STATISTICS IN TRANSITION new series, December 2025
Vol. 26, No. 4, pp. xxx–xxx, https://doi.org/10.59139/stattrans-2025-xxx
Received – xx.xx.xxxx; accepted – xx.xx.xxxx

The impact of Cyber Supply Chain Risk Management on Supply Chain 4.0

Abdellah Sassi[1], **Mohamed Ben Ali**[2], **Oumaima Oullada**[3], **Said Rifai**[4]

Abstract

Cyber Supply Chain Risk Management (CSCRM) is a novel risk management approach with Cyber Security (CS) being its crucial component. In the age of digitalization, CS has become a major concern worldwide. This study investigates the influence of CSCRM on Supply Chain 4.0 (SC 4.0) using a causal model to evaluate the connection between CS, CSCRM, and SC 4.0. The research investigates the link between CS and CSCRM, and between CSCRM and the levers of SC 4.0. The results highlight that CSCRM significantly influences various supply chain activities. The findings show that the integration of CSCRM, supported by CS is essential for improving the performance of SC 4.0. The "Statistical Package for the Social Sciences" was employed after administering a questionnaire to stakeholders in the Moroccan automotive and aeronautic industries.

Key words: Supply Chain 4.0, Cyber Supply Chain Risk Management, Cyber Security, Causal model.

1. Introduction

The shift toward Supply Chain 4.0 requires the integration of Industry 4.0 (I4.0) technologies such as the Internet of Things (IoT), Big Data Analytics (BDA), and Artificial Intelligence (AI), thereby enhancing digitalization while simultaneously

[1] National Higher School of Electricity and Mechanics – ENSEM – Hassan II University of Casablanca – B.P: 8118 Oasis – Casablanca – Morocco. Laboratory of Process, Mechanics, Materials, and Industrial Engineering – LP2MGI – Higher School of Technology of Casablanca – EST, Hassan II University of Casablanca – B.P 8112 Oasis – Casablanca, Morocco. E-mail: abdellah.sassi@ensem.ac.ma. ORCID: https://orcid.org/0009-0000-6798-2879.

[2] Laboratory of Process, Mechanics, Materials, and Industrial Engineering – LP2MGI – Higher School of Technology of Casablanca – EST, Hassan II University of Casablanca – B.P 8112 Oasis – Casablanca, Morocco. E-mail: benali8mohamed@gmail.com. ORCID: https://orcid.org/0000-0002-8615-7935.

[3] National Higher School of Electricity and Mechanics – ENSEM – Hassan II University of Casablanca – B.P: 8118 Oasis – Casablanca – Morocco. Laboratory of Process, Mechanics, Materials, and Industrial Engineering – LP2MGI – Higher School of Technology of Casablanca – EST, Hassan II University of Casablanca – B.P 8112 Oasis – Casablanca, Morocco. E-mail: oumaimaoullada@gmail.com. ORCID: https://orcid.org/0009-0004-6313-5532.

[4] Laboratory of Process, Mechanics, Materials, and Industrial Engineering – LP2MGI – Higher School of Technology of Casablanca – EST, Hassan II University of Casablanca – B.P 8112 Oasis – Casablanca, Morocco. E-mail: dptgmp@gmail.com. ORCID: https://orcid.org/0000-0002-2813-1606.

increasing exposure to cyber risks and global supply chain uncertainties (Foli *et al.*, 2022). As stated by Muller Raschid et al. (2022), principal vulnerabilities include cyber-attacks and lack of cybersecurity awareness among decision-makers (Muller, 2022). Another gap identified in our previous studies highlights the necessity of integrating Cyber Security (CS) and Cyber Supply Chain Risk Management to address privacy and security challenges (Sassi *et al.*, 2024). Notable cyber incidents for example the 2017 WannaCry attack, which used ransomware to hit several businesses (Creazza *et al.*, 2022). This study explores how effectively CSCRM influences the advancement of SC 4.0 within Morocco's automotive and aeronautic industries. The objectives of this research paper include: (1) exploring the motivation behind practitioners' adoption of CSCRM, (2) analyzing the relationship between Cyber Security and CSCRM, and (3) investigating the connection between CSCRM and Supply Chain 4.0. This is accomplished through the utilization of a conceptual framework to evaluate the importance of linkages between CS, CSCRM, and SC 4.0. The paper presents the study's context, research questions, methods, findings, and conclusions with suggestions for future research.

2. Background of the study

Effective Cyber-risk management in Supply Chains must be integrated from the outset of strategic planning, not addressed at the end (Pandey *et al.*, 2020). Recent studies have mainly explored cyber risks in limited firm samples (Colicchia *et al.*, 2019; Creazza *et al.*, 2022). Industry 4.0 is defined as a cost-effective, data-driven, and adaptable supply network that responds dynamically to fluctuations in both demand and supply (Ivanov *et al.*, 2021).

