Into the unknown: A qualitative exploration on Cyber Supply Chain Risk Management practices in the Egyptian Context

Yasmine Afifi Mohamed Afifi
Lecturer's assistant , Business Administration, Faculty of commerce, Cairo University

Supervised by:

Abd' Elazez Hashem,
Professor of Business Administration, Faculty of commerce, Cairo University

Raghda Abulsaoud Ahmed Younis
Associate Professor of Business Administration, Faculty of commerce, Cairo University

Abstract

In today's digitally interconnected world, cybersecurity risks in developing countries are rising rapidly in both scale and complexity. As a result, managing these risks from an integrated management perspective has become a strategic necessity rather than a luxury. However, research on Cyber Supply Chain Risk Management (C-SCRM) practices remains scarce, particularly in the Egyptian context. Therefore, this pioneering study explores how C-SCRM practices are conceptualized and implemented within Egypt's financial sector. The study conducted ten in-depth semi-structured interviews with experienced professionals and

analyzed the findings using the Technological-Organizational-Environmental (TOE) framework and ecosystem theory. The results indicate that Egyptian financial institutions face challenges comparable to those of their global counterparts. C-SCRM is a dynamic and adaptive process that mainly depends on both internal preparedness and coordinated actions to collectively or individually manage these cybersecurity risks across the broader financial ecosystem. In addition, the findings reveal that successful C-SCRM implementation requires balancing technological and organizational capabilities with effective inter-organizational collaboration and regulatory alignment. By integrating the TOE framework with an ecosystem perspective, this research enriches the limited body of literature on C-SCRM in developing economies and offers practical insights for policymakers and industry leaders seeking to strengthen the security and resilience of Egypt's financial sector.

Keywords: Cyber Supply Chain Risk Management (C-SCRM), financial sector, Technological-Organizational-Environmental (TOE) framework, ecosystem theory, developing economies

الملخص :

تشهد الدول النامية تزايدًا في حجم وتعقيد مخاطر الأمن السيبراني في ظل الترابط الرقمي المتسارع عالميًا .نتيجة لذلك، أصبحت إدارة هذه المخاطر بمنظور إداري متكامل ضرورة استراتيجية .ومع ذلك، ما تزال الأبحاث حول ممارسات إدارة مخاطر سلسلة التوريد السيبرانية (C-SCRM) محدودة، خاصة في السياق المصري. تهدف هذه الدراسة الرائدة إلى كيفية تصوّر وتطبيق ممارسات C-SCRM

داخل القطاع المالي المصري. اعتمدت الدراسة إلى إجراء عشر مقابلات معمّقة شبه مهيكلة مع عدد من المتخصصين ذوي الخبرة، وتم تحليل النتائج باستخدام إطار التكنولوجيا والتنظيم والبيئة (TOE) ونظرية النظام البيئي. أظهرت النتائج أن المؤسسات المالية المصرية تواجه تحديات مشابهة لتلك التي تواجهها نظيراتها عالميًا. وتبيّن من النتائج أن C-SCRM عملية ديناميكية وتكيفية تعتمد بشكل أساسي على مستوى الاستعداد الداخلي والإجراءات المنسّقة لإدارة هذه المخاطر سواء بشكل فردي أو جماعي ضمن النظام المالي الأوسع. كما كشفت النتائج أن نجاح تطبيق هذه الممارسات يتطلب تحقيق توازن فعّال بين القدرات التقنية والتنظيمية الداخلية من جهة، وتعزيز التعاون بين المؤسسات والتوافق التنظيمي من جهة أخرى. ومن خلال الدمج بين إطار TOE ومنظور النظام البيئي، تسهم هذه الدراسة في إثراء الأدبيات المحدودة حول C-SCRM في الاقتصادات النامية، وتقدّم رؤى عملية لصنّاع القرار وقادة القطاع المالي لتعزيز أمن ومرونة القطاع المالي المصري.

الكلمات المفتاحية: إدارة مخاطر سلسلة التوريد السيبرانية(C-SCRM) ، (، القطاع المالي، إطار التكنولوجيا والتنظيم والبيئة(TOE) ، نظرية النظام البيئي، الاقتصادات النامية

1. Introduction

In today's interconnected world, organizations increasingly rely on diverse technologies that have fundamentally transformed their operations into complex cyber supply chains (C-SC)(Fernando et al., 2023).This digital transformation extends beyond traditional organizational boundaries, and creates networks of interdependencies among partners, suppliers, and other stakeholders across the globe(Friday et al., 2024). In fact, C-SC consist of a comprehensive ecosystem that integrates people, technology components, and processes throughout the

entire product and service lifecycle(Gani & Fernando, 2024). This change has automated and digitalized operations and supply chain management activities (Sadeghi R. et al., 2024). It also has revolutionized traditional supply chain relationships by improving collaboration, visibility and operational capabilities among diverse supply chain partners (Ghadge et al., 2020). To exemplify, advanced digital technologies like digital platforms now allow organizations to track operations in real-time, share critical data securely, and optimize processes across multiple stakeholders(Ivanov, 2021)

However, several scholars and practitioners have expressed growing concern about the surging rate of emerging cyber threats that disrupt the entire supply chain ecosystem (Aarland, 2024; Jazairy et al., 2024; Sadeghi R. et al., 2024). To clarify, when organizations integrate their systems and share data with multiple partners, each connection potentially creates new and unforeseen vulnerabilities for cyber threats that present have both known and unknown cyber risks (Cheung et al., 2021). In response to emerging cyber threats, there is a growing strategic necessity to manage risks from an integrated management perspective rather than a purely technical one (Creazza et al., 2022; Pandey et al., 2020). A single focal organization cannot adequately protect exposures to different significant vulnerabilities into critical systems and infrastructure across the entire ecosystem(Gani et al., 2023; Gani & Fernando, 2024). Instead, this end-to-end C-SCRM approach can protect

against emerging cybersecurity risks by fostering relational connections and collaborations between various stakeholders (Friday et al., 2024). C-SCRM was described as a systematic process for managing exposures to different cybersecurity risks (Fernando et al., 2023; Gani et al., 2023; Gani & Fernando, 2024). However, to date, research on C-SCRM remain limited (Jazairy et al., 2024).

While previous empirical studies have mainly examined C-SCRM practices within the manufacturing sector (Fernando et al., 2023; Gani et al., 2023; Gani & Fernando, 2024), there remains a notable research gap concerning their application in other critical industries like the financial sector. This gap highlights the need for an in-depth exploratory study to generate comprehensive understanding of C-SCRM practices in the financial sector. Therefore, this study aims to address this gap by investigating the following research questions:

RQ1. **How can C-SCRM practices be conceptualized and implemented in the financial sector to manage cybersecurity risks within the cyber supply chain ecosystem?**

RQ2. **What are key factors influencing the implementation of C-SCRM?**

In this regard, this study employs two main theoretical frameworks to investigate C-SCRM practices and associated challenges within the Egyptian financial sector. First, ecosystem theory (Adner, 2017) that provides a comprehensive lens for

understanding C-SCRM practices that could extend beyond focal organization and require complex network of relationships and interdependencies. This theoretical foundation enables deep analysis of how C-SC create both opportunities and vulnerabilities in C-SCRM. Second, the TOE framework provides a comprehensive theoretical lens for understanding different challenging factors that influence implementation of C-SCRM practices. This framework examines three key contextual elements (technology, organization and environment) that influence organizational decision-making and implementation processes.

