regulations and standards. It promotes worker consciousness and care, strengthens supply chain pliability, and improves business continuity. In addition, it helps to minimize reputational damage and financial wounded. By ordering safety culture, entities can effectively alleviate risks associated with supply chain disturbances, improve relations and message with dealers, improve risk management capabilities, and protect long-term sustainability. This highlights the critical role that the ethos of structural safety plays under the defence of source chains.

2. Literature Review

2.1. Key Concepts

The works review efficiently defines the vital concepts needed to understand the relationship between structural safety culture and supply chain disturbances.

2.2. Definition of Key Terms

Structural Safety Culture: This period refers to the collective values, attitudes, and practices within an group that prioritize safety and actively mitigate risks. A strong safety culture promotes an setting where safety is a shared accountability among all workers.

Supply chain pliability: Supply chain pliability is a supply chain's ability to cope with, adapt to, and recover from outages. This competence assurances the continuity of operations and, at the same time, reduces the effect of the unexpected facts.

Supply cable disruptions: These are unexpected events or circumstances that suspend the ordinary operations of a supply chain, which can cause financial losses, reputational injury, or stoppage.

Security practices: Gather source chain possessions against threats, theft, or other safety breaches, applied data defence events, and operations. Effective safety does are critical to upholding the uprightness and flexibility of source manacles.

By founding these senses, the review brings a fundamental sympathetic to analyze how organizational safety culture influences supply chain pliability and give to mitigating turbulences.

2.3. Relationship Between Security Culture, Supply Chain Practices, and Disruption Mitigation

2.3.1. Encouraging Collaborative Risk Management

Co-operative risk organisation is an vital component of a strong care culture, which indorses a proactive vision to identify and mitigate possible threats. This procedure involves distribution danger intellect among investors, leading joint risk valuations to find susceptibilities, and developing eventuality plans that advantage all parties involved in treatment possible disturbances. In addition, collaborative risk administration recovers source chain visibility, allowing stakeholders to monitor in real-time and respond to risks. By indorsing collaboration, a robust safety culture protections that all investors work together to identify and alleviate risks, thus reducing the probability of turbulences and increasing supply chain flexibility.

Eventually, a strong safety culture fosters collaboration and safeguards that savers are combined in efforts to classify and combat potential risks. This shared method is critical to maintenance working uprightness and improving the overall efficiency of risk government plans.

2.3.2. Implementing Effective Security Protocols

Effective safety protocols are dangerous to founding a strong security culture, defensive supply chain assets from possible threats. These events adopt a series of important measures:

Access Controls: Limits unlawful access to subtle areas and schemes, defensive critical info that only official workers can access.

Data encryption: Defends subtle info from capture and cyberattacks by changing data into prearranged format and decrypting it with the right key to decode it.

Regular security audits: Foremost these reviews is imperative to identify susceptibilities and ensure compliance with manufacturing values, refining your overall safety posture.

Incident response plans: These plans will allow entities to take swift and decisive action in the event of a security breach, minimizing downtime and financial losses.

A strong safety culture ensures not only these events, but that all investors attach and follow to strictly. This collective promise creates an ecosystem of secure and hardy supply chains talented of dealing with various threats while upholding the working whole. By ordering these security measures, entities will be able to meaningfully alleviate the risks related with supply chain turbulences.

2.3.3. Promoting Employee Security Awareness

A strong security ethos ensures that these protocols are not only applied but also professionally connected and strictly followed to by all savers. This shared potential creates a secure and resilient supply chain ecosystem, capable of lasting numerous threats while upholding working integrity. By ordering these security measures, governments can evocatively alleviate risks related with supply chain disturbances

By investing in worker care awareness, organisations work on a ethos of watchfulness and encourage workers to recognize and report unsure acts. This proactive approach minimizes not only supply cable assets, but also the risk of security incidents, eventually fundamental to a safer and more hardy working setting.

2.3.4. Ensuring Compliance with Regulations

Obedience means that obedience is a dangerous aspect of a strong safety ethos that ensures obedience with stringent industry standards and rules. This involves complying with established orders, obeying with strict data protection provisions, and leading regular audits to identify and treat possibly vulnerable. In addition, the maintenance of important certificates shows a promise to enduring safety fineness.

By ordering obedience, organisations will be able to significantly minimalize the risks of suspension, reputational damage, and financial penalties related to non-compliance. This active approach protects not only operations, but also subtle data, ultimately causal to supply chain pliability. A strong safety culture fosters a obedience mindset throughout the group, joining them into everyday practices and ensuring that all labours understand the role they play in conference these values.

2.4. Supply Chain Practices for Disruption Mitigation

2.4.1. Supplier Vetting

Supplier investigate calls for real supplier investigate to be a critical constituent of supply chain risk organisation, safeguarding that external partners do not take security at risk. This difficult process requires a detailed assessment of a vendor's security posture through a detailed valuation of its substructures, policies, and procedures. Suppliers' risk is diligently assessed to identify potential vulnerabilities, while regular account audits attest to obedience with recognised security standards. In addition, votive security circumstances are clearly defined and enforced, so suppliers are responsible for upholding robust safety events.

By applying these procedures, entities will be able to protect themselves against security openings, intelligent stuff theft, and injury caused by unconfident suppliers. This proactive method eventually protects the integrity of the supply chain and reduces the risk of outages and security incidents. Real supplier vetting is critical to maintaining a robust and safe supply chain bionetwork.

2.4.2. Inventory Management

Efficient inventory management is a critical strategy for minimizing supply chain disruptions. This multifaceted method must enhance list levels to equilibrium supply and demand, thereby reducing needless storage prices. On-time delivery (JIT) allows institutions to reduce storage circumstances and alleviate the risk of list uselessness.

In addition, dealer diversification helps prevent vulnerabilities associated with vendor lock-in, and maintaining a defensive list protects against deep disruptions. By adopting these events, entities can improve supply chain resilience, reduce lead times, and improve overall working competence.

Ultimately, effective inventory management meaningfully reduces the impact of disruptions, ensuring that businesses can reply quickly to altering market conditions and uphold steadiness of operations.

2.4.3. Logistics Optimization

Logistics optimisation means that logistics optimization is dangerous to ensuring supply chain resilience. To achieve this, conveyance itineraries are streamlined, reducing transit times and costs and improving delivery dependability. Real-time continuity allows you to proactively screen and rapidly resolve issues as they occur. In addition, improved warehouse security, effective inventory nursing and management, protects goods from theft and injury. In addition, developing contingency plans for unexpected disruptions, such as natural disasters or

transport failures, ensures business continuity and reduces downtime.

Overall, effective logistics optimization significantly reduces the risks of suspension, allowing entities to maintain their operational integrity and respond quickly to supply chain challenges.

2.5. Interplay Between Security Culture and Supply Chain Practices

A strong safety culture recovers source chain resilience: A strong safety culture is the cornerstone of supply chain resilience, providing a multifaceted framework for alleviating threats. By defensive effective supply cable practices, entities can ensure agile operations and effective risk government. This ethos fosters collaboration among investors, indorsing open message and active risk government tactics.

Sanctioning workers' safety awareness is dangerous as it enables workers to identify and report safety threats. Comprehensive training agendas educate workers on best practices, data defence, and threat acceptance, significantly reducing susceptibilities associated with human error. In addition, compliance assurance protects against reputational damage and financial penalties.

Integrating these basics into a cohesive security strategy strengthens supply chain resilience, protects assets, and ensures business control. This proactive approach not only improves employed integrity, but also makes institutions to reply efficiently to the risks that are happening in an progressively multifaceted setting.

2.6. Theory and Hypothesis Development

This education analyzes the effect of physical safety attitude on the occurrence of sole cable outages, particularly on intermediate roles that fulfill unlike types of safety in source chain does, such as data group, contestant group, and human reserve care.

2.7. Contingency Theory and Dynamic Capabilities Theory

The research inspects the effects of organisational security culture using the theories of contingency and dynamic capabilities. According to contingency theory, there isn't a single best way to organise, make decisions, or lead; rather, successful management techniques depend on particular settings (Lawrence & Lorsch, 1967; Schermerhorn, 2011). This theory challenges the notion of a one-size-fits-all approach by highlighting the significance of situational elements in organisational management (Burns & Stalker, 1966; Donaldson, 2001). It aims to distinguish between external variables, such as broader economic and social factors, which are frequently outside of managerial control, and internal variables, such as organisational structures and processes, which management can control. This helps to understand how internal and external environmental factors affect organisational behaviour. Accordingly, contingency theory implies that both internal and external circumstances have an impact on the best organisational decisions (McAdam et al., 2019). According to this study, exposure to supply chain threats shapes an organization's organisational security culture, which in turn influences the adoption of supply chain security (SCS) practices and ultimately impacts the firm's capacity to minimise disruptions.