2.1. Cyber-attacks

Cyber-attacks are breaches of IT systems that can disturb operations or compromise systems over time (Boyson, Corsi and Paraskevas, 2022). They include malicious intentional and unintentional threats such as data leakage, phishing mails or hacking (Kessler *et al.*, 2022). According to the literature, cyber-attacks contain different categories, most of which are cited in the table below:

Table 1. Examples of Cyber-attacks

Reference	Attack Types	Description
(Larriva-Novo *et al.*, 2020)	Fuzzers	Fuzz testing is an automated method that tests software by inputting random or invalid data to detect vulnerabilities.
	Backdoors	In Cyber Security, a backdoor is a way to get beyond an organization's current security measures.

Table 1. Examples of Cyber-attacks (cont.)

Reference	Attack Types	Description
(Larriva-N	DoS	Denial of Service is a cyber-attack that prevents a device or a computer's intended users from using it
	Exploits	A malicious program that exploits holes in hardware or software security
	Shellcode	Attackers use it to target vulnerable processes on local, intranet, or remote systems
(Eggers, 2021)	IP or data theft	Insider disclosure without authorization may lead to further attacks or financial losses
	''Malicious substitution''	Substitution of the entire technological infrastructure, from hardware to firmware
	Tempering, manipulating	It refers to unauthorized changes or commands aimed at manipulating a device's operation or function
(Kern and Szanto, 2022)	Cyber SC attacks	Threats called Cyber SC Attacks aim to compromise the final target particularly through operational endpoint vulnerabilities, by using rusted channels within the supply chain
(Zhang *et al.*, 2019)	Port Scan	Port scanning is a common technique used by hackers to detect unsecured entry points in a network
	DoS Hulk	One of the widely used DoS attacks tools is Hulk. It produces distinct requests in an unstable pattern

2.2. Cyber Security (CS)

Cyber Security (CS) or IT security systems is the shield that protects data and knowledge flows, and prevents data leakage. According to Aamer and *et al.*, 7.35% of the articles cited Cyber Security as a crucial element of preparation for the transition to Supply Chain 4.0 (Aamer, Sahara and Al-Awlaqi, 2023). CS in the supply chain is essential for safeguarding its operations, as it is highly susceptible to threats such as cyberterrorism and malware-malicious software intended to damage computer systems or networks without the user's knowledge (Salem and Al-Saedi, 2023), including data theft. Therefore, Cyber Security measures must be in place to minimize risks, such as buying only from reliable suppliers and disconnecting critical systems from external connectivity (Politeknik Mukah Sarawak, Sarawak, Malaysia *et al.*, 2021).

2.3. Supply Chain 4.0 (SC 4.0)

SC 4.0 denotes the evolution of traditional supply chains through the adoption of I4.0 technologies, such as IoT, CS, AI and Radio Frequency Identification (RFID). This integration facilitates digitalization, interconnectivity, and adaptability, with the

objective of addressing operational challenges, enhancing competitiveness, and optimizing business performance (Sassi *et al.*, 2021). SC 4.0 is a network of coordinated operations that integrates forecasting, production, distribution, and sales to deliver value to customers and suppliers. By aligning these activities, it aims to enhance efficiency, boost innovation, and increase revenue (Martins, Simon and Campos, 2020).

2.4. Cyber Supply Chain Risk Management (CSCRM)

CSCRM is an integrative practice, its goal is to provide strategic oversight across the end-to-end business processes of both the focal organization and its extended enterprise partners, it synthesizes principles of CS, Supply Chain Management, and enterprise risk management (Colicchia, Creazza and Menachof, 2019). According to Muller and al., CSCRM is a process that identifies, evaluates and reduces any risks related to the IT/OT (Operational Technology) goods and services (Muller, 2022). Additionally, it is regarded as a novel and potent idea that integrates business risk management supply chain management, and CS components (Tatt*, Ganesan and Fernando, 2019). Supply chain attacks are cyber threats that can bypass advanced third-party defenses. Their frequency has risen significantly since 2020. Moreover, the integration of I4.0 technologies has further increased system vulnerability (Nygård and Katsikas, 2022). Hence, governments have increasingly focused on cyber supply chain risk management to protect their supply chains at all stages, from procurement and production to distribution, sales, and after-sales, aiming to minimize cybersecurity risks.

2.5. Recommendations from previous studies to strengthen CSCRM

Table 2 presents a synthesis of key recommendations extracted from previous studies aimed at enhancing CSCRM, highlighting technological, organizational, and environmental dimensions.