The remainder of this paper is organized as follows: The next section provides an overview of recent literature on C-SCRM. Section Three introduces the theoretical frameworks underpinning the study. Section Four outlines the research methodology adopted for this study. Section Five presents and discusses the findings of the qualitative study. At the end, the paper offers a brief conclusion, followed by discussion of limitations and proposed directions for future research.

2. Literature review

Cybersecurity risks have emerged as one of the top risks in 2024 and are expected to significantly impact the global landscape over the next decade (World Economic Forum, 2024). Perhaps the best way to manage those different cybersecurity risks is to start understanding what they mean. One common definition is that any risks emerge from the use of IT system that could compromise

three fundamental aspects of security, including confidentiality, availability and integrity(Eling & Schnell, 2016). Another perspective viewed cybersecurity risk as an event involving exposure to danger or loss(Pandey et al., 2020).

As evident in the literature, cybersecurity risks can be categorized into three distinct classifications: The first classification depends on the nature of the activity, differentiating between criminal and non-criminal incidents. Criminal incidents typically involve intentional efforts to compromise systems for malicious purposes, whereas non-criminal incidents might result from unintentional errors or system failures that create security vulnerabilities (Colicchia et al., 2019; Creazza et al., 2022). The second classification focuses on the type of target attacks such as malware deployment, insider attacks leveraging internal access, spam campaigns targeting users, and distributed denial of service (DDoS) attacks (Ghadge et al., 2020). The final classification is based on the source of the risk as proposed by Pérez-Morón (2022) who categorized risks based on the source into three dimensions. First, supply risk emerges from interactions with external vendors and suppliers including potential threats from inaccessible supplier systems, theft of vendor credentials, breaches within vendor networks, and malicious modifications to source code through malware. Second, operational risk focuses on internal processes and systems, such as plant malfunctions, unexpected operational disruptions, coding error detection

failures, product specification fraud, and data theft. Finally, customer risk addresses threats related to end-user interactions and data protection, including intellectual property theft, unauthorized data access and manipulation, fraudulent communications, and unauthorized payment gateway access.

Furthermore, recent reports have revealed that the number of cybersecurity incidents in the financial sector rose dramatically from 1,829 in 2022 to 3,348 in 2023(Statista, 2023). This sharp upward trend highlights huge cybersecurity challenges to the financial sector. Similarly, the International Monetary Fund (2024) stated that these cybersecurity risks in the financial institutions not just disrupt day-to-day operations but also potentially destabilize entire financial markets and shake public confidence in the financial system. As financial institutions form the backbone of our economic stability, this concerning increase in cyber incidents calls for an urgent review and strengthening of current practices and defense mechanisms.

According to Global Cybersecurity Index (GCI) 2023-2024, Egypt stands among role modelling group of 47 nations and ranks within the top 12 countries globally (ITU, 2024). This remarkable achievement reflects Egypt's commitment to advance its national cybersecurity capabilities, frameworks, and preparedness. It worth noting that Egypt achieved a perfect score of 100 points across all evaluation criteria, marking substantial progress from its 2020 score of 95.48 points. This improvement

indicates Egypt's successful implementation of robust security frameworks and its dedication to maintaining high standards in cybersecurity practices.

At the same time, Egypt ranks 50th among the top breached countries in 2023(Surfshark, 2023). According to the National Telecommunications Regulatory Authority (NTRA), Egypt ranks among the top 20 vulnerable countries to cyberattacks. Furthermore, according to Incident Response Team (EG-FinCIRT), the financial sector confronts an increasing rate of cyber threats, including vendor updates, zero-day vulnerabilities and rising malware with 137 critical, 375 high, and 148 medium-severity (EG-FinCIRT, 2023). This highlights an important gap between development and practical implementation of the practices that address and manage cybersecurity risks. While Egypt has established robust cybersecurity frameworks and strategies, earning recognition in the GCI, the high number of successful breaches indicates ongoing challenges in operationalizing these capabilities across all sectors.

However, while Egypt's overall cybersecurity progress, there remains a critical need to examine specific C-SCRM practices within the financial sector. The increasing digitalization of financial services and growing interconnectedness among supply chain partners creates new vulnerabilities that require detailed investigation. Understanding how financial institutions implement C-SCRM practices becomes crucial for managing

different emerging cybersecurity risks maintaining this cybersecurity excellence, particularly as cyber threats continue to evolve and become more sophisticated.

Extant literature shed light on the relevance and significance of C-SCRM approach for managing cybersecurity risks in cyber supply chains(Colicchia et al., 2019; Creazza et al., 2022; Fernando et al., 2023; Gani et al., 2023; Gani & Fernando, 2021, 2024). C-SCRM practices are meant to identify, assess, mitigate and manage cybersecurity risks within the entire ecosystem (Colicchia et al., 2019; Creazza et al., 2022; Fernando et al., 2023; Gani et al., 2023; Gani & Fernando, 2021, 2024). Specifically, three foundational practices include governance, systems integrations and operations to establish comprehensive end-to-end supply chain control that enables continuous adaptation to emerging challenges (Boyson, 2014; Fernando et al., 2023; Gani et al., 2023; Gani & Fernando, 2021, 2024).

Furthermore, multiple empirical studies extensively examined C-SCRM practices in the manufacturing sector (Fernando et al., 2023; Gani et al., 2023; Gani & Fernando, 2021). However, to date, C-SCRM research in the financial sector has underdeveloped (Uddin et al., 2020). This gap is particularly significant given the sector's critical role in national infrastructure and its unique cybersecurity challenges. Therefore, investigating C-SCRM practices in Egyptian financial sector would provide valuable insights for maintaining and enhancing the country's distinguished position in global

cybersecurity rankings.

3. Conceptual background

The concept of supply chain risk management (SCRM) has been highlighted clearly in management research that mainly focused on identifying, assessing, and mitigating various risks such as operational, supply, or demand risks that can affect the flow of goods and services from suppliers to customers (Guerra et al., 2024). C-SCRM represents an evolution of traditional supply chain risk management (SCRM) by explicitly incorporating cyber security issues into managing the risks associated with supply chains(Fernando et al., 2023; Friday et al., 2024; Gani et al., 2023; Gani & Fernando, 2024; Melnyk et al., 2022). Cyber risks have been considered as equally important as other traditional risks because of the increasing use of digital technology and connectivity in modern supply chains(Herburger et al., 2024). Consequently, scholars and practitioners acknowledge that digital processes, data flows, and interconnected IT systems brought new vulnerabilities that require an integrated management approach(Gani & Fernando, 2024; Gaudenzi & Baldi, 2024; Herburger et al., 2024).

In this regard, C-SCRM was defined as the management approach designed to identify, assess, and mitigate risks that steam from cyber threats throughout the entire IT/OT supply chain (Pandey et al., 2020). To a similar extent, Gani and Fernando (2024) defined C-SCRM as a comprehensive

integration of cybersecurity, enterprise risk management, and supply chain management to address the unique risks posed by evolving threats in cyber supply chains. This comprehensive approach extends beyond traditional technical security measures to encompass both managerial and human controls across the entire supply chain ecosystem.

Current literature reveals confusion in terminology and concepts related to C-SCRM practices. Scholars and practitioners highlight the need for tailored methodologies to manage cyber risks across different industries and organizations(Friday et al., 2024; Gani & Fernando, 2024). For instance, Hasan et al. (2021) The level of an organization's awareness, preparedness and commitment to prevent and combat cyber-attack.