With its foundation in the resource-based view, dynamic capabilities theory highlights how a company can take advantage of rapid environmental change to obtain a competitive edge. To respond to shifts in the market and develop fresh approaches that add value, a company must be able to effectively integrate, construct, and reorganise both internal and external resources via organisational procedures (Cyfert et al., 2021; Ferreira et al., 2020). The theory of Eisenhardt and Martin (2000) and Singh looks at how well a company can spot opportunities and modify its resource base to gain a sustained competitive advantage under challenging circumstances. According to Kumar and Anbanandam (2019), a strong organisational security culture helps businesses adapt to supply chain disruptions. Secondly, disruptions are a sign of turbulent environments, and a business's ability to live depends on its ability to develop and use its lively competences. In reviewing these two points, the theory of dynamic competences is significant for this study.

The variables that cause supply chain disruptions can be understood in depth, combining contingency theory with dynamic capabilities theory (Eckstein et al., 2014). While the theory of facts elucidates how safety events should be allied with the state, the theory of dynamic capacities highlights adaptive capacities (Wilden et al., 2013; Shonhadji & Maulidi, 2020). When joint, they provide a robust logical outline that improves theoretical understanding and real-world application, eventually helping to achieve supply cable resilience and security.

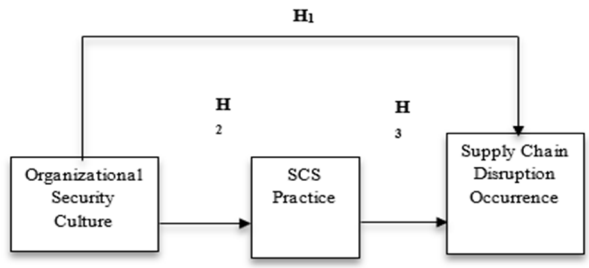

Figure 1: Conceptual Framework

2.7.1. Organizational Security Culture and Supply Chain Disruption Occurrence

The mutable star that reason source chain turbulences can be unspoken in depth, combination eventuality theory with lively capabilities philosophy (Eckstein et al., 2014). While the philosophy of facts clarifies how safety measures should be aligned with the state, the theory of dynamic capacities tourist magnetisms adaptive volumes (Wilden et al., 2013; Shonhadji & Maulidi, 2020). When combined, they provide a robust analytical framework that improves theoretical understanding and real-world application, ultimately helping to manage supply chain resilience and security.

H1: Organizational security culture has a positive effect on supply chain disruption occurrence

2.7.2. Organizational Security Culture and Information Management Security

According to the theory of fact, for effective organisation of source chain turbulences, groups must align their safety culture with info government practices. Investigate has shown that a company's information security directly effects its overall security culture (Chege & Bett, 2019). Grant, 2021; Asamoah et al., 2016). Research has also shown that workers' information security behavior affects the overall security of the group (Da Veiga et al., 2020). In addition, experts stress that a strong security culture is critical to maintaining strong information security and underscore the need for major cultural changes to mitigate security breaches (Ključnikov et al., 2019; Nasir et al., 2019). According to Da Veiga, businesses with a strong security culture are better equipped to respond to cyber threats and other info security risks, as they can develop robust capabilities to manage information and systems security. This is seen after the point of view of dynamic capabilities. This serves to underline the important impact of an institution's safety culture on its policies and procedures. Therefore, based on the influences, the investigate raises the following hypothesis:

H2a: Organizational security culture has a positive effect on information management security

2.7.3. Organizational Security Culture and Facility Management Security

According to Dixit et al. (2019), the theory of facts underscores that an institution's safety culture shapes the tactics for protecting the vital elements of safety in facility management. Herath et al. (2020) highpoint the effect of safety culture on the application and maintenance of safety measures. Also, Renay (2020) makes the point that an effective security culture inspires staff devotion to security procedures, which recovers attentiveness and protocol adherence. As per the dynamic capability theory, organisations with a robust security culture can improve their capacity to handle evolving threats and disturbances in facility security. Consequently, a company's strategic approach to facilities management security is greatly influenced by its security culture. Thus, founded on the overhead, it is imagined that:

H2b: Organizational security culture has a positive effect on facility management security

2.7.4. Organizational Security Culture and Human Resource Security

Warner and Wäger (2019) emphasise that to consume a helpful effect on worker behaviour and operations, organisational strategy and culture must be in harmony. This alignment, according to Agrawal and Hockerts (2019), generates a strong organisational security culture, which is important in determining how employees behave when it comes to security. In support of this, Saglam et al. (2020) points out that managerial decisions about mitigation measures are heavily influenced by a firm's risk management culture. According to Uchendu et al. (2021), cultural changes are required to modify security behaviour since an organization's security culture sets expectations for staff security initiatives. Contador et al. (2020) refer to contingency theory, which holds that the alignment of different organisational components determines the outcomes of an organisation. According to Ali et al. (2021), companies that have a good security culture frequently use strict security measures to stop breaches caused by employees. According to Sharma et al. (2020), companies with strong security cultures leverage this advantage to develop a workforce that is security-conscious, which makes it possible to establish security policies and procedures to effectively manage evolving risks and disruptions. This is in line with the dynamic capability's theory. Founded on the above-mentioned arguments, it is imagined that:

H2c: Organizational security culture has a positive effect on human resource security

2.7.5. Information Management Security and Supply Chain Disruption Occurrence

Bag et al. (2023) highlight how important information is to the efficient running of supply chains, especially for day-to-day operations and interruption control (Katsaliaki et al., 2021). Strong information flow policies and IT resource protection are crucial tactics for reducing supply chain interruptions, according to contingency theory (Colicchia et al., 2019). Mitigating disruptions requires prompt access to supply chain data and efficient information management (Messina et al., 2020). According to Otieno (2021), non-compliance with staff security

policies accounts for a large proportion of security breaches. Dynamic capabilities theory states that businesses with strong information and IT security management are better equipped to deal with changes in an altering setting (Hassija et al., 2021). The significance of giving information management security top priority in order to successfully reduce supply chain disruptions is shown by these findings. Therefore, based on the above discussion, the theory is expressed as shadows:

H3a: Information management security has a negative effect on supply chain disruption occurrence

2.7.6. Facility Management Security and Supply Chain Disruption Occurrence

Facilities are vital bodily assets for companies, and their secure and efficient use can provide a competitive edge by reducing supply chain disruptions. Security breaches at these sites can lead to severe consequences, causing important supply chain interruptions (Aldrighetti et al., 2021). Asamoah highlight the necessity for businesses to put safety in the supply chain plans in place to safeguard both material and irrelevant possessions and successfully minimise disruptions. The main goal of facility management security is to defend physical assets in businesses. Applying ability government safety strategies that address source cable hazards to amenities can help businesses minimise disruptions, according to contingency theory. Supply chain interruptions can be minimised by refining working flow, lowering incidents, and relieving blocks through real ability government safety (Amos et al., 2021). Furthermore, it is critical to protect products, cargo, and important data kept in these facilities because any loss or damage could cause the supply chain to break (Azadegan et al., 2019). Dynamic competences theory states that companies' facilities can modify their facility management security protocols to address emerging risks and shifts in the business landscape, they will be more adept at reducing the incidence and intensity of source chain disturbances. Based on these influences, the research imagines that:

H3b: Facility management security has a negative effect on supply chain disruption occurrence

2.7.7. Human Resource Security and Supply Chain Disruption Occurrence

Facilities are crucial physical assets for businesses, and by minimising supply chain interruptions, their safe and effective use can give them a competitive advantage. These locations are vulnerable to serious security breaches that could disrupt the supply chain significantly. The primary goal of facility management security is to protect physical assets in businesses. According to contingency theory, implementing facility management security strategies that address supply chain risks to facilities can help businesses minimise disruptions. An organisation can strategically benefit from effective facility management security by improving operational flow, lowering accident rates, easing operational bottlenecks, and eventually minimising supply chain interruptions. Facilities house vital resources such as goods, freight, and sensitive data, hence facility management security is crucial for businesses. Dynamic capacities theory states that companies can better lessen the incidence and impact of supply chain interruptions when they are able to modify or reconfigure their security protocols for site management in reaction to emerging risks and modifications in the commercial landscape. Based on the above considerations, the hypothesis can be stated as follows:

H3c: Human resource security has a negative effect on supply chain disruption occurrence The Mediating Role