Table 2. Literature review recommendations for enhancing CSCRM

Recommendations	Authors
Enhance supply chain visibility through a (Technology–Organization–Environment) TOE-based approach to move from fragmented security practices toward a cohesive and productivity-driven CSCRM strategy.	(Gani and Fernando, 2024)
Use agency theory to align roles and responsibilities among supply chain partners, enhancing accountability and reducing cyber risk through governance, risk protocols, and incentives. Support this with capacity building and transparent communication to improve cybersecurity readiness and coordination.	(Firth and Srivastava, 2024)
Embed supplier cybersecurity into logistics and procurement by using a process-driven framework, assigning clear accountability, and treating cyber risk as a core supply chain concern.	(Handfield, Earp and Sadeghi, 2025)

2.6. Overview of the Moroccan automotive and aeronautical industries

2.6.1. Automotive industry

Over the past decade, the Moroccan automotive industry has experienced remarkable and sustained growth, becoming the country's leading export sector. It has created over 147,000 new jobs, attracted more than 250 companies, and established Morocco as the continent's foremost automotive manufacturing hub (Ministry of trade and commerce, 2023).

2.6.2. Aeronautic industry

Morocco is now one of the most competitive and alluring bases on the global map of aviation construction, confirming the Kingdom's great ambition in this high added value industry, after 20 years defined by a singular technological and human journey. Morocco is becoming a prime site and location, with 140 companies (Ministry of trade and commerce, 2023).

3. Research methodology

This research paper explores various research designs, data collection methods, survey instruments, variable measurements, and data analysis techniques. It examines potential relationships, significant or not, among the tested methodologies. As noted by Sassi et al., linear regression models how a dependent variable varies in relation to one or more independent variables, through the least squares method. It includes simple regression (involving a single independent variable) and multiple regression (involving several). A p-value below 0.05 indicates a statistically significant correlation, while regression coefficients reflects the strength of each variable's impact (Sassi et al., 2025).

3.1. Problem description

The reputation of automotive and aeronautic companies for safety is critical to both the companies and their stakeholders. Global supply chain has a very large information flows through all its levers. Its digitalization and transformation will force it to deal with multiple internal and external risks that converge, threatening its stability (Azouzi, Iqqi and Amri, 2023). Therefore, these companies are very proactive about securing their supply chain which leads us to the main problem in this research paper. How to secure the supply chain after the transformation to SC 4.0?

3.2. Questions guiding the study

- Is CSCRM positively associated with SC 4.0?
- Does CS have a very important influence on CSCRM?

3.3. Research objectives

This study aims to examine how directly CSCRM affects Supply Chain 4.0 by explaining variables.

This research aims to achieve the following key objectives:

- To examine the connection between CSCRM and SC 4.0.
- To examine the connection between CS and CSCRM.

3.4. Purpose of the study

SC 4.0 is the fusion of I4.0 technologies with traditional supply chains, resulting in digitalization and increased vulnerability to cyber threats. To manage these risks, CSCRM becomes essential for ensuring the safety and performance of Supply Chains 4.0. This research paper presents a pioneering empirical study on the impact of CSCRM on SC 4.0, offering both theoretical insights and practical contributions for industry and practitioners.

3.4.1. First research construct: CS

The Cyber Security (CS) involves measures such as the trust level of the authenticity and reliability of data, information security and management, and the handling of external data from stakeholders.

3.4.2. Second research construct: CSCRM

CSCRM is measurable by determining at which level the companies respect different governmental guidelines and apply different procedures associated with risk identification, management and evaluation.

3.4.3. Third research construct: SC 4.0

The SC 4.0 could be measured throughout all its levers (PS): ''Purchase and Supply'', (PR): ''Production'', (SD): ''Storage and Distribution'', (SaS): ''Sales and after Sales'' (Sassi *et al.*, 2024).

3.4.4. Presentation of the model research

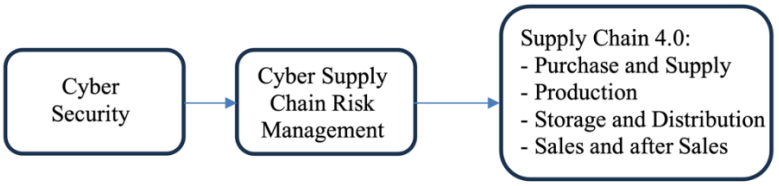

Figure 1. Theoretical Framework

Drawing on the research problem and the literature review, the proposed theoretical framework is organized into six criteria, divided across three categories: one for CS, one for CSCRM, and four for SC 4.0 (as shown in Figures 1 and 2). The model assumes causal relationships among all criteria, with five hypotheses developed to represent the five causal links in the conceptual framework.