Friday et al. (2024) proposed some of a set of practices that might improve supply chain cybersecurity such as information sharing, joint decision making, alignment of incentives, standard guidelines and supply chain integration. In contrast, Jazairy et al. (2024) emphasized on the different strategic C-SCRM activities including risk identification, protection, detection, response and recovery that could improve the performance of supply chain in terms of two dimensions cyber resilience and robustness. Furthermore, other scholars attempt to propose foundational practices of C-SCRM practices that could be placed to improve cyber supply chain performance based on three dimensions including, governance, system

integration and operations (Boyson, 2014; Fernando et al., 2023; Gani et al., 2023; Gani & Fernando, 2021, 2024). The study adopted the latter foundational key C-SCRM practices and defined it as a set of distinct but complement activities

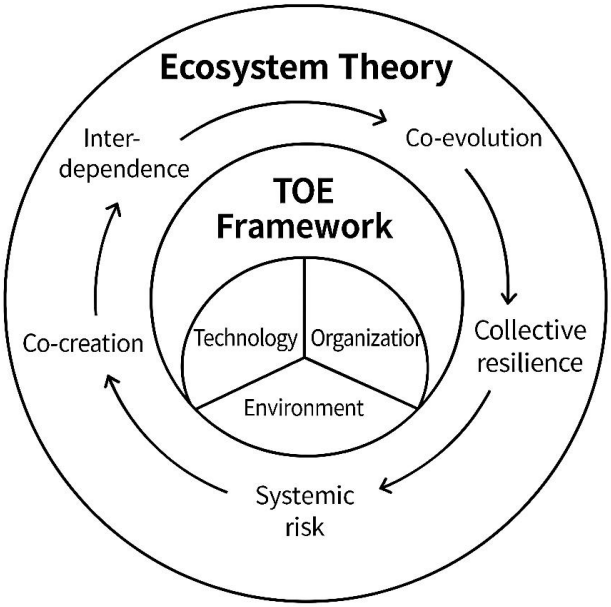
Furthermore, the implementation of these practices varies across countries, sectors and organizations. With respect to the researchers' best of knowledge, there is no scientifically based scale of C-SCRM practices in the financial sector so far. Therefore, C-SCRM practices might differ from those of manufacturing contexts(Fernando et al., 2023; Gani et al., 2023). Therefore, this study adopts two main theoretical frameworks to understand the nature and implementation of C-SCRM practices in the Egyptian financial sectors. First, Ecosystem theory provides valuable insights into how different actors within the financial sector conceptualizes and implement C-SCRM practices (Adner, 2017). This perspective highlights the importance of integration of C-SCRM efforts across the supply chain. Organizations cannot view their cybersecurity in isolation but must consider how their practices affect and are affected by other ecosystem members. This requires developing comprehensive risk management strategies that account for both direct and indirect relationships within the supply chain network (Adner, 2017).

Furthermore, this study employed the technology-organization-environment-framework to understand the challenging factors influencing implementing C-SCRM practices in Egypt that was originally proposed by Depietro and Fleischer (1990). This

framework has emerged as a valuable theoretical lens to analyze C-SCRM implementation due to its comprehensive and adaptable nature. For instance, Hasan et al. (2021) captured key factors affecting the cyber security readiness of organizations including IT infrastructure, top management support, organizational skills, organizational culture, collaboration with competitors, supplier/partner relationships, government regulations, government support, and industry standards.

Figure 1

Embedding the TOE Framework within Ecosystem Theory



***Source*: authors own work**

4. Methodology

This study adopted a qualitative exploratory research design to investigate C-SCRM practices within the Egyptian financial sector. The exploratory nature of this study was deemed appropriate due to the scarcity of empirical research examining C-SCRM implementation in emerging market contexts, particularly within the Egyptian financial context, which requires

an in-depth understanding of current practices and challenges.

A purposeful sampling strategy was employed to select participants with different professional backgrounds and expertise relevant to C-SCRM practices. Specifically, criterion-based purposeful sampling was used to ensure participants possessed knowledge and experience in information security, network security, risk management, or audit functions within Egyptian financial institutions. The sampling criteria included: (1) minimum three years of experience in relevant areas such as information security, network security, or risk management roles (2) and current employment in the Egyptian financial sector.

The final sample consisted of ten participants who were from different backgrounds in the Egyptian financial sector as shown in Table 1. It is worth noting that for confidentiality's sake, participants who were assigned as P1, P2 and so on, up to P10. While this sample size is small, it is considered sufficient for exploratory purposes to reach data saturation and obtain enough perspectives about C-SCRM in the Egyptian context(Clarke & Braun, 2013).

Semi-structured interviews served as the primary data collection method. This approach was selected for its ability to provide flexibility in exploring participants' lived experiences and perspectives while maintaining sufficient structure to address key research themes. These interviews consist of open-ended questions to seek different perspectives of conceptualizing and

practicing C-SCRM. The final interview protocol was developed to discuss topics about C-SCRM practices and implementation challenges including 4 questions. some of the interview questions were adapted from relevant research (Tonn et al., 2019). This guide primarily incorporates open-ended questions, with additional follow-up and closed-ended questions to obtain clarification or elaboration on participants' responses. The average duration of each interview ranged from 60 to 90 minutes. Six interviews were conducted face-to-face, while the others were carried out over the phone. The participants were assured about their identities and responses would be kept anonymous and confidential to encourage their participation. Throughout these interviews, the researcher diligently took notes. Another two participants refused the full interview in person due to the scheduling conflicts and requested a questionnaire to supplement the conversation. These in-depth interviews were conducted till the theoretical saturation was reached as determined by the diversity of participant perspectives and the emergence of consistent concepts and themes within the data.

Table 1

Overview of Participants

Participants	Position
1	Technical Information Security Manager
2	IT Director
3	Business Information Security Manager

4	Identity and Access Management Senior officer
5	Applications and Cybersecurity Team Leader
6	Network and Cybersecurity Senior Officer
7	Business Information Security Manager
8	SOC analyst
9	Security architect
10	IT Director

***Source*: authors own works**

After the collection, interview transcripts were shared with participants for review and verification to ensure their reliability. Furthermore, the data were coded manually using excel sheets and analyzed through an experiential thematic analysis which based on subjective experiences and perspectives of participants(Creswell, 2015). The analysis began by identifying subsets of data that represent meaningful concepts, ideas, or patterns. These codes were typically assigned as short phrases or labels that capture the essence of the data. Subsequently, the codes were organized into overarching themes and patterns that provided insights into the research questions and objectives for more details see Table (2) and Table (3). Finally, the identified themes were reviewed and refined to ensure accurate representation of the data and coherent interpretation of participants' perspectives.