2.8. Information Management Security on Organizational Security Culture and Supply Chain Occurrence

Information management security plays a mediating role between supply chain incidents and organisational security culture, implying that information management security practices within an organisation impact supply chain disruption frequency as well as the organisational security culture. By raising awareness and adherence to security procedures, effective information management security methods including employee training, access control, and encryption support a robust organisational security culture. According to Ali, companies that have robust information management security policies also tend to have more robust security cultures since their staff members follow established standards and are more aware of security dangers. This research supports the theory of contingency by showing that efficient security procedures are customised to meet the unique needs of the company. According to Burrell et al. (2020), information management security breaches have a detrimental effect on organisational security culture, which raises supply chain risk and fosters a lack of trust. According to Patel et al. (2023), companies with efficient staff access control—which includes enforcing role-based access restrictions and keeping an eye on access logs—saw a decrease in supply chain security breaches. Organisations that incorporated information management security practices into their overall security strategy showed increased resilience and adaptability in addressing new threats, according to Zaini et al. (2020). The aforementioned discovery underscores the significance of information management security in serving as a mediator between supply chain incidents and organisational security culture. It further underscores the

imperative for organisations to consistently enhance their security protocols to effectively manage supply chain risks. Founded on the overhead influences, the research imagines that:

H4a: Information management security mediates the relationship between organizational security culture and supply chain occurrence

2.8.1. Human Resource Security on Organizational Security Culture and Supply Chain Occurrence

The impact of human resource-related security practices on an organization's security culture and the frequency of supply chain disruptions is demonstrated by the function that human resource security plays in mediating the relationship between supply chain events and organisational security culture. Good human resources security practices, like background checks, access control, and employee training, increase employee awareness and adherence to security procedures, which in turn strengthens the organisational security culture. According to Tolah, a stronger security culture and higher employee compliance are associated with comprehensive HR security measures. Homoliak et al. (2019) noted that thorough background checks diminish insider risks, whereas Yu et al. (2019) provided evidence that investing in security training helps reduce incidents within the supply chain. The significance of access control in mitigating security breaches was underscored by Yaacoub et al. (2021), while Mughal (2022) emphasised the enhancement of organisational adaptability and resilience through the integration of human resource security into overall security plans. These findings highlight the critical role that human resource security plays in mediating the relationship between supply chain events and organisational security culture. They also highlight the necessity of integrating these practices into organisational security frameworks in order to manage supply chain security risks in an efficient manner. Based on the above, it is hypothesized that:

H4b: Human resource security mediates the relationship between organizational security culture and supply chain occurrence

2.8.2. Facility Management Security on Organizational Security Culture and Supply Chain Occurrence

Facility management security shapes how facility management security practices impact supply chain incidents and organisational security culture. Strong organisational security cultures are developed through the implementation of efficient facilities management security measures, such as access control, surveillance systems, and physical security protocols. These methods provide a safe working environment that promotes trust and adherence to security protocols. Companies with well-implemented facility management security measures reported improved employee satisfaction and felt safety, which strengthened the security culture, according to Muñoz et al. (2023) Strong facility management security procedures are crucial, as Asamoah showed when they showed how investments in cutting-edge surveillance and access control systems dramatically decreased security incidents in the supply chain. According to Jones, companies that perform frequent security audits and risk assessments for their facilities report decreased rates of theft and vandalism. This is good news for supply chain security as well as organisational security culture. In line with the dynamic capability's theory, Technology (2019) discovered that including facility management security in the overall security plan increased adaptation and resilience in the face of new threats. According to Handfield et al. (2022), supply chain interruptions were reduced when facility management employees received training on security protocols and emergency response techniques. To effectively handle supply chain security concerns, this emphasises how crucial it is to include facility management security into organisational security frameworks. These results demonstrate how important facility management security is as a mediator between supply chain incidents and organisational security culture. Based on the above, it is hypothesized that:

H4c: Facility management security mediates the relationship between organizational security culture and supply chain occurrence

3. Research Methods and Materials

3.1. Study Design

This quantitative study, conducted in Ghana's manufacturing and service sectors, employed a structured questionnaire survey to investigate the relationships between supply chain security practices, organizational security culture, and supply chain disruptions. The study's setting in Ghana's rapidly growing industrial and service sectors provides valuable insights into the complexities of supply chain management in a developing economy, with implications for improving supply chain resilience and mitigating disruptions.

3.2. Measures

Employing a structured questionnaire survey, the study used a quantitative approach to evaluate latent components using a variety of indicators that were modified from earlier studies. To improve clarity and relevance, the item wording was modified. On a 5-point Likert scale that ranges from

"strongly disagree" to "strongly agree," with a midpoint option of "neither agree nor disagree," the variables measured were the mediating variable (supply chain security practices), the independent variable (organizational security culture), and the dependent variable (supply chain disruption). Asamoah provided the adaptation of items for measuring supply chain security practices, including information management security, human resource security, and facility management security. Items from Park were used as the basis for the supply chain disruption evaluation. Two academic specialists and two business professionals examined the measuring items to make sure they were adequate. The survey instruments were pre-tested by managers from several companies in Ghana, and the instruments were improved based on their comments. After this improvement, data was gathered for the suggested model's testing using the main survey. By taking a strict approach, the goal was to guarantee the accuracy and consistency of the data used to analyse the connections between supply chain security practices, organizational security culture, and supply chain disruptions.

3.3. Data Collection

Based on the Ghana Statistical Service's 2021 Integrated Business Establishment Survey, which identified 28,493 businesses in various sectors with over a million employees, the study concentrated on manufacturing and service companies in Ghana (Ghana Statistical Service, 2022). Ghana was chosen because of its quickly developing industrial and service sectors, as well as its economy, which is rising at a faster rate than other emerging markets. The study focused on managers at different levels of these companies who oversaw supply chain and security operations. Using directories from business associations like the Ghana Services Suppliers Association and the Association of Ghana Industries, a purposive sample frame was developed. This framework made it easier to choose a sample of 394 managers by considering factors like firm size, operational experience, and exposure to other countries, guaranteeing a diverse group. After quality checks, 350 of the 394 distributed questionnaires were found to be valid. The study used AMOS (processing of Moment Structures) software for data processing and testing the conceptual model. This program was selected for its capacity to do structural equation modelling (SEM). With an emphasis on how organizational security culture influences supply chain disruptions and the mediating function of supply chain security policies, SEM was perfect for assessing the measurement and structural models as well as testing direct, indirect, and total effects among the latent variables.

3.4. Sample Selection

A purposive sampling frame was developed using directories from business associations such as the Ghana Services Suppliers Association and the Association of Ghana Industries. This framework facilitated the selection of 394 managers based on specific criteria, including firm size, operational experience, and international exposure, ensuring a diverse and representative group. This targeted approach enhances the validity of the research by focusing on individuals most likely to provide relevant insights into the study's objectives.

3.5. Data Analysis

The study utilized quantitative data analysis techniques to investigate the relationships between supply chain security practices, organizational security culture, and supply chain disruptions. This methodological approach allowed for a systematic examination of how these variables interact and influence one another, providing valuable insights into the dynamics of supply chain resilience.

Statistical software: AMOS (Examination of Constructions of the Instant) software was used to procedure data and test the concept model, taking advantage of its competences in reckonings to model structure (SEM). This influential tool effectively analyzes the complex relationships amid variables, making it easier to comprehensively comprehend the data.

3.5.1. Data Analysis Techniques

Bodily Equation Modeling (SEM): Used to assess physical and measurement copies, as well as to test direct, indirect, and whole effects among latent variable star. Evocative figures: It is used to précis the demographic and structural features of the defendants, providing an overview of the sample. Dependability analysis: It is performed to ensure the heftiness and accuracy of the measurement instruments used in the inspection. Value analysis: It was carried out to value the building and ensure the precision of the dimension tools of the deliberate buildings.

3.5.2. Measurement Model

Factor Analysis (CFA): It is used to validate the measurement model and evaluate the loads of the masonry, ensuring the exact representation of the buildings.

Construct Reliability: Evaluated using Cronbach's alpha coefficients to determine the internal consistency of the measurement instruments.

3.6. Structural Model

Path Analysis: Conducted to examine the relationships between latent variables, providing insights into the direct and indirect effects within the model. Mediation Analysis: Employed to assess the mediating effect of supply chain security practices on the relationships among the variables.

Sample Size and Power Analysis A sample size of 350 was determined to be sufficient based on power analysis, ensuring the ability to detect significant relationships between the variables effectively.

4. Results

4.1. Demographic Results

Utilising frequency tables, the respondent's demographic information was displayed. According to the research, middle-level management accounted for 55.6% of the respondents, while senior-level management accounted for 27.1%. 48.9% of those with first degrees and 26.3% with second degrees were the educational status of the population. 53.7 percent of respondents reported having worked for six to ten years, while 24.3% reported having worked for ten or more years. Firm-level demographic data revealed that the majority of the firms (77.1%) had been in operation for more than three years, indicating that they had sufficient experience to offer pertinent data for the study. Companies in the food and beverage sector made up 56.3% of the industry, followed by those in the energy, electrical, and electronics sectors (25.1%), agricultural (15.5%), and building, mining, and construction areas (3.4%).