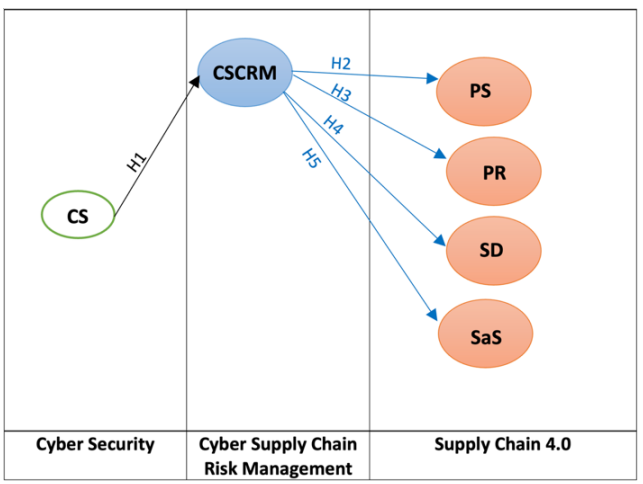

Figure 2. Detailed theoretical model

Table 3. Presenting the codes used within the proposed theoretical model (Sassi *et al.*, 2024)

Proposed Model Constructs	Codes	Titles
Cyber Security	CS	''Cyber Security''
Cyber Supply Chain Risk Management	CSCRM	''Cyber Supply Chain Risk Management''
Supply Chain 4.0	PS	''Purchase and Supply''
	PR	''Production''
	SD	''Storage and Distribution''
	SaS	''Sales and after Sales''

3.4.5. Formulation of the Hypothesis

This research seeks to confirm or refute the 5 hypotheses listed below.

Table 4. Formulated hypotheses

Hypothesis N°	Causal Connection	Formulated Hypothesis
H1	CS ⟶ CSCRM	We hypothesized that CS positively influences CSCRM
H2	CSCRM ⟶ PS	We hypothesized that CSCRM positively influences PS
H3	CSCRM ⟶ PR	We hypothesized that CSCRM positively influences PR
H4	CSCRM ⟶ SD	We hypothesized that CSCRM positively influences SD
H5	CSCRM ⟶ SaS	We hypothesized that CSCRM positively influences SaS

3.5. Preparation of the methodological framework of research:

3.5.1. Formulated hypothesis

For this study, primary data will be gathered using a structured survey, distributed either in paper format or through Google Forms, targeting industrial and supply chain managers as well as general managers in Morocco's automotive and aeronautics industries. The selection of automotive companies is based on information from the directory provided by the Moroccan Automotive Federation "The directory of the automotive sector in Morocco" (La fédération de l'automobile, 2023). For the aeronautic sector, data was sourced from the Group of Moroccan Aeronautical and Space industries. A total of 200 firms were identified across both sectors, including company names and key contact details of high-ranking representatives. The aim was to reach a diverse sample of active firms. The survey was distributed via LinkedIn in August 2023 to 190 companies (140 automotive and 50 aeronautic), and data collection was completed in November 2023. Out of 50 surveys sent to aeronautic companies in the data set, there are 33 responses, which means that the response rate of 66% is deemed representative. Out of 140 surveys distributed to automotive companies, there are 75 responses, which means that the response rate is 53.57% which is considered moderated. Notice that the total number of interviewers who answered the survey is 94 but since some companies are considered active in both sectors, the total number of responses amounts to 108, thus, the total rate of response is 56.84%. According to the classification criteria by the Moroccan High Commission for planning, the firms selected for this study represent various organizational strata (1.1% small firms, 22.5 % medium-sized firms, and the remaining 76.4% big firms). The demographics of the companies featured in the study are summarized in Table 5 (Moroccan High Commission for Planning, 2019).

Table 5. Demographics of participating firms

Characteristics	Categories	Frequency	Percentage
Year of foundations	<11 y	38	40.4%
	11 – 20 y	24	25.8%
	>20 y	32	33.7%
Region	Casablanca and region	32	33.7%
	Tanger and region	38	40.4%
	Marrakech and region	01	0.01%
	Kenitra and region	23	25.8%
Company's work force	<10	01	1.1%
	<200	21	22.5%
	>200	72	76.4%
Capital	<50 000 dhs	01	1.3%
	50 001 – 400 000 dhs	02	2.6%
	400 001 – 600 000 dhs	04	5.1%
	600 001 – 1 000 000 dhs	03	3.8%
	>1 000 000 dhs	83	87.2%

3.6. Questionnaire design

3.6.1. Questionnaire steps

This study's questionnaire consists of two primary sections, with the first focusing on respondent and company information, and the second on evaluating the study's conceptual model constructs, CS, CSCRM and SC 4.0, using 44 items (7 for CS, 8 for CSCRM, and 30 for SC 4.0). A six-point Likert scale, from 0 = Abs/No to 6 = Very High, was used for assessment (Likert, 1932). The measurement instrument was developed following Churchill's (1979) paradigm (Churchill, 1979), which involves defining the construct through an extensive literature review, generating diverse measurement items, collecting data, and refining the instrument using statistical tools like coefficient alpha and factor analysis. Reliability and validity were further tested using methods such as split-half reliability and the multirait-multimethod matrix. Norms were then established to enable meaningful interpretation and comparisons.

3.6.2. Reliability test

The reliability of the questionnaire instrument was assessed using Cronbach's Alpha. As shown in Table 6, all constructs and measurement items used in the study demonstrate acceptable reliability, with values exceeding the threshold of 0.7 (Fornell and Bookstein, 1982; Kline, 1999).