Table 2

Generation of initial codes from primary data

Initial Code	Examples of representative quote	Reference
Implementing CBE cybersecurity framework	Our financial sector is adopting the CBE Cybersecurity guide to manage cybersecurity risks.	P1
Conducting risk assessments	We assess cyber risk security maturity and work on them to implement security controls per our policies and standards.	P3
Developing security policies and standards	We follow a defined C-SCRM guideline based on CBE	P10
Hiring security personnel	This period we tried to deal with CBE assessment by hiring employees to perform certain function	P5
Training employees on cybersecurity	This move is not just about crisis management; it is a clear demonstration of the importance of proactive, collaborative defense strategies in the face of evolving cyber threats	P1
Auditing vendors and suppliers	We conduct regular cybersecurity audits of our vendors and suppliers, as mandated by the CBE, to ensure the integrity of our extended network	P3
Monitoring and scanning for threats	Continuous monitoring is a cornerstone of CBE strategy. The team employ security ratings services, network scans, and log data analysis to keep a vigilant eye on supplier environments	P5
Responding to cyber threats	In the wake of supply chain cyberattacks, the CBE usually sends an alert to all banks	P1
Cultivating leadership buy-in	CBE's cybersecurity framework highlighted the importance of leadership buy-in. It's not just about having policies, but about making them a lived reality	P3
Investing in cybersecurity	Adapting to the CBE's cybersecurity standards requires significant investment, a hurdle particularly for smaller banks with limited resources	P5
Reducing security incidents	Since implementing enhanced cybersecurity measures, we've noticed a significant reduction in security incidents, contributing to a stronger trust bond with our customers	P3
Supply chain cyber security	The CBE's focus on third-party cybersecurity has led us to develop robust protocols for vendor management, ensuring that every link in our chain is secure	P4
Building trust with customers	Strengthening our cybersecurity posture has had a positive impact not just on security, but also on our organization's reputation and market standing	P4
Collaborating with regulators	It underscores the critical role of regulatory bodies in guiding and safeguarding the financial ecosystem against emerging cyber threats	P1

Initial Code	Examples of representative quote	Reference
Reduced Downtime and Increased Resilience	**The proactive cybersecurity measures we've adopted have significantly reduced downtime and disruptions, demonstrating our increased resilience in practical terms. I think that in line with regulatory requirements, has built a resilient infrastructure capable of withstanding evolving cyber threats**	**P2**
Managing third-party risks	**Managing third-party cybersecurity risks requires collaborative effort. We work closely with our vendors to adhere to the cybersecurity standards set by the CBE**	**P5**
Adapting to evolving threats	**The evolution of digital banking has brought cybersecurity to the forefront of our operational priorities. Protecting our clients' financial information is paramount**	**P2**
Cultural shifts	**Implementing the CBE's cybersecurity regulations is not just a technical challenge; it also demands a cultural shift within financial institutions towards security-first thinking**	**P1**
Emerging technologies adoption	**Although the use of emerging technologies brought us different cyber-attacks, organizations and individuals can use them too for security purposes. The more we are surrounded by AI driven attacks, the more we need to involve these technologies to detect them earlier.**	**P7**

Note: **P; participant**

Source**: authors own work**

Table 3

Generation of final themes by combining sub-themes

Final Themes	Subthemes	Description	Codes
C-SCRM Practices	Governance	References to following regulations and guidance from CBE	Implementing CBE cybersecurity framework Conducting risk assessments Developing security policies and standards Auditing vendors and suppliers Collaborating with regulators Hiring security team
	Systems integration	Collaboration among firms, regulators, supply chain, and customers to enable effective decision making	Auditing vendors and suppliers Managing third-party risks
	Operations	The development and implementation of daily cybersecurity measures	Monitoring and scanning for threats. Responding to cyber threats Adapting to evolving threats
C-SCRM Outcomes	Cyber supply chain performance	Internal security performance perspective, external security performance, resilience	Reducing security incidents Supply chain cyber security. Reduced Downtime and Increased Resilience
Contextual Factors	Organizational factors	Resource constraints Management support Cybersecurity culture,	Firm size Culture
	Technological factors	Emerging technologies	use of data analytics, API, cloud computing, AI, two
	Environmental factors	Regulations Collaboration	Regulator, regulatory role
	Relational factors	Trust Interdependence	

***Source*: authors' own work**

5. Findings

This section presents the key results derived from the exemplary quotations of personal comments and notes on the interviews undertaken. The main aim of the interviews was to gain various insights into the nature of C-SCRM practices in the financial sector. in addition, the interviews aimed to provide some of the challenges for implementing C-SCRM practices.

5.1 The nature of C-SCRM practices in Egypt

All participants had confirmed that The Central Bank of Egypt (CBE) and the Egyptian Financial Regulatory Authority (FRA) developed and published comprehensive cybersecurity frameworks to provide all the banking and non-banking financial institutions with best practices, standards, and requirements that put in place to identify, assess, and mitigate cyber-related risks that can affect the financial ecosystem. However, some of these practices were mandatory, and others are advisable depending on the criticality of the situation. As P1 stated, "*Our financial sector is adopting the CBE Cybersecurity guide to manage cybersecurity risks. Since 2021, CBE sent us this framework to strengthen cybersecurity posture and protect against evolving cyber threats*".

In addition, multiple participants believed that CBE plays an important regulatory role and provides guidelines that consist of security policies and programs to manage cybersecurity risks. This framework includes governance practices such as establishing risk management processes. *"We follow a defined SCRM guideline based on CBE. Firstly, we assess cyber risk security maturity and work on them to implement security controls per our policies and standards. We do our best to follow the formal C-SCRM program based on well-defined processes."* Other participants mentioned that CBE cybersecurity framework may require creating dedicated cybersecurity teams and training to build expertise. As exemplified by P5, "*This period we tried to*

deal with CBE assessment by hiring employees to perform certain functions and conduct plans for raising current and future employment awareness about cybersecurity risks".

Furthermore, all participants agreed that the CBE framework introduced many practices related to managing multitier supply chain cybersecurity risks. Several responses acknowledged the importance of securing the entire supply chain networks through vendor audits, assessments, collaboration, and monitoring. For instance, P2 reported that *"In our bank, we implement strict compliance checks in line with CBE's directives. Recently, we developed supplier risk assessment questionnaires that require all suppliers to complete a cybersecurity questionnaire and conduct onsite audits for high-risk partners."*

Other responses viewed that implementing C-SCRM practices no longer becomes the sole internal responsibility of focal financial institution, but also the entire supply chain that requires collaborative efforts of all stakeholders. This supports the importance of ensuring the security of all nodes in the network to maintain the resilience of embedded systems in the financial ecosystem. For instance, P4 *"The CBE's focus on third-party cybersecurity has led us to develop robust protocols for vendor management and ensure that every link in our chain is secure."* This can be done by establishing maintaining sustainable relationships with supply chain partners as reflected by P5: *"Managing third-party cybersecurity risks requires*

collaborative effort between our internal environments with Fintech companies, our developers our vendors, other cybersecurity service providers to adhere to the cybersecurity standards set by the CBE".