Table 1: Demographic Results

Employee status	Frequency	Percentage (%)
Lower level	57	16.3
Middle level	198	56.6
Senior Level	95	27.1
Total	350	100.0
Educational Status		
Diploma	87	24.9
Degree	171	48.9
Masters	92	26.3
Total	350	100.0
Work Experience		
1-5 years	77	22.0
6-10 years	188	53.7
Above 10 years	85	24.3
Total	350	100.0
Years of Existence		
Less than 1 year	37	10.6
1-3 years	43	12.3
4-6 years	54	15.4
7-9 years	68	19.4
10 or more years	148	42.3
Total	350	100.0
Industry type		
Food and beverages	197	56.3
Building, mining, and construction	12	3.4
Energy, electrical and electronics	88	25.1
Agriculture	53	15.1
Total	350	100.0

Source: Prepared by the author (2024)

4.1.1. Descriptive Statistics, Correlation Analysis, Non-response, and Common Method Bias

Table 2 displays the findings of the study constructs' intercorrelation and descriptive statistics. The results show that organisational security culture (r=.565, p=.000; r=.517, p=.000; r=.507, p=.000), facility management security (r=.609, p=.000; r=.630, p=.000; r=.628, p=.000), human resource management security (r=.569, p=.000; r=.557, p=.000; r=.567, p=.000), and information management security (r=.635, p=.000; r=.591, p=.000; r=.521, p=.000) are all positively and significantly correlated with disruptions caused by internal, supplier, and customer. The univariate normality of the data was confirmed by the values of skewness and kurtosis (see Table 2).

Table 2: Descriptive Statistics and Correlation Matrix

Constructs	Mean	STDV	Skewness	Kurtosis	OSC	FMS	HRMS	IMS	ID	SD	CD
OSC	3.93	0.817	-0.412	-0.002	0.782						
FMS	3.92	0.836	-0.473	-0.002	.694**	0.799					
HRMS	3.97	0.822	-0.395	-0.260	.544**	.657**	0.831				
IMS	4.02	0.802	-0.406	-0.301	.595**	.513**	.565**	0.849			
ID	4.03	0.804	-0.286	-0.563	.565**	.609**	.569**	.635**	0.853		
SD	4.12	0.743	-0.604	0.601	.517**	.630**	.557**	.591**	.502**	0.866	
CD	4.01	0.773	-0.527	0.087	.507**	.628**	.567**	.617**	.521**	.571**	

Note(s); OSC = Organizational Security Culture; FMS = Facility Management Security; HRMS = Human Resource Security; IMS = Information Management Security; ID = Internal Disruption; SD = Supplier Disruption; CD = Customer Disruption. **Correlation is significant at 0.01 level (2-taled)

As advised by Rogelberg and Stanton (2007), t-tests were performed in SPSS 23 to compare early and late participants (n=200) to evaluate non-response bias. There were no discernible variations between these groups in the data, suggesting that non-response bias was not an issue. Using Harman's single-factor test, which explained roughly 35% of the variation and fell below the 50% criterion, it was determined that common method bias (CMB) was not a significant influence. Furthermore, a common latent factor (CLF) was included using AMOS in the confirmatory factor analysis (CFA) per Podsakoff et al. (2003). The lack of a discernible decline in factor loadings was evident in the results, indicating that CMB had no impact on the data. Table 2 displays moderate correlations between the research constructs, which do not surpass r>0.90, suggesting that CMB was not an issue in our study.

4.2. Validity and Reliability

Using factor loadings, composite reliability (CR), alpha values, and average variance extracted (AVE), and Hoe (2008) and Fornell and Larcker (1981), the study evaluated convergent validity. Table 3 illustrates that alpha values exceeded the acceptable threshold of 0.7, with values ranging from 0.884 to 0.933. The AVE values ranged from 0.612 to 0.750, while the CR values were between 0.885 and 0.934. These values both met the corresponding cut-off standards of 0.5 and 0.7. All constructs had item loadings between 0.736 and 0.894, over the minimum threshold of 0.70, according to confirmatory factor analysis (CFA) (Hu & Bentler, 1999). The validity and reliability of each measure are confirmed by these findings. To assess discriminant validity, the intercorrelation values were compared to the square root of AVE. The square root of AVE surpasses all intercorrelation values in Table 2, which shows strong discriminant validity for all measures. Table 2 also shows the intercorrelation values between the components.

Table 3: Confirmatory Factor Analysis

Constructs	Items	Loadings	Alpha	CR	AVE
Organizational security culture	OSC5	0.736	0.887	0.887	0.612
	OSC4	0.763			
	OSC3	0.802			
	OSC2	0.809			
	OSC1	0.798			
Facility management security	FMS9	0.779	0.933	0.934	0.638
	FMS8	0.809			
	FMS7	0.799			
	FMS6	0.834			
	FMS5	0.844			
	FMS4	0.823			
	FMS3	0.752			
	FMS2	0.743			
Human resources security	HRMS4	0.850	0.989	0.899	0.691
	HRMS3	0.827			
	HRMS2	0.872			
	HRMS1	0.774			
Information management security	IMS3	0.850	0.885	0.885	0.72
	IMS2	0.842			
	IMS1	0.853			
Internal disruption	ID3	0.803	0.886	0.888	0.727
	ID2	0.876			
	ID1	0.876			
Supplier disruption	SD3	0.870	0.900	0.900	0.750
	SD2	0.888			
	SD1	0.840			
customer disruption	CD3	0.867	0.884	0.886	0.721
	CD2	0.894			
	CD1	0.783			

Source: Prepared by the author (2024)

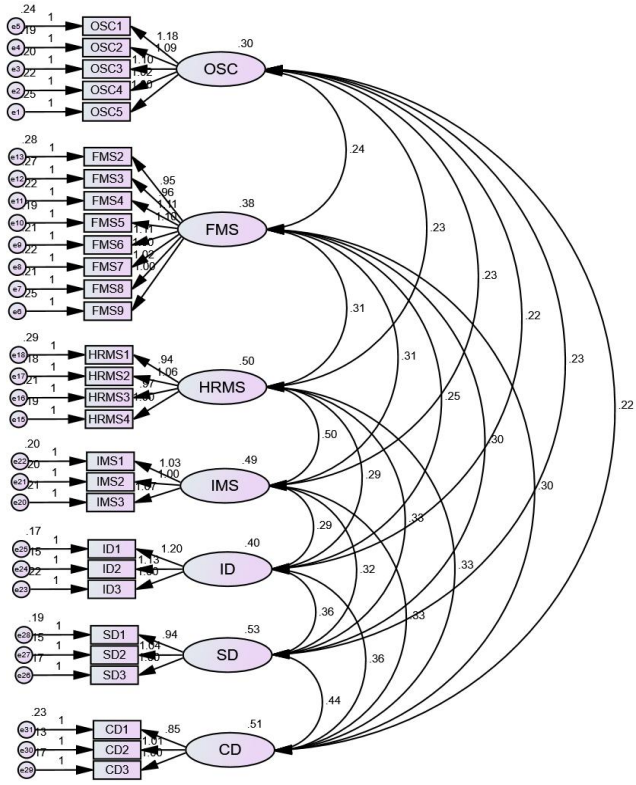

Figure 2: Confirmatory Factor Analysis

4.3. Confirmatory Factor Analysis

Two stages of confirmatory factor analysis (CFA) were used to evaluate how well the suggested measurement model fit the data. We assessed organisational security

culture, data organisation security, humanoid reserve safety, ability organisation security, and internal disruption in the first phase of the study. The model fit well, according to the CFA results, with the following indices demonstrating a good match: χ^2 (CMIN/DF) = 725.209/356 = 2.037, p = 0.000, CFI = 0.956, SRMR = 0.023, RMSEA = 0.055, IFI = 0.956, TLI = 0.949. We combined all of the study variables into an extensive measurement model in the second phase. The CFA findings verified that this model satisfies the model fitness acceptance requirements as well: CFI = 0.903, SRMR = 0.055, RMSEA = 0.066, IFI = 0.905, TLI = 0.896, \2 (CMIN/DF) = 1694.38/697 = 2.431, p = 0.000.

Table 4: Model Fitness

Model-indices	independent variables MM	Overall -MM	Structural Model	Cut-off values
Chi-square (CMIN/DF	2.037	2.431	2.263	<3
p-value	0.000	0.000	0.473	>.05
CFI	0.956	0.903	0.989	>.95
SRMR	0.023	0.055	0.017	<.06
RMSEA	0.055	0.066	0.031	<.08
IFI	0.956	0.905	0.989	<.95
TLI	0.949	0.896	0.985	<.90
Note(s): MM = measurement model				

Source: Prepared by the author (2024)

4.4. Structural Model and Hypothesis Testing

The postulated relationships were verified by converting the authentication of the dimension perfect into a structural perfect. Based on Hoe and Hu and Bentler criteria, the structural model was deemed to be fit. A satisfactory match was shown by the structural model's indices, which were as follows: χ^2(CMIN/DF)=6.789/3=2.263, p=0.473, CFI= 0.989, SRMR=0.017, RMSEA=0.031, IFI=0.989, TLI= 0.985. Utilising the greatest likelihood approach, the hypotheses were tested using AMOS 23.0. The findings of the analysis supported hypotheses 1, 3a, and 3b by showing that organisational security culture (β= -0.149, t= -2.291, p= 0.022), data organisation security (β= -0.275, t= -6.604, p= 0.000), and facility management security (β= -0.349, t= -6.703, p=0.000) all significantly reduce supply chain disruptions.