Table 6. Evaluation summary of the three constructs' reliability and validity

Constructs	Variables	Code	Number of items	Cronbach's Alpha α
Cyber Security	Cyber Security	CS	7	0.949
Cyber Supply Chain Risk Management	Cyber Supply Chain Risk Management	CSCRM	8	0.968
Supply Chain 4.0	Purchase and Supply	PS	7	0.957
	Production	PR	8	0.985
	Storage and Distribution	SD	7	0.965
	Sales and after Sales	SaS	8	0.976

4. Results of the study

In this section, we detail the findings obtained from the empirical analysis.

4.1. Examining the connection between CS and CSCRM

4.1.1. Global Model: Cyber Security (CS) – Cyber Supply Chain Management (CSCRM)

Overall, Table 7 indicates a strong correlation between CS and CSCRM (R = 0.616). The dependent variable, CSCRM, accounts for 38.0 % of the variance in the predicted variable CS, as shown by the R-squared value of 0.380. Additionally, the model is statistically significant, with a p-value of 0.00 (Table 9), which is well below the 5% threshold, confirming the model's overall validity.

Table 7. Summary of model characteristics (CS-CSCRM)

Model	R	R-squared	Adjusted R-squared	Standard error of estimation
CS-CSCRM	0.616	0.380	0.373	0.79193260

a. Predicted (Independent) value: CS.
b. Dependent variable: CSCRM.
c. Linear regression at the origin.

Table 8. Variance Analysis (CS-CSCRM)

Model	Sum of squares	ddl	Average Square	D	Sig
Regression	35.302	1	35.302	56.288	0.000
Residual	57.698	92	0.627		
Total	93.000	93			

a. Dependent variable: CSCRM.
b. Linear regression at the origin.
c. Predicted value: CS.

4.1.2. Linear model equation: Cyber Security (CS) – Cyber Supply Chain Risk Management (CSCRM)

Based on Table 9, the linear regression equation is expressed as follows:

$$CSCRM = 0.616\ CS \quad (1)$$

The causal relationship between CS and CSCRM is statistically significant (P-value = 0 < 5%), indicating that CS has a strong impact on CSCRM. Additionally the t-student exceeds |2.775| (|1.960|), confirming that the parameter estimates are significant at the 1% (or 5%) significance level (Oullada *et al.*, 2023).

Table 9. Criteria coefficients (CS-CSCRM)

Model	Unstandardized coefficients		Standardized coefficients	t-student	Sig. (P-value)
	A	Standard error	Beta		
CS-CSCRM	0.616	0.082	0.616	7.503	0.000

4.2. Examining the connection between CSCRM and PS

4.2.1. Overall model: Cyber Supply Chain Risk Management (CSCRM) – Purchase and Supply (PS)

According to Table 10, we notice that the causal relationship between CSCRM and PS is positively significant (R = 0.723). The explanatory variable, PS, accounts for 52.3% of the variance in the dependent variable CSCRM, as indicated by an R-squared value of 0.523. Furthermore, the model is globally valid since its significance value is lower than 5%.

Table 10. The overall model (CSCRM-PS)

Model	R	R-squared	Adjusted R-squared	Standard error of estimation
CSCRM-PS	0.723	0.523	0.518	0.69408436

a. Predicted value: CSCRM.
b. Dependent variable: PS.
c. Linear regression at the origin.

Table 11. Variance analysis (CSCRM-PS)

Model	Sum of squares	ddl	Average Square	D	Sig
Regression	48.679	1	48.679	101.045	0.000
Residual	44.321	92	0.482		
Total	93.000	93			

a. Dependent variable: PS.
b. Linear regression at the origin.
c. Predicted value: CSCRM.

4.2.2. Linear model equation: Cyber Supply Chain Risk Management (CSCRM) – Purchase and Supply (PS)

According to Table 12, the linear regression equation is formulated as follows:

$$PS = 0.723\ CSCRM \quad (2)$$

Note that the causal relationship between CSCRM and PS is highly significant (p-value = 0 < 5%), which means that CSCRM has a strong impact on PS.

Table 12. Criteria coefficients (CSCRM-PS)

Model	Unstandardized coefficients		Standardized coefficients	t-student	Sig. (P-value)
	A	Standard error	Beta		
CSCRM-PS	0.723	0.072	0.723	10.052	0.000

4.3. Examining the connection between CSCRM and PR

4.3.1. Overall model: Cyber Supply Chain Risk Management (CSCRM) – Production (PR)

There is a moderately strong connection between CSCRM and PR (R = 0.504). The dependent variable PR, accounts for 25.40 % of the variance in the predicted variable CSCRM (R-squared = 0.254). The model is considered globally reliable since the significance value (p-value) is below 5% (Table 15).