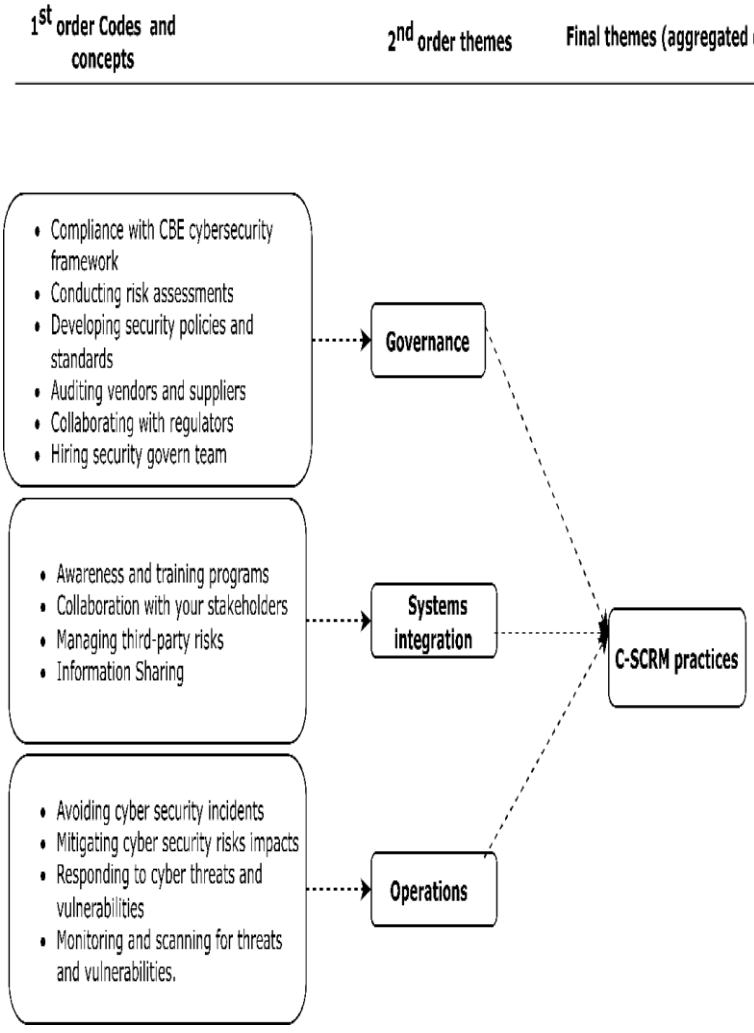
As well as the role of regulatory role of CBE, it always plays continuous monitoring role in ensuring the security posture of financial sector in Egypt referring to the recent attacks taken. As illustrated by P1:

*"*In the wake of supply chain cyberattacks, the CBE usually sends an alert to all banks. It guides and safeguards the financial ecosystem against emerging cyber threats. This move is not just about crisis management; it is a clear demonstration of the importance of proactive defense strategies in the face of evolving cyber risks.*"*

Additionally, there is a common agreement among participants about the importance of sharing reliable and accurate information role among supply chain partners. In the words of P7*: "In the cyber welfare age, supply chain transparency isn't just beneficial; it's essential. You must know what you need to protect then trace the origins of vulnerabilities and respond more swiftly to potential threats."* However, the level of visibility may differ across entities based on the type of data itself. P7 mentioned that *"Although CBE enable us to have authority to have a complete visibility in our supply chain partners, we currently monitor all published assets rather their internal assets."*

Figure 2

Coding representation of C-SCRM practices



Source: authors own work

5.2 Theme 2: factors influencing C-SCRM practices implementation

Several challenges were found that participants face, especially for smaller entities with limited resources. These challenges include the need for significant investment and a "cultural shift" towards security-first thinking, as stated by P1 *"Implementing the CBE's cybersecurity regulations is not just a technical challenge; it also demands a cultural shift within financial institutions towards security-first thinking."*

Most of participants agreed that there is also a shortage of cybersecurity skills and talent within the sector. P2 mentioned *"The rigorous demands of the CBE's cybersecurity framework underscore the need for hiring cybersecurity experts and professionals and enhanced skills and training within the banking sector, and this is what we are currently working on*". Also, specific personnel must be recruited for cyber defense and governance roles to meet CBE framework requirements, explained by P4 *"CBE proposed a cybersecurity structure of key functions essential to implement. This necessitates the recruitment of additional personnel to undertake specific tasks related to cyber defense and information security management governance."* Additionally, different vacancies must be addressed to fulfill the audit demands described by P5.

Further, top management support is another critical factor. When leaders are genuinely committed to a policy, their support can help ensure that the policy is not just a formal document but is formally practiced. This is implied by P3 *"CBE's cybersecurity framework highlighted the importance of leadership buy-in. It's not just about having policies, but about making them a lived reality."*

Moreover, not all the participants have a basic understanding of the concept of Industry 4.0. That is why the researcher provided them with some examples of Industry 4.0. Unlike other industries, the FinTech industry has accelerated the use of disruptive technologies to provide and improve existing financial services and systems. P1 stated that "*The FinTech industry in Egypt has undergone a digital transformation that is beneficial for both clients and companies.*" He added:

"The adoption of mobile applications, e-registration, e-KYC, e-applications, e-contracts, e-signatures, and e-disbursements through digital wallets, POS terminals, and cards enables more convenient for clients to apply for loans and signing them electronically. On the other hand, adopting mobile apps, customer relationship management systems, loan origination systems, and loan management systems with recovery and field officer components has significantly boosted operational efficiency and customer service for companies. Additional disruptive technologies like chatbots, robotic process

automation, optical character recognition, AI-powered image recognition, process mapping, and machine learning have further enhanced operations by improving accuracy and efficiency".

Therefore, the FinTech industry relies more on mobile applications and devices which make it vulnerable to data breaches, fraud, and compliance violations. P3mentioned "*With every new technology, there is a risk of unknown threats and vulnerabilities".*

There are conflicting views raised by the participants about the strategic role of emerging technologies. Some believe it increases cyber threats. For instance, P4 mentioned that *"I believe that AI-driven attacks increased these days because of the extensive use of custom ChatGPT bots to exploit vulnerabilities or entry points."* Others highlight the importance of leveraging these technologies like APIs and two-factor authentication for security (P2,7 and 8). P2 mentioned that "*APIs application programming interface software act as the digital gatekeepers which enforce security protocols and ensuring a robust defense against cyber threats, making them indispensable in fortifying our digital landscapes*." Regarding two factor authentication, P7 stated that "*Egyptian financial sector recognizes the importance of robust security, embrace two-factor authentication as shield against unauthorized access, safeguarding the wealth and trust of their valued customers.*" However, there is common consensus that the more digital payment methods are used, the greater the need for

cybersecurity measures to implement to protect sensitive financial data such as authentication, device security, and encryption.

Furthermore, some mentioned that not all the emerging technologies have been adopted in the entire sector. For example, The CBE prohibited the adoption of cloud computing services for local banks to ensure the security in terms of availability, confidentiality, and integrity of these sensitive financial data and financial systems. As illustrated by P9: "*Storing data on public cloud platforms can cause data breaches and loss of control over the country's financial information*". Although cloud services platforms have not been widely adopted by banks, some fintech companies have currently used them. There is increasing collaboration between banks and fintech companies, as well as with other support service providers such as software technology companies. This collaboration increases the attack surface and complexity of security management, especially if proper enterprise application integration is still lacking.