Nevertheless, supply chain disruptions were not significantly impacted by human resource security (β= -0.092, t=-0.963, p=0.178), refuting hypothesis 3c. Information management security (β= 0.681, t=13.833, p= 0.000), facility management security (β=0.709, t=17.983, p=0.000), and human resource security (β=0.478, t=12.113, p=0.000) were all significantly positively impacted by organisational security culture, confirming hypotheses 2a, 2b, and 2c. A significant portion of the variation in data organisation security (35.4%), facilities management security (48.1%), and human resource security (29.6%) can be attributed to organisational security culture. Of the variance in supply chain interruptions, the research predictors accounted for 55.5%.

Following Preacher and Hayes' (2008) methodology, a mediation analysis was carried out using AMOS 23.0 with bias-corrected bootstrapping (5,000 iterations) at a 95% sureness intermission. Results of the mediation analysis showed that organisational security culture had a important unintended effect on supply chain disruptions through security practices (security of information management, security of facilities, and security of human resources), supporting hypotheses 4a, 4b, and 4c. (see Table 5).

Table 5: Hypotheses Testing

Relationships	Path	Estimate	SE	CR (t)	p-value	Decision
Hypothesis 1	$OSC \rightarrow SCD$	-0.149	0.065	-2.291	0.022	Supported
Hypothesis 2a	$OSC \rightarrow IMS$	0.681	0.049	13.833	0.000	Supported
Hypothesis 2b	$OSC \rightarrow FMS$	0.709	0.039	17.983	0.000	Supported
Hypothesis 2c	$OSC \rightarrow HRS$	0.478	0.039	12.113	0.000	Supported
Hypothesis 3a	$IMS \rightarrow SCD$	-0.275	0.042	-6.604	0.000	Supported
Hypothesis 3b	$FMS \rightarrow SCD$	-0.349	0.052	-6.703	0.000	Supported
Hypothesis 3c	$HRS \rightarrow SCD$	-0.092	0.052	-0.963	0.178	Not Supported
Bootstrapping		Indirect Effect	SE	Lower 95% CI	Upper 95% CI	Decision
Hypothesis 4a	$OSC \rightarrow IMS \rightarrow SCD$	0.3261	0.0501	0.2505	0.4054	Supported
Hypothesis 4b	$OSC \rightarrow HRS \rightarrow SCD$	0.2525	0.0373	0.1822	0.328	Supported
Hypothesis 4c	$OSC \rightarrow FMS \rightarrow SCD$	0.4035	0.0507	0.307	0.5069	Supported
Note(s): The number of sampling iterations equal to 5,000 times						

Note(s); OSC = Organizational Security Culture; FMS = Facility Management Security; HRMS = Human Resource Security; IMS = Information Management Security; ID = Internal Disruption; SD = Supplier Disruption; CD = Customer Disruption.

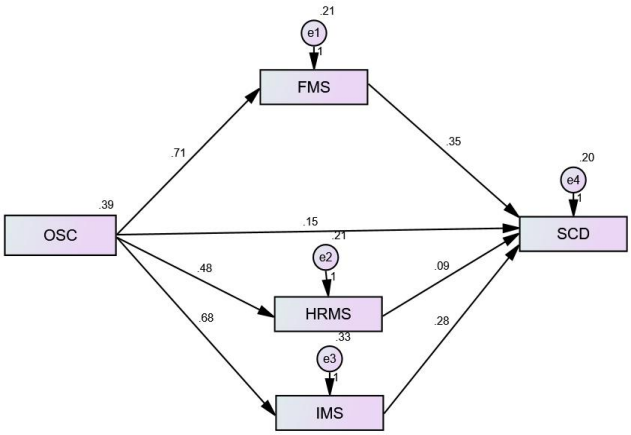

Figure 3: Structural Model

The study's findings effectively connect the theoretical framework with empirical data, revealing significant relationships between organizational security culture, supply chain security practices, and the occurrence of disruptions. The results indicate that a strong organizational security culture promotes effective supply chain security practices, which, in turn, help mitigate the occurrence of disruptions.

4.3.1. Theoretical Implications

The study protects the theoretical zone, as the culture of fingerprint security indirectly affects suspension actions through supply chain security practices. This discovery underscores the critical role that organizational security culture and supply chain security practice play in ensuring supply chain continuity and resilience..

4.3.2. Practical Implications

Empirical evidence offers valuable insights to supply chain managers and decision-makers, and highlights the importance of promoting a safety-conscious organizational culture, establishing effective supply chain safety practices, and minimizing suspension risks. To recover supply cable resilience, companies must prioritize developing a strong structural security ethos and capitalise in robust safety does.

4.3.3. Key Takeaways

Structural safety ethos meaningfully effects source cable safety does. Supply cable safety does play a critical role in reducing outages. Structural security ethos indirectly influences the incidence of disturbances through its effect on source chain security practices.

4.3.4. Future Research Directions

Future educations should travel the influence of organizational safety ethos on supply cable pliability, examine the role of technology in strengthening supply chain safety does, and examine the association amid supply chain security does and general supply chain presentation.

4.3.5. Managerial Recommendations

Supply chain bosses should order the growth of a strong structural safety culture, capitalise in robust security does, and integrate technology to reinforce supply chain resilience. Politicians should also join structural safety culture into source chain regulations and values.

5. Discussion

Our study examined how structural safety affects supply cable (SC) disturbances and if SC safety does mediate the association between structural security culture and SC disruption, guided by the theories of contingency and dynamic capacities. Our education authenticates hypothesis 2a, as it shows that the culture of structural security favors and favors safety in info organisation. This is reliable with the idea that groups with strong safety cultures are better armed to create info organisation security events that efficiently grip new risks and developments (Da Veiga & Eloff, 2010; Von Solms & Von Solms, 2004). Furthermore, our research supported Hypothesis 2b by positive that structural care ethos has a positive impact on aptitude government safety. This demonstrates how facility organisation security outlines may be wired by a strong security culture, increasing their ability to handle ecological vicissitudes and intimidations (Chunsheng et al., 2019).

Our study supported Hypothesis 2c, which states that organisational safety philosophy affects humanoid reserve safety. According to Hintsa et al. (2009), this implies that companies with a strong security culture make investments in hiring and educating security-aware staff members. This strengthens the security of their human resources. All things considered, our results highlight how important organisational security culture is to developing and putting into practice successful SC security procedures (Lu et al., 2019; Kurniawan et al., 2017).

Our research indicates that supply chain disruptions are far less common when facility management security is in place. This outcome is in stroke with educations (Zailani et al., 2015; Tse et al., 2016) that demonstrate how efficient ability organisation improves supply chain presentation and lowers interruption rates (Ahmad et al., 2019). Zailani found that although human resource security may help to reduce disruptions, its influence is not statistically significant. As a result, the effect of HRS on supply chain disturbances was determined to be negative (Alsharari & Aljohani, 2023).

On the other pointer, educations that highlight the significance of strong data management in improving supply chain performance and resilience are supported by the fact that information management security dramatically lowers supply chain interruptions (Anwar & Abdullah, 2021). Effective information management security significantly reduces disruptions, which emphasises its vital role in enhancing supply chain operating efficiency. In addition, our study demonstrated that supply chain disruptions and organizational security culture are very intermediate due to supply chain security (SCS) practices (Fainshmidt et al., 2018). According to the results, the adoption of effective supply chain security procedures (SCS), which reduce risks, is a great safety culture. These findings highlight the relationship between supply chain disruptions, SCS procedures, and the institution's safety culture. They also highlight the need to combine an effective SCS procedure with a strong safety culture to actively manage and reduce supply chain risks (Magdy et al., 2023).

The debate really summarizes the findings and perceives them easily with a review of the literature and its theoretical consequences. The author confirms the fundamental findings and highlights the significant relationships between organizational security culture, supply chain security practices, and the occurrence of disruptions. These results are related to the existing literature, reinforcing the theoretical bases and supporting the ongoing academic discourse.

In addition, the discussion specifies practical implications, offering practical recommendations for managers and decision-makers. It emphasizes the mediating role of supply chain security practices, underscoring the importance of integrating both cultural and practical dimensions. The author also identifies avenues for future research, encouraging further exploration of the complex relationships between organizational security culture, supply chain resilience, and overall performance.