Table 13. The overall model (CSCRM-PR)

Model	R	R-squared	Adjusted R-squared	Standard error of estimation
CSCRM-PR	0.504	0.254	0.246	0.86812659

a. Predicted value: CSCRM

b. Dependent variable: PR

c. Linear regression at the origin

Table 14. Variance analysis (CSCRM-PR)

Model	Sum of squares	ddl	Average Square	D	Sig
Regression	23.665	1	23.665	31.400	0.000
Residual	69.335	92	0.754		
Total	93.000	93			

a. Dependent variable: PR.

b. Linear regression at the origin.

c. Predicted value: CSCRM.

4.3.2. Linear model equation: Cyber Supply Chain Risk Management (CSCRM) – Production (PR)

The linear regression equation is written as follows on the basis of Table 15:

$$PR = 0.504\ CSCRM \tag{3}$$

We notice that (p-value = 0 < 5%), thus, the causal relationship CSCRM-PR is considered significant, and we conclude that the CSCRM strongly impacts PR.

Table 15. Criteria Coefficients (CSCRM-PR)

Model	Unstandardized coefficients		Standardized coefficients	t-student	Sig. (P-value)
	A	Standard error	Beta		
CSCRM-PR	0.504	0.090	0.504	5.604	0.000

4.4. Examining the connection between CSCRM and SD

4.4.1. Overall model: Cyber Supply Chain Risk Management (CSCRM) – Storage and Distribution (SD)

There is a strong connection between CSCRM and SD, with a correlation of R=0.454. The dependent variable SD, explains 20.6% of the variance in the independent variable CSCRM, as indicated by an R-squared value of 0.206. Additionally, the model's significance value is below the 5% threshold, confirming its overall statistical validity.

Table 16. The overall model (CSCRM-SD)

Model	R	R-squared	Adjusted R-squared	Standard error of estimation
CSCRM-SD	0.454	0.206	0.197	0.89595774

a. Predicted value: CSCRM.
b. Dependent variable: SD.
c. Linear regression at the origin.

Table 17. Variance Analysis (CSCRM-SD)

Model	Sum of squares	ddl	Average Square	D	Sig
Regression	19.148	1	19.148	23.853	0.000
Residual	73.852	92	0.803		
Total	93.000	93			

a. Dependent variable: SD.
b. Linear regression at the origin.
c. Predicted value: CSCRM.

4.4.2. Linear model equation: Cyber Supply Chain Risk Management (CSCRM) – Storage and Distribution (SD)

Based on the results presented in Table 18, the linear regression equation is expressed as follows:

$$SD = 0.454\ CSCRM \quad (4)$$

The causal relationship CSCRM-SD is considered significant since the (sig. =0<5%), thus, the CSCRM strongly impacts SD.

Table 18. Criteria coefficients (CSCRM-SD)

Model	Unstandardized coefficients		Standardized coefficients	t-student	Sig. (P-value)
	A	Standard error	Beta		
CSCRM-SD	0.454	0.93	0.454	4.884	0.000

4.5. Examining the connection between CSCRM and SaS

4.5.1. Overall model: Cyber Supply Chain Risk Management (CSCRM) – Sales and after Sales (SaS)

In general, a moderate strong positive correlation exists between CSCRM and SaS criterion (R = 0.514). The model's significance level (p-value = 0.00, Table 20) is below the 5% threshold, confirming the model's reliability.

Table 19. The overall model (CSCRM-SaS)

Model	R	R-squared	Adjusted R-squared	Standard error of estimation
CSCRM-SaS	0.514	0.264	0.256	0.86246393

a. Predicted value: CSCRM.
b. Dependent variable: SaS.
c. Linear regression at the origin.

Table 20. Variance analysis (CSCRM-SaS)

Model	Sum of squares	ddl	Average Square	D	Sig
Regression	24.566	1	24.566	33.026	0.000
Residual	68.434	92	0.744		
Total	93.000	93			

a. Dependent variable: SaS.
b. Linear regression at the origin.
c. Predicted value: CSCRM.

4.5.2. Linear model equation: Cyber Supply Chain Risk Management (CSCRM) – Sales and after Sales (SaS)

The linear regression model derived from Table 21 is formulated as follows:

$$SaS = 0.514\ CSCRM \tag{5}$$

The causal relationship between CSCRM and SaS is statistically significant (p-value = 0 < 0.05), suggesting that CSCRM exerts a notable influence on SaS.

Table 21. Criteria coefficients (CSCRM-SaS)

Model	Unstandardized coefficients		Standardized coefficients	t-student	Sig. (P-value)
	A	Standard error	Beta		
CSCRM-SaS	0.514	0.089	0.514	5.747	0.000

4.6. Overall model summarizing hypothesis testing outcomes

The outcomes of the hypothesis test (Table 22) and the global model (Figure 3) are detailed below:

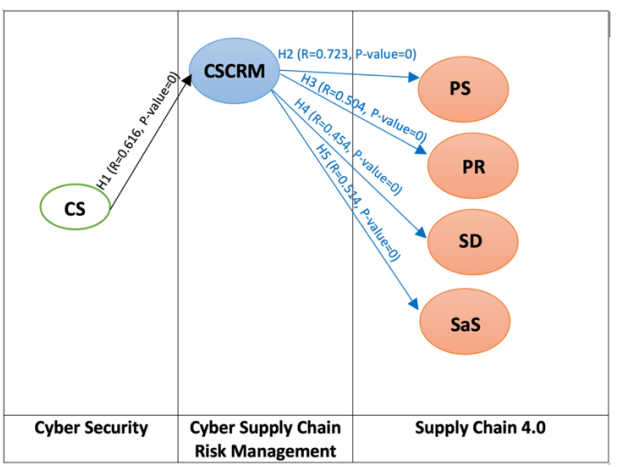

Figure 3. Overall model summarizing hypothesis test results.