P7 stated: *Although emerging technologies brought different cyber-attacks to us, we can use them for security purposes as well. The more you are surrounding by AI driven attacks, the more need to involve these technologies to detect them earlier."*

6. Discussion

This qualitative study explores the concept of C-SCRM

within an emerging economy context. The study proposes novel insights into the contextual factors that shape C-SCRM practices in the financial sector. The results clearly showed that the financial sector, much like its counterparts in other parts of the world, faces various cybersecurity risks that need to be addressed and managed rather than prevented

The interconnected financial ecosystem: the findings of the study demonstrate that the Egyptian financial sector operates as an interdependent and interconnected ecosystem of suppliers, customers, regulators, technology providers, and other stakeholders (Adam, 2021). This evolving perspective highlights the necessity of understanding relational factors such as dynamic interactions and co-dependence among various actors in the financial ecosystem (Jazairy et al., 2024) or trust(Hampton et al., 2021). This interconnectedness presents both opportunities and vulnerabilities. The findings reveal that a security breach in one part of the network, whether with a supplier or third-party partner, can generate ripple effects throughout the entire ecosystem. This finding aligns with previous research emphasizing the cascading effects of cyber risks in interconnected systems (Aarland, 2024; Colicchia et al., 2019; Pandey et al., 2020). Indeed, these results reflect a growing recognition that managing cyber risks within complex digital ecosystems require dynamic interactions and co-dependencies among multiple stakeholders, including suppliers, service providers, regulatory bodies, and customers(Jazairy et al., 2024). The study also reveals that focal institutions are encouraged to not only secure their internal

processes but also collectively collaborate with their ecosystem members to ensure comprehensive protection across the network(Aarland, 2024; Friday et al., 2024).

When financial institutions engage in information sharing, align cybersecurity standards, and collaborate on risk management strategies, they enhance the entire ecosystem's collective capacity to detect, respond to, and recover from cyber threats.

Concept evaluation: A key finding of this study is the clear distinction between C-SCRM concepts and constructs. The concept of C-SCRM pertains to theoretical understanding of practices related to identifying, assessing, and mitigating risks across the cyber supply chain. In contrast, the construct of C-SCRM refers to its operationalization through various indicators or dimensions. The findings suggest that bridging the gap between conceptual understanding and practical implementation remains a key challenge for many institutions.

Three-dimensional construct: the study findings confirm that C-SCRM practices can be conceptualized through three dimensions: governance, system integration, and operations. These dimensions align with prior research (Boyson, 2014; Fernando et al., 2023; Gani et al., 2023; Gani & Fernando, 2021, 2024; Guerra et al., 2024). Furthermore, the study reveals unique characteristics within the Egyptian financial context where key practices were categorized in this study based on their functional roles by type (people, process and technology) and criticality

(mandatory or advisable). This classification serves as a strategic tool to guide implementation priorities which may vary across financial institutions.

Governance: This study clearly defined governance as the structured mechanism of setting clear policies and make decisions based on guidelines as issued by the CBE and FRA cybersecurity frameworks to effectively manage cyber risks in the Egyptian financial Ecosystem. In this study, key components of governance were identified as processes and practices of decision-making structure, policy and procedures in terms of compliance, formal risk management, continuous risk monitoring, asset management, change management, disaster recovery planning, and business continuity planning. According to the results, governance also has clear processes for accountability and control where roles and responsibilities of individuals, or groups have been defined for meeting objectives or addressing issues, ensuring that corrective measures are taken on time. As per most participants' responses, this study reveals there is strong evidence suggesting that many financial institutions in Egypt are still in the early stages of establishing structured cybersecurity governance, with implementation efforts varying in both depth and maturity across institutions. Responsibilities, such setting cybersecurity policies, monitoring cyber risk levels, and making decisions to secure the digital

infrastructure, are still being defined and assigned under the supervision of the CBE and FRA. In practice, this study reveals new cybersecurity roles that have been proposed such as SOC analysts, SOC managers, business continuity analysts, data custodians, and security engineers in the financial sector to manage cybersecurity risks. This critical finding reinforces earlier studies that referred to the talent shortage emerged a significant inhibitor factor to effective implementation of C-SCRM (Hasan et al., 2021; Orji & U-Dominic, 2024).

System integration: this study also defined system integration as the process of coordinating and aligning various embedded systems, software applications or solutions to work as a unified and cohesive unit. This system integration was proposed to include internal and external systems integration where it effectively works to enable seamless secure information flow and coordinated operations across the entire network. This finding also supports prior work that integration allows systems to automatically exchange data and information which also in turn stop cyberattacks before they cause harm to focal financial institutions and to the entire supply chain(Fernando et al., 2023; Gani et al., 2023; Jazairy et al., 2024). Also, participants mentioned that there is continuous integration among various actors in the financial ecosystem who work in parallel to manage cybersecurity risks.

Operations: this study conceptualized operations as

human-driven processes, policies, and steps that ensure that systems and users are well prepared to prevent and respond to potential threats effectively. In the Egyptian financial ecosystem, participants defined practical processes that financial institutions employed to maintain cyber hygiene by continuously monitor and scan for threats, respond, handle and recover from cyber-attacks. Key subcomponents of operational procedures were identified to include threat intelligence, regular audits and assessment, security incident and event monitoring (SIEM), incident response plans, communication protocols, and employee training and awareness programs. This finding aligns the previous studies that demonstrated that operations in C-SCRM are all about putting in place, managing, and continuously improving the practical measures that ensure cybersecurity threats are effectively managed in a daily basis(Gani et al., 2023; Gani & Fernando, 2024)

According to the results of this study, cybersecurity risks have become unavoidable and emerged from anywhere in the network. Given the diverse nature of financial services and the varying levels of risk exposure, a one-size-fits-all approach to C-SCRM is unlikely to be effective. Instead, a shift towards more customizable and flexible C-SCRM practices that can be tailored to the specific needs and different risk profiles of different entities within the ecosystem. This would allow for more effective management of cyber risks in a way that is aligned with

each institution's operational realities and business objectives.

Contextual factors influencing C-SCRM practices: this qualitative study sheds light on key challenging factors influencing C-SCRM. Drawing from the Technology–Organization–Environment (TOE) framework and ecosystem theory, these factors can be classified into technological factors, organizations factors, and environmental factors.

Technological factors: Two technological factors: the extent of digitalization, and digital competencies were proposed. The extent of digitalization refers to how an organization adopts digital tools into its operations. This implies the transformation from traditional methods to digital approaches and is essential because the more digital an organization becomes, the more it relies on robust IT systems to secure its operations. Implementation of technologies includes the actual deployment and use of technological solutions (including hardware, software, and related IT systems). The extent to which these technologies are implemented influences an organization's readiness for cyber-security, as advanced and well-integrated technologies form a key defensive layer against cyber-attacks. This study also supports the ongoing debate about the paradoxical role of emerging technologies in cybersecurity(Arroyabe, Arranz, de Arroyabe, et al., 2024; Ivanov, 2021; Pandey et al., 2020). Some of participants argued that technological advancements bring new opportunities for enhancing operations but also create new

vulnerabilities. For example, the rapid advancement of artificial intelligence has made it possible for attackers to exploit system weaknesses using AI-driven attacks. On the defense side, some institutions have begun to adopt robust security measures such as application programming interfaces (APIs) and two-factor authentication to further secure their network. Also, the study shed light on the digital maturity of the financial institutions, where local financial banking institutions were restricted to adopt cloud computing technologies as infrastructure.