The strengths of the discussion include clear and concise language, effective integration of findings with the literature review and theoretical implications, practical recommendations, and identification of future research directions. However, there is limited critical evaluation of the findings, and the analysis of theoretical implications could be more in-depth.

5.1. Implications of the Study

The study delivers important new information for theoretical advancement as well as real-world application. There has remained a shortage of experiential information concerning the drivers of SCS practices in the SCS literature. This study adds fresh insights by highlighting the critical role that organisational security culture plays in determining the amount of SCS inside enterprises. The study fills a knowledge gap in SCS practices and their causes and effects in emerging economies, especially in Africa, where research has been sparser than in affluent nations, by analysing these relationships in an African context.

The results highlight the significance of developing a security-focused culture by indicating that SCS practices may not succeed in achieving their desired goals in the absence of a strong organisational security culture. The study also shows that supply chain disruptions are lessened by organisational security culture when supply chain practices are used as a go-between. The interdependence of supply chain resilience, operational procedures, and security culture is highlighted by this mediation effect. It illustrates how a strong security culture together with certain SCS practices is necessary to minimise interruptions, highlighting an integrated strategy that blends cultural values with useful security measures.

Practically speaking, managers should concentrate on building a strong security culture to increase the achievement of their SCS projects, as the finding that organisational security culture influences the implementation of SCS practices reveals. Establishing a strong culture is crucial because it impacts the three facets of SCS practices. The research tourist attractions that although every aspect of supply chain disruption prevention strategies is important, facility management security needs to take precedence to minimise supply chain interruptions. Companies ought to commit resources to putting SCS plans into action and protecting both material and immaterial assets. The report also emphasises how crucial it is to combine practical security measures with cultural aspects. Encouraging a robust security culture in isolation is not enough; it needs to be combined with efficient SCS procedures, such as information management security, facilities management security, and compliance controls. These procedures are essential for converting a culture that prioritises security into concrete measures that anticipate and address possible supply chain issues. The education tourist attractions how important it is to create an air where staff memberships remain involved and helpful of security events. Fruitful SCS events can result after a strong safety culture, which safeguards staff associations are conscious of, keen to, and often adhere to care proceedings.

5.2. Practical Implications for Industry Professionals

The education's responses have significant practical insinuations for manufacturing authorities, emphasising how organizational security culture can improve the

effectiveness of care does in plunging source chain disruptions. Exactly, the investigate suggests that:

- Managers should prioritize building a strong security culture to bolster supply chain resilience.
- Companies should allocate resources to implement effective supply chain security practices.
- Integrating cultural and practical aspects of supply chain security is essential for comprehensive protection.
- Employee awareness and commitment to security procedures are crucial for maintaining a secure environment.

By focusing on these areas, organizations can better safeguard their operations against potential disruptions and enhance overall performance.

The education underlines the dangerous role of organizational security ethos in ornamental the effectiveness of security practices to reduce supply chain disruptions. By development a healthy security culture, organizations can improve worker awareness and commitment to security events, boost supply chain resilience, minimize disruption risks, and ensure long-term business control. This addition of cultural and practical aspects of supply chain security is essential for achieving optimal results. Fundamentally, a strong security ethos acts as a multiplier, intensifying the impact of security practices and leading to improved supply chain pliability.

By prioritizing structural security culture, manufacturing specialists can nurture a active and receptive security carriage that efficiently alleviates disturbances and safeguards working steadiness.

6. Conclusion

According to this study, supply chain security (SCS) practices influence the culture of organizational security, i.e., the security of the data organization, the organization of competencies, and human reserve, to mitigate supply chain disruptions due to significant operational and financial consequences. Using the fields of fact theory and dynamic capabilities philosophy, the study analyzed how SCS practices moderate this relationship and suggested that stronger organizational security cultures would have fewer disruptions in the original chain. The responses showed that the disruptions of the source chain have had a negative impact on the institution's safety culture and that all three SCS practices have had a positive impact. According to the study's findings, HR security did not significantly reduce supply chain disruptions. In addition, security in data organization and security in facility management were shown to be important, significantly reducing the frequency of outages. The results demonstrate that the effective implementation of SCS techniques, especially the organization of competition, is decisive to reduce supply chain disruptions, and underlines the importance of building a strong organizational security culture to support SCS activities, as underlined by the role of the mediator of the SCS practice, since the great safety culture is fundamental. But we must also protect viable and effective security measures, which are those that have a cultural ideal. to turn resilience into operational and reduce disruptions. According to the study's findings, it highlights the critical role of organizational security culture in improving supply chain resilience. By underscoring the importance of this culture, the study shows how it can mitigate supply chain disruptions and how it can improve your operational efficiency.

The implications of these findings are substantial for industry professionals, encouraging them to reassess their supply chain security strategies. It also prompts researchers to explore related topics, while policymakers are urged to consider organizational security culture in the formulation of supply chain regulations and standards.

Overall, the conclusion synthesizes the study's key findings and implications, providing a comprehensive roadmap for enhancing supply chain resilience. By integrating theoretical frameworks with empirical evidence, the study offers valuable insights for developing effective supply chain security strategies and underscores the need for ongoing research in this critical area.

The study's emphasis on Ghana's manufacturing subdivision whitethorn consumes incomplete the discoveries' applicability to other areas or businesses. The upcoming study must cover a better range of industries and geographies to increase the conclusions' applicability. Furthermore, there may be biases introduced by using self-reported survey data; however, these could be reduced in subsequent research by using objective measures or a mixed-methods approach to provide more thorough insights. To understand how potential moderating factors, such as organisational size or complexity, may affect the observed associations, more research could look into these in addition to the direct and mediating impacts that this study addressed. This investigation has the potential to improve theoretical comprehension as well as real-world applications.

References

Agrawal, N., & Hockerts, N. (2019). Impact Investing Strategy: Managing Conflicts between Impact Investor and Investee Social Enterprise. *Sustainability*, *11*(15), 4117. https://doi.org/10.3390/su11154117

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2019). How integration of cyber security management and incident response enables organizational

learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

Al Izki, F. H. S. (2019). *Exploring the organisational, social and cultural factors influencing those employee attitudes and behaviours that impact the implementation of an information security culture within Omani organisations* [University of Strathclyde]. https://stax.strath.ac.uk/concern/theses/9019s255m

Aldrighetti, R., Battini, D., Ivanov, D., & Zennaro, I. (2021). Costs of resilience and disruptions in supply chain network design models: A review and future research directions. *International Journal of Production Economics*, *235*, 108103. https://doi.org/10.1016/j.ijpe.2021.108103

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences*, *11*(8), 3383. https://doi.org/10.3390/app11083383

Ali, Z., Gongbing, B., & Mehreen, A. (2021). Do vulnerability mitigation strategies influence firm performance: the mediating role of supply chain risk. *International Journal of Emerging Markets*, *18*(3), 748–767. https://doi.org/10.1108/ijoem-04-2020-0397

Alsharari, N. M., & Aljohani, M. S. (2023). The benchmarking implementation and management control process as influenced by interplay of environmental and cultural factors: institutional and contingency perspectives. *Benchmarking an International Journal*. https://doi.org/10.1108/bij-11-2022-0733

Amos, D., Au-Yong, C. P., & Musa, Z. N. (2021). The mediating effects of finance on the performance of hospital facilities management services. *Journal of Building Engineering*, *34*, 101899. https://doi.org/10.1016/j.jobe.2020.101899

Anwar, G., & Abdullah, N. N. (2021). The impact of Human resource management practice on Organizational performance. *International Journal of Engineering Business and Management*, *5*(1), 35–47. https://doi.org/10.22161/ijebm.5.1.4

Asamoah, D., Andoh-Baidoo, F. K., & Agyei-Owusu, B. (2016). Examining the Relationships between Supply Chain Integration, Information Sharing, and Supply Chain Performance: A Replication Study. *Americas Conference on Information Systems*. http://129.122.16.11/handle/123456789/11634

Asamoah, D., Nuertey, D., Agyei-Owusu, B., & Acquah, I. N. (2021). Antecedents and outcomes of supply chain security practices: the role of organizational security culture and supply chain disruption occurrence. *International Journal of Quality & Reliability Management*, *39*(4), 1059–1082. https://doi.org/10.1108/ijqrm-01-2021-0002

Autry, C. W., & Bobbitt, L. M. (2008). Supply chain security orientation: conceptual development and a proposed framework. *The International Journal of Logistics Management*, *19*(1), 42–64. https://doi.org/10.1108/09574090810872596

Azadegan, A., Parast, M. M., Lucianetti, L., Nishant, R., & Blackhurst, J. (2019). Supply Chain Disruptions and Business Continuity: An Empirical assessment. *Decision Sciences*, *51*(1), 38–73. https://doi.org/10.1111/deci.12395