Table 22. Hypothesis testing outcomes

Hypotheses	Results
H1: CS ➡ CSCRM	Valid
H2: CSCRM ➡ PS	Valid
H3: CSCRM ➡ PR	Valid
H4: CSCRM ➡ SD	Valid
H5: CSCRM ➡ SaS	Valid

5. Discussion and Conclusion

This section presents the findings of the empirical investigation, revealing growing public concern over CSCRM due to rising cyberattacks and scams. In Morocco, this concern is increasingly evident, especially in the key automotive and aeronautic industries. Serhane et al. (2023) emphasized that greater connectivity heightens industrial systems' vulnerability to cyber threats, including attacks and unauthorized access (Serhane, Hamzaoui and Ibrahimi, 2023). Industrial systems were long vulnerable to cyberattacks due to limited security in their design and their isolation from the internet. With Industry 4.0, this isolation has diminished, exposing them to a wider spectrum of cyber threats (Tamy *et al.*, 2020). Digitalizing supply chains is challenging as it demands specialized digital skills, unique organizational competencies, and a clear digital strategy (Kohnke, 2017). Hence, companies operating within Industry 4.0 need to cultivate dynamic capabilities to effectively navigate Supply Chain risks. Using the DEMATEL approach, Pandey et al. identified behavioral risk as the most critical among the various risk categories. Future research should focus on risks linked to specific I4.0 technologies within Supply Chains (Pandey, Singh and Gunasekaran, 2021). This study clarifies how CSCRM directly affects Supply Chain 4.0, linking key variables. CSCRM, supported by Cyber Security, addresses cyberattack emerging from the shift to digital supply chains.

Based on the applied research methodology, this study also finds that, Cyber Security can also affect positively CSCRM to help it influence positively the SC 4.0.

Our exploratory study's findings indicate that:

- The relationship between CS and CSCRM is both significant and positively correlated.
- The relationship between the CSCRM and Purchase and Supply (PS) is significant and positive.
- The relationship between the criterion CSCRM and Production (PR) criterion is fairly high.
- CSCRM has a positive and quite high influence on Storage and Distribution criterion.
- The relationship between CSCRM and Sales and after Sales (SaS) is fairly strong and positive.

The study shows Cyber Security positively influences CSCRM, whose success depends on strong CS. Implementing CSCRM enhances Supply Chain 4.0 by positively impacting its key levers. Therefore, supply chain managers must understand and adopt CSCRM, aligning with Tamy and al. (2020)'s strategic approach to safeguarding Industry 4.0 networks (Tamy *et al.*, 2020). These results are also in line with the outcomes of Aarland et al. (2025), who emphasized the prominence of establishing clear cybersecurity requirements and ensuring proper management within digital supply chains (Aarland, 2025). This study shows that CSCRM enhances SC 4.0 performance in Morocco's automotive and aeronautical sectors. The integration of CS, CSCRM, and SC 4.0 into one framework highlights the essential role of CS in effective CSCRM and offers practical strategies for managing digital risks in emerging industries.

6. Limitations

Although the findings are promising, the study has limitations, notably an average response rate. Larger samples should be used in future research to ensure more representative and reliable results. Moreover, the research was limited in scope to samples from only two sectors: the automotive and aeronautic industries. It is recommended that this model be applied to other fields, such as textiles, agriculture, and others. Furthermore, given that this study concentrates on one specific enabling technology, subsequent research could examine a broader spectrum of technologies to validate and refine the proposed framework.

References

Aamer, A., Sahara, C.R. and Al-Awlaqi, M. A., (2023) Digitalization of the supply chain: transformation factors. *Journal of Science and Technology Policy Management*, 14(4), pp. 713–733. Available at: https://doi.org/10.1108/JSTPM-01-2021-0001.

Aarland, M., (2025) Cybersecurity in digital supply chains in the procurement process: introducing the digital supply chain management framework, *Information & Computer Security*, 33(1), pp. 5–24. Available at: https://doi.org/10.1108/ICS-10-2023-0198.

Azouzi, M., Iqqi, I. and Amri, M., (2023) Safety and security as risk management factors in supply chains. *Journal of Operations Management*, 3(1), pp. 1-10.