Digital competencies refer to the level of digital skills and competencies within an organization which could impact the ability to implement and manage cybersecurity effectively. Also, this dimension was supported by technological factors that could influence(Arroyabe, Arranz, Fernandez De Arroyabe, et al., 2024)

Organizational factors: The results of this study found that talent with right skills gaps, resource constraints, and driving cultural shifts were identified as organizational factors in this study. As previously mentioned, the shortage of cybersecurity talent within financial institutions where they do not always have enough skilled professionals to manage and mitigate risks. Participants highlighted the need for significant investment and cultural transformation towards "security first thinking". top management support was identified as crucial for translating cybersecurity policies from formal documents into practiced reality. This finding is consistent with

Additionally, the size of an institution was considered an important organizational factor. The size of an institution often influences the way it governs itself. For example, a larger institution usually has more complex systems of governance to manage its diverse operations and many stakeholders. This means that large financial institutions often have multiple layers of management, formalized policies, and more structured decision-making processes where larger financial institutions are typically more capable of implementing complex systems and adhering to cybersecurity protocols compared to smaller organizations. Furthermore, the size of an institution also plays a role in its relationship with external influences like regulators, investors, and suppliers. For instance, a large organization with a significant market share tends to have more power and influence over regulatory changes and supplier agreements. This size-driven influence might mean that these institutions can negotiate more favorable terms or might be subject to stricter regulatory compliance due to their considerable impact on the economy

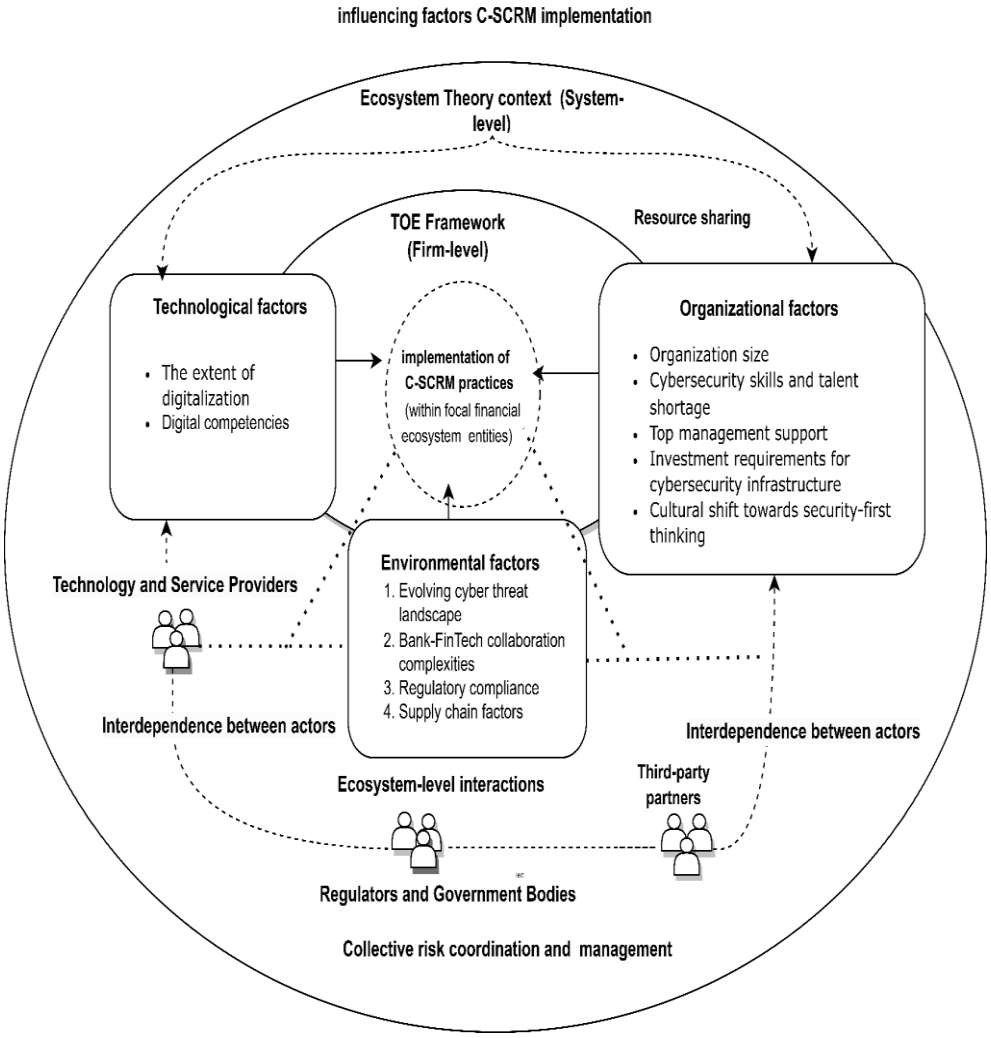
Environmental Factors: two main factors were identified: regulatory requirements and stakeholder collaboration. The CBE plays a proactive regulatory role that often issues alerts to financial banking institutions and develop precautionary actions after cybersecurity incidents. The CBE's regulatory factors usually drive specific organizational structures and compliance measures within the financial ecosystem. Additionally, the study sheds light on

increasing collaboration between banks and fintech companies creates complexity in security management, particularly when proper enterprise application integration is lacking

Towards an Integrative Framework Development: this study proposes an integrative framework that combines the TOE framework with ecosystem theory. In this framework, technological, organizational, and environmental determinants are interconnected through collaborative network effects that extend beyond the boundaries of individual focal entities. As illustrated in Figure 4, the framework not only captures the factors influencing C-SCRM implementation at the firm level but also explains how these practices collectively contribute to improving cyber supply chain performance across the broader ecosystem. By integrating firm-level and ecosystem-level perspectives, this study explores the multi-actor nature of cybersecurity challenges and highlights the importance of coordination and interdependence among stakeholders.

Figure 3

An Integrative framework: TOE and Ecosystem influences on the implementation of C-SCRM practices



Source: authors own work

7. Conclusion

This qualitative study is the first phase of two-phase research design that explores the conceptualizations of C-SCRM practices in the Egyptian financial sector. Through in-depth interviews, the study proposed new ways of understanding how these practices are implemented in the Egyptian context. C-SCRM is conceptualized as a dynamic and iterative process, by which focal entities could either individually or collectively identify, assess, and mitigate cyber risks within the financial ecosystem. These risks not only threaten internal operations but may also compromise the broader network of interconnected partners and systems. Therefore, C-SCRM can be viewed as an evolving journey requiring continuous adaptation and influenced by different factors rather than one time intervention.

This study makes several significant theoretical contributions to C-SCRM literature. The study provides a novel theoretical framework that integrates the Technology-Organization-Environment (TOE) framework and ecosystem theory to capture different factors influencing C-SCRM across financial ecosystems. The study provides conceptual clarity of C-SCRM which may support future theoretical development. It also confirms the multi-dimensional nature of C-SCRM, including governance, system integration, and operations within the Egyptian context. Finally, it emphasizes the dynamic nature of C-SCRM, promoting adaptive capability theories in response to evolving cyber risks.

This study provides actionable insights for key stakeholders in the financial ecosystem. It highlights the necessity for financial institutions to develop talent management strategies including recruitment, training, and retention programs for new cybersecurity roles like SOC analyst, and system architect. The findings also have significant implications for regulators and policymakers, emphasizing the need to integrate digital transformation and cybersecurity in supply chain rather than treating them separate policies. It suggests the importance of having specific policies tailored for financial institutions. This includes investing in partnerships with educational institutions and professional development organizations which may help address skill shortages.

8. Limitations and future research avenues

This research employed a qualitative methodology to address the research questions, which presents certain inherent limitations that should be acknowledged. The primary limitation of qualitative research relates to the generalizability of the findings. While the qualitative approach provided rich insights into C-SCRM practices within Egypt's financial sector, these findings cannot be broadly generalized for two key reasons. First, this exploratory study focused on understanding and developing theoretical frameworks rather than validating and refining them through hypothesis testing. Additional confirmatory research would be necessary to test and verify relationships. Second, the

relatively small number of interviewees drawn exclusively and non-probability from the financial sector limits the broader applicability of the findings across different industries and contexts. Future research could employ mixed methods to test the model across different industries.