Bag, S., Rahman, M. S., Srivastava, G., Shore, A., & Ram, P. (2023). Examining the role of virtue ethics and big data in enhancing viable, sustainable, and digital supply chain performance. *Technological Forecasting and Social Change*, *186*, 122154. https://doi.org/10.1016/j.techfore.2022.122154

Burns, T., & Stalker, G. M. (1966). *The Management of Innovation*. Tavistock Publications. https://books.google.ie/books?id=C2fgAAAAMAAJ&q=The+Management+of+Innovation&dq=The+Management+of+Innovation&hl=&cd=1&source=gbs_api

Burrell, D. N., Bhargava, N., Bradley-Swanson, O., Harmon, M., Wright, J., Springs, D., & Dawson, M. (2020). Supply chain and logistics management and an open door policy concerning cyber security introduction. *International Journal of Management and Sustainability*, *9*(1), 1–10. https://doi.org/10.18488/journal.11.2020.91.1.10

Chege, S. W., & Bett, S. (2019). Total quality management practices and performance of organizations in the real estate industry, case of property developers in Nairobi City County, Kenya. *International Journal of Current Aspects*, *3*(IV), 14–31. https://doi.org/10.35942/ijcab.v3iiv.44

Chunsheng, L., Wong, C. W., Yang, C., Shang, K., & Lirn, T. (2019). Value of supply chain resilience: roles of culture, flexibility, and integration. *International Journal of Physical Distribution & Logistics Management*, *50*(1), 80–100. https://doi.org/10.1108/ijpdlm-02-2019-0041

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management an International Journal*, *24*(2), 215–240. https://doi.org/10.1108/scm-09-2017-0289

Contador, J. C., Satyro, W. C., Contador, J. L., & De Mesquita Spinola, M. (2020). Taxonomy of organizational alignment: implications for data-driven sustainable performance of firms and supply chains. *Journal of Enterprise Information Management*, *34*(1), 343–364. https://doi.org/10.1108/jeim-02-2020-0046

Cyfert, S., Chwiłkowska-Kubala, A., Szumowski, W., & Miśkiewicz, R. (2021). The process of developing dynamic capabilities: The conceptualization attempt and the results of empirical studies. *PLoS ONE*, *16*(4), e0249724. https://doi.org/10.1371/journal.pone.0249724

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Dixit, M. K., Venkatraj, V., Ostadalimakhmalbaf, M., Pariafsai, F., & Lavy, S. (2019). Integration of facility management and building information modeling (BIM). *Facilities*, *37*(7/8), 455–483. https://doi.org/10.1108/f-03-2018-0043

Donaldson, L. (2001). *The Contingency Theory of Organizations*. SAGE. https://sk.sagepub.com/books/the-contingency-theory-of-organizations

DuHadway, S., Carnovale, S., & Hazen, B. (2017). Understanding risk management for intentional supply chain disruptions: risk detection, risk mitigation, and risk recovery. *Annals of Operations Research*, *283*(1–2), 179–198. https://doi.org/10.1007/s10479-017-2452-0

Eckstein, D., Goellner, M., Blome, C., & Henke, M. (2014). The performance impact of supply chain agility and supply chain adaptability: the moderating effect of product complexity. *International Journal of Production Research*, *53*(10), 3028–3046. https://doi.org/10.1080/00207543.2014.970707

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: what are they? *Strategic Management Journal*, *21*(10–11), 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)21:10/11

Fainshmidt, S., Wenger, L., Pezeshkan, A., & Mallon, M. R. (2018). When do Dynamic Capabilities Lead to Competitive Advantage? The Importance of Strategic Fit. *Journal of Management Studies*, *56*(4), 758–787. https://doi.org/10.1111/joms.12415

Ferreira, J., Coelho, A., & Moutinho, L. (2020). Dynamic capabilities, creativity and innovation capability and their impact on competitive advantage and firm performance: The moderating role of entrepreneurial orientation. *Technovation*, *92-93*, 102061. https://doi.org/10.1016/j.technovation.2018.11.004

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.1177/002224378101800104

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

Grant, R. M. (2021). *Contemporary Strategy Analysis*. John Wiley & Sons. https://www.wiley.com/en-us/Contemporary+Strategy+Analysis%2C+11th+Edition-p-9781119815211

Hallin, C., & Höök, M. (2023). *Resilient Horizons: Identifying and Overcoming Disruptions in the Semiconductor Supply Chain: From Chip Woes to Chip Wows: Establishing Resilience Strategies in a World of Semiconductors.* Linköping University. https://www.diva-portal.org/smash/get/diva2:1776823/FULLTEXT01.pdf

Handfield, R., Apte, A., & Finkenstadt, D. J. (2022). Developing supply chain immunity for future pandemic disruptions. *Journal of Humanitarian Logistics and Supply Chain Management*, *12*(4), 482–501. https://doi.org/10.1108/jhlscm-09-2021-0096

Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2021). A survey on supply chain security: application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, *8*(8), 6222–6246. https://doi.org/10.1109/jiot.2020.3025775

Hendriks, K. B., & Singhal, V. R. (2016). Managing disruptions in contemporary supply chains. In *Dynamic Supply Chain Alignment*. 311-322. Routledge.

Herath, T. C., Herath, H. S. B., & D'Arcy, J. (2020). Organizational adoption of information security solutions. *ACM SIGMIS Database the DATABASE for Advances in Information Systems*, *51*(2), 12–35. https://doi.org/10.1145/3400043.3400046

Hintsa, J., Gutierrez, X., Wieser, P., & Hameri, A. P. (2009). Supply Chain Security Management: an overview. *International Journal of Logistics Systems and Management*, *5*(3/4), 344. https://doi.org/10.1504/ijlsm.2009.022501

Hoe, S. L. (2008). Issues and procedures in adopting structural equation modelling technique. *Journal of Quantitative Methods*, *3*(1), 76. http://ink.library.smu.edu.sg/sis_research/5168/

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2). https://ui.adsabs.harvard.edu/abs/2018arXiv180501612H/abstract

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling a Multidisciplinary Journal*, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Jonsen, L. (2016). The Significance of Supply Chain Security Practices on Operational Performances among Logistics Providers in Malaysia. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2883417

Kaaria, A. G. (2023). Human resource information systems information security and organizational performance of commercial state corporations in Kenya. *East African Journal of Information Technology*, *6*(1), 256–278. https://doi.org/10.37284/eajit.6.1.1612

Katsaliaki, K., Galetsi, P., & Kumar, S. (2021). Supply chain disruptions and resilience: a major review and future research agenda. *Annals of Operations Research*, *319*, 965–1002. https://link.springer.com/article/10.1007/s10479-020-03912-1

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Journal of Entrepreneurship and Sustainability Issues*, *6*(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37

Kumar, S., & Anbanandam, R. (2019). 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

Kurniawan, R., Zailani, S. H., Iranmanesh, M., & Rajagopal, P. (2017). The effects of vulnerability mitigation strategies on supply chain effectiveness: risk culture as moderator. *Supply Chain Management an International Journal*, *22*(1), 1–15. https://doi.org/10.1108/scm-12-2015-0482

Lawrence, P. R., & Lorsch, J. W. (1967). Differentiation and integration in complex organizations. *Administrative Science Quarterly*, *12*(1), 1. https://doi.org/10.2307/2391211

Li, T. (2013). Establishing an integrated framework for security capability development in a supply chain. *International Journal of Logistics Research and Applications*, *17*(4), 283–303. https://doi.org/10.1080/13675567.2013.861396

Lu, H., Zhao, Y., & While, A. (2019). Job satisfaction among hospital nurses: A literature review. *International Journal of Nursing Studies*, *94*, 21–31. https://doi.org/10.1016/j.ijnurstu.2019.01.011

Magdy, M., Grida, M., & Hussein, G. (2023). Disruption mitigation in the semiconductors supply chain by using public

blockchains. *The Journal of Supercomputing*, *80*(2), 1852–1906. https://doi.org/10.1007/s11227-023-05543-2

McAdam, R., Miller, K., & McSorley, C. (2019). Towards a contingency theory perspective of quality management in enabling strategic alignment. *International Journal of Production Economics*, *207*, 195–209. https://doi.org/10.1016/j.ijpe.2016.07.003

Messina, D., Barros, A. C., Soares, A. L., & Matopoulos, A. (2020). An information management approach for supply chain disruption recovery. *The International Journal of Logistics Management*, *31*(3), 489–519. https://doi.org/10.1108/ijlm-11-2018-0294

Mughal, A. A. (2022). Well-Architected Wireless Network Security. *Journal of Humanities and Applied Science Research*, *5*(1), 32–42. https://journals.sagescience.org/index.php/JHASR/article/view/52