There are several promising avenues for future investigation. First, employing mixed methods would enable both statistical validation of the theoretical frameworks and deeper qualitative insights into implementation. This methodological approach would strengthen the findings through triangulation of multiple data sources and analytical techniques. Second, future scholars could enhance understanding of how C-SCRM practices vary across different industries and contexts. For instance, a cross-sector comparative analysis would reveal both common challenges and industry-specific considerations in managing cyber supply chain risks. This broader perspective would contribute valuable insights into developing more robust and adaptable risk management frameworks. Additionally, longitudinal studies could examine how C-SCRM practices evolve over time in response to emerging technologies and changing threat landscapes. This temporal dimension would provide important insights into the dynamic nature of cyber supply chain risks and the effectiveness of various mitigation strategies across different organizational contexts.

References

Aarland, M. (2024). Cybersecurity in digital supply chains in the procurement process: introducing the digital supply chain management framework. *Information & Computer Security*. https://doi.org/10.1108/ICS-10-2023-0198

Adam, H. (2021). Fintech and Entrepreneurship Boosting in Developing Countries: A Comparative Study of India and Egypt. In *Studies in Computational Intelligence* (Vol. 974, pp. 141–156). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-73057-4_12

Adner, R. (2017). Ecosystem as Structure: An Actionable Construct for Strategy. *Journal of Management*, *43*(1), 39–58. https://doi.org/10.1177/0149206316678451

Arroyabe, M. F., Arranz, C. F. A., de Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges. *Technological Forecasting and Social Change*, *199*. https://doi.org/10.1016/j.techfore.2023.123051

Arroyabe, M. F., Arranz, C. F. A., Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, *78*. https://doi.org/10.1016/j.techsoc.2024.102670

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342–353. https://doi.org/10.1016/j.technovation.2014.02.001

Cheung, K. F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*. https://doi.org/10.1016/j.tre.2020.102217

Clarke, V., & Braun, V. (2013). *Successful Qualitative Research: A Practical Guide for Beginners*. https://www.researchgate.net/publication/256089360

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

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management*, *27*(1), 30–53. https://doi.org/10.1108/SCM-02-2020-0073

Creswell, J. W. (2015). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research* (Fifth).

Depietro, R. , W. E. , & Fleischer, M. (1990). The Context for Change: Organization, Technology and Environment. . In *The processes of technological innovation* (pp. 151–175).

EG-FinCIRT. (2023). *Cyber Threats Statistics for 2023*.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? In *Journal of Risk Finance* (Vol. 17, Issue 5, pp. 474–491). Emerald Group Publishing Ltd. https://doi.org/10.1108/JRF-09-2016-0122

Fernando, Y., Tseng, M. L., Wahyuni-Td, I. S., de Sousa Jabbour, A. B. L., Chiappetta Jabbour, C. J., & Foropon, C. (2023). Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia. *Journal of Industrial and Production Engineering*, *40*(2), 102–116. https://doi.org/10.1080/21681015.2022.2116495

Friday, D., Melnyk, S. A., Altman, M., Harrison, N., & Ryan, S. (2024). An inductive analysis of collaborative cybersecurity management capabilities, relational antecedents and supply chain cybersecurity parameters. *International Journal of Physical Distribution and Logistics Management*. https://doi.org/10.1108/IJPDLM-01-2023-0034

Gani, A. B. D., & Fernando, Y. (2021). The cybersecurity governance in changing the security psychology and security posture: insights into e-procurement. *Int. J. Procurement Management, 14*(3), 2021.

Gani, A. B. D., & Fernando, Y. (2024). Ten-year review of cyber supply chain security: driving productivity with visibility. *International Journal of Productivity and Quality Management, 42*(2), 153–169.

Gani, A. B. D., Fernando, Y., Lan, S., Lim, M. K., & Tseng, M. L. (2023). Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management and Data Systems*. https://doi.org/https://doi.org/10.1108/IMDS-05-2022-0313

Gaudenzi, B., & Baldi, B. (2024). Cyber resilience in organisations and supply chains: from perceptions to actions. *International Journal of Logistics Management*, *35*(7), 99–122. https://doi.org/10.1108/IJLM-09-2023-0372

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. In *Supply Chain Management* (Vol. 25, Issue 2, pp. 223–240). Emerald Group Holdings Ltd. https://doi.org/10.1108/SCM-10-2018-0357

Guerra, J. H. L., Souza, F. B. de, Pires, S. R. I., & Sá, A. L. R. de. (2024). A maturity model for supply chain risk management. *Supply Chain Management*, *29*(1), 114–136. https://doi.org/10.1108/SCM-11-2022-0435

Hampton, C., Sutton, S. G., Arnold, V., & Khazanchi, D. (2021). Cyber Supply Chain Risk Management: Toward an Understanding Cyber Supply Chain Risk Management: Toward an Understanding of the Antecedents to Demand for Assurance of the Antecedents to Demand for Assurance Cyber Supply Chain Risk Management: Toward an Understanding of the Antecedents to Demand for Assurance. *Journal of Information Systems*, *2*(35), 37-60. https://doi.org/10.2308/ISYS-19-050

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*. https://doi.org/10.1016/j.jisa.2020.102726

Herburger, M., Andreas, W., & Carina, H. (2024). Building supply chain resilience to cyber risks: a dynamic capabilities perspective. *Supply Chain Management*, *29*(7), 28–50. https://doi.org/10.1108/SCM-01-2023-0016

International Monetary Fund. (2024). *Rising cyber threats pose serious concerns for financial stability*.

ITU. (2024). *Global Cybersecurity Index*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx

Ivanov, D. (2021). Digital Supply Chain Management and Technology to Enhance Resilience by Building and Using End-to-End Visibility During the COVID-19 Pandemic. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2021.3095193

Jazairy, A., Brho, M., Manuj, I., & Goldsby, T. J. (2024). Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness. *International Journal of Physical Distribution and Logistics Management*, *54*(11), 1–29. https://doi.org/10.1108/IJPDLM-12-2023-0445

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, *60*(1), 162–183. https://doi.org/10.1080/00207543.2021.1984606

Orji, I. J., & U-Dominic, C. M. (2024). Modelling the conundrums to cyber-risks management in logistics firms for supply chain social sustainability. *Journal of Enterprise Information Management*. https://doi.org/10.1108/JEIM-12-2023-0635

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

Pérez-Morón, J. (2022). Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda.

Journal of Asia Business Studies, *16*(2), 371–395. https://doi.org/10.1108/JABS-11-2020-0444

Sadeghi R., K., Azadegan, A., & Ojha, D. (2024). Explainable artificial intelligence and agile decision-making in supply chain cyber resilience. *Decision Support Systems*, *180*. https://doi.org/10.1016/j.dss.2024.114194

Statista. (2023). *Number of cyber incidents in the financial industry worldwide from 2022 to 2023.*

Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy*, *79*, 103–114. https://doi.org/10.1016/j.tranpol.2019.04.019

Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability? *International Review of Financial Analysis*, *72*. https://doi.org/10.1016/j.irfa.2020.101587