Muñoz, R. M., Andrade, S. M., Peña, I., & Donate, M. J. (2022). Wellness programs in times of COVID-19, perceived organizational support and affective commitment: effects on employee innovative behavior. *European Journal of Innovation Management*, *26*(7), 23–44. https://doi.org/10.1108/ejim-02-2022-0072

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, *44*, 12–22. https://doi.org/10.1016/j.jisa.2018.11.003

Nissen, C., Gronager, J. E., Metzger, R. S., & Rishikof, H. (2018). Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War. *The MITRE Corporation*. https://apps.dtic.mil/sti/citations/AD1108046

Otieno, E. O. (2021). *The Impact of Organizational Culture on Information Security Compliance Culture: a Case of Kenyan Universities* [University of Nairobi Research Archive]. http://erepository.uonbi.ac.ke/handle/11295/157060

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

Park, K., Min, H., & Min, S. (2016). Inter-relationship among risk taking propensity, supply chain security practices, and supply chain disruption occurrence. *Journal of Purchasing and Supply Management*, *22*(2), 120–130. https://doi.org/10.1016/j.pursup.2015.12.001

Patel, K. R. (2023). Enhancing Global Supply Chain Resilience: Effective Strategies for Mitigating Disruptions in an Interconnected World. *BULLET : Jurnal Multidisiplin Ilmu*, *2*(1), 257–264. https://journal.mediapublikasi.id/index.php/bullet/article/view/3482

Podsakoff, P. M., MacKenzie, S. B., Lee, J., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Renay, C. (2020). A framework for fostering a dynamic information security culture. *Cyber Security: A Peer-Reviewed Journal*, *4*(2), 145–159. https://www.ingentaconnect.com/contentone/hsp/jcs/2020/00000004/00000002/art00006?crawler=true&mimetype=application/pdf

Rogelberg, S. G., & Stanton, J. M. (2007). Introduction: Understanding and Dealing With Organizational Survey Nonresponse. *Organizational Research Methods*, *10*(2), 195–209. https://doi.org/10.1177/1094428106294693

Saglam, Y. C., Çankaya, S. Y., & Sezen, B. (2020). Proactive risk mitigation strategies and supply chain risk management performance: an empirical analysis for manufacturing firms in Turkey. *Journal of Manufacturing Technology Management*, *32*(6), 1224–1244. https://doi.org/10.1108/jmtm-08-2019-0299

Schermerhorn, J. R. (2011). *Introduction to Management*. John Wiley & Sons. https://books.google.ie/books?id=wbAmkdoG4O8C&printsec=frontcover&dq=Introduction+to+Management&hl=&cd=1&source=gbs_api#v=onepage&q=Introduction%20to%20Management&f=false

Scholten, K., & Fynes, B. (2016). Risk and uncertainty management for sustainable supply chains. In *Springer series in supply chain management*. 413–436. https://doi.org/10.1007/978-3-319-29791-0_19

Sharma, A., Adhikary, A., & Borah, S. B. (2020). Covid-19′s impact on supply chain decisions: Strategic insights from NASDAQ 100 firms using Twitter data. *Journal of Business Research*, *117*, 443–449. https://doi.org/10.1016/j.jbusres.2020.05.035

Shonhadji, N., & Maulidi, A. (2020). Is it suitable for your local governments? A contingency theory-based analysis on the use of internal control in thwarting white-collar crime. *Journal of Financial Crime*, *29*(2), 770–786. https://doi.org/10.1108/jfc-10-2019-0128

Technology, N. I. N. I. O. S. A. (2019). *Developing Cyber Resilient Systems: a Systems Security Engineering Approach: NIST SP 800-160 Volume 2*. Amazon Digital Services LLC - Kdp. https://books.google.ie/books?id=R904zQEACAAJ&dq=Developing+cyber+resilient+systems&hl=&cd=2&source=gbs_api

Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security*, *108*, 102354. https://doi.org/10.1016/j.cose.2021.102354

Tse, Y. K., Matthews, R. L., Tan, K. H., Sato, Y., & Pongpanich, C. (2016). Unlocking supply chain disruption risk within the Thai beverage industry. *Industrial Management & Data Systems*, *116*(1), 21–42. https://doi.org/10.1108/imds-03-2015-0108

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

Warner, K. S., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, *52*(3), 326–349. https://doi.org/10.1016/j.lrp.2018.12.001

Wieteska, G. (2018). Business Impact Analysis of supply chain disruptions. *The 8th International Conference on*

Management, Economics and Humanities. https://doi.org/10.33422/8icmeh.2018.12.48

Wilden, R., Gudergan, S. P., Nielsen, B. B., & Lings, I. (2013). Dynamic Capabilities and Performance: strategy, structure and environment. *Long Range Planning*, *46*(1–2), 72–96. https://doi.org/10.1016/j.lrp.2012.12.001

Yaacoub, J. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, *21*(1), 115–158. https://doi.org/10.1007/s10207-021-00545-8

Yang, C., & Hsu, W. (2018). Evaluating the impact of security management practices on resilience capability in maritime firms—a relational perspective. *Transportation Research Part a Policy and Practice*, *110*, 220–233. https://doi.org/10.1016/j.tra.2017.06.005

Yang, C., & Wei, H. (2013). The effect of supply chain security management on security performance in container shipping operations. *Supply Chain Management an International Journal*, *18*(1), 74–85. https://doi.org/10.1108/13598541311293195

Yu, W., Jacobs, M. A., Chavez, R., & Yang, J. (2019). Dynamism, disruption orientation, and resilience in the supply chain and the impacts on financial performance: A dynamic capabilities perspective. *International Journal of Production Economics*, *218*, 352–362. https://doi.org/10.1016/j.ijpe.2019.07.013

Zailani, S. H., Subaramaniam, K. S., Iranmanesh, M., & Shaharudin, M. R. (2015). The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy. *International Journal of Physical Distribution & Logistics Management*, *45*(7), 652–673. https://doi.org/10.1108/ijpdlm-12-2013-0286

Zailani, S., Govindan, K., Iranmanesh, M., Shaharudin, M. R., & Chong, Y. S. (2015). Green innovation adoption in automotive supply chain: the Malaysian case. *Journal of Cleaner Production*, *108*, 1115–1122. https://doi.org/10.1016/j.jclepro.2015.06.039

Zaini, M. K., Masrek, M. N., & Sani, M. K. J. A. (2020). The impact of information security management practices on organisational agility. *Information and Computer Security*, *28*(5), 681–700. https://doi.org/10.1108/ics-02-2020-0020

APPENDIX

Table 3. Measurement Items

Organizational Security Culture (OSC)

OSC1: The leadership of this organization considers security culture to be a strategic asset.
OSC2: Management prioritizes security, making it a key concern for all employees.
OSC3: Management establishes supply chain security as a standard practice for all employees.
OSC4: Management actively works to develop a workforce that is focused on supply chain security.
OSC5: Management promotes a culture of vigilance among all employees regarding supply chain security.

SC Security Practices

Facility management security (FMS)

FMS1: Our organization has implemented a fire safety system.
FMS2: The lighting conditions in our facilities are adequate.
FMS3: We have security personnel in place to respond to emergencies.
FMS4: We have identified and designated restricted areas within our facilities.
FMS5: We regularly inspect our security measures to ensure their effectiveness.
FMS6: We limit access to our facilities to only those individuals who are authorized to enter.
FMS7: We utilize camera surveillance systems to enable monitoring of our facilities.
FMS8: We monitor entry points to prevent unauthorized individuals from gaining access to our facilities.
FMS9: We monitor exit points to prevent unauthorized individuals from leaving our facilities.

Human resource management security (HRMS)

HRMS1: We implement a thorough screening process when hiring new employees.
HRMS2: We provide security training programs for all of our employees.
HRMS3: We have procedures in place to identify and verify our employees.
HRMS4: Our organization disseminates security-related information and updates throughout the company.

Information management security (IMS)

IMS1: We have procedures in place to back up data from our computer systems.
IMS2: We maintain records of information for possible security audits.
IMS3: We facilitate data sharing among our supply chain partners.
IMS4: Our organization safeguards business information against unauthorized access and use.

Supply Chain Disruption Occurrence (SCDO)

Internal disruption (ID)

ID1: Internal machine breakdowns negatively impact our business operations.
ID2: Internal utility outages have a detrimental effect on our business.
ID3: Our business suffers due to internal equipment operating outside of specifications.

Supplier disruption (SD)

SD1: Unexpected capacity fluctuations from our suppliers have a negative impact on our business.

SD2: Inconsistent product quality from our suppliers adversely affects our business operations.
SD3: Our business is impacted by poor delivery performance from our suppliers, such as inconsistent delivery times.

Customer disruption (CD)
CD1: Inaccurate information from our customers regarding order quantities negatively impacts our business.
CD2: Unpredictable demands from our customers for product features adversely affect our business operations.
CD3: Our business is affected by orders that involve various combinations of products.