Boyson, S., Corsi, T. M. and Paraskevas, J.-P., (2022) Defending digital supply chains: Evidence from a decade-long research program. *Technovation*, 118, p. 102380. Available at: https://doi.org/10.1016/j.technovation.2021.102380.

Churchill, G. A., (1979) A Paradigm for Developing Better Measures of Marketing Constructs. *Journal of Marketing Research*, 16(1), pp. 64–73. Available at: https://doi.org/10.1177/002224377901600110.

Colicchia, C., Creazza, A. and 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), pp. 215–240. Available at: https://doi.org/10.1108/SCM-09-2017-0289.

Creazza, A. *et al.,* (2022) Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, 27(1), pp. 30–53. Available at: https://doi.org/10.1108/SCM-02-2020-0073.

Eggers, S., (2021) A novel approach for analyzing the nuclear supply chain cyber-attack surface. *Nuclear Engineering and Technology*, 53(3), pp. 879–887. Available at: https://doi.org/10.1016/j.net.2020.08.021.

Firth, R., Srivastava, M., (2024) Identifying Critical Success Factors (CSF) for Cyber Supply Chain Risk Management (CSCRM): A Qualitative Study Using Agency Theory, in K.S. Soliman (ed.) *Artificial intelligence and Machine Learning*. Cham: *Springer Nature Switzerland* (Communications in Computer and Information Science), pp. 173–186. Available at: https://doi.org/10.1007/978-3-031-62843-6_19.

Foli, S. *et al.*, (2022) Supply Chain Risk Management in Young and Mature SMEs. *Journal of Risk and Financial Management*, 15(8), p. 328. Available at: https://doi.org/10.3390/jrfm15080328.

Fornell, C., Bookstein, F. L., (1982) Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory. *Journal of Marketing Research*, 19(4), p. 440. Available at: https://doi.org/10.2307/3151718.

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), pp. 153–169. Available at: https://doi.org/10.1504/IJPQM.2024.139156.

Handfield, R., Earp, J. and Sadeghi, A. H., (2025) Reducing cybersecurity vulnerabilities in the supply base: Insights from cyber experts, *Technology in Society*, 82, p. 102947. Available at: https://doi.org/10.1016/j.techsoc.2025.102947.

Ivanov, D. *et al.*, (2021) Researchers' perspectives on Industry 4.0: multi-disciplinary analysis and opportunities for operations management. *International Journal of Production Research*, 59(7), pp. 2055–2078. Available at: https://doi.org/10.1080/00207543.2020.1798035.

Kern, E. Szanto, A., (2022) Cyber Supply Chain Attacks, in Tim H. Stuchtey (eds). *BIGS Policy Paper Brandenburg Institute for Society and Security*, p. 10.

Kessler, M. *et al.*, (2022) Curse or Blessing? Exploring risk factors of digital technologies in industrial operations. *International Journal of Production Economics*, 243, p. 108323. Available at: https://doi.org/10.1016/j.ijpe.2021.108323.

Kline, R. B., (1999) Book Review: Psychometric theory (3rd ed.). *Journal of Psychoeducational Assessment*, 17(3), pp. 275–280. Available at: https://doi.org/10.1177/073428299901700307.

Kohnke, O., (2017) It's Not Just About Technology: The People Side of Digitization, in G. Oswald and M. Kleinemeier (eds). *Shaping the Digital Enterprise*. Cham: Springer International Publishing, pp. 69–91. Available at: https://doi.org/10.1007/978-3-319-40967-2_3.

La fédération de l'automobile, (2023) Annuaire du secteur automobile au Maroc. Available at: https://cgem.ma/structures/federations-statutaires/federation-de-lautomobile-fa/ (Accessed: 15 August 2023).

Larriva-Novo, X. A. *et al.*, (2020) Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies. *IEEE Access*, 8, pp. 9005–9014. Available at: https://doi.org/10.1109/ACCESS.2019.2963407.

Likert, R., (1932) *A technique for the measurement of attitudes*. Academic Dissertation. Columbia University.

Martins, F. D. C., Simon, A. T. and Campos, R. S. D., (2020) Supply Chain 4.0 challenges. *Gestão & Produção*, 27(3), p. e5427. Available at: https://doi.org/10.1590/0104-530x5427-20.

Ministry of Industry and Trade, (2023) Aeronautic. [Online] Available at: https://www.mcinet.gov.ma/fr/content/aeronautique. Consulted: May 2023.

Ministry of Industry and Trade, (2023) Automobile. [Online] Available at: https://www.mcinet.gov.ma/fr/content/aeronautique. Consulted: May 2023.

Moroccan High Commission for Planning, (2019) Classification criteria of Moroccan companies. *19 Novembre 2019*, 19 November, p. 28.

Muller, S. R., (2022) Analyzing Deficits in Awareness Among Chief Supply Chain Officers Who Have Not Adopted Cybersecurity as a Threat to Supply Chains, in *2022 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*. *2022 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*, Soyapango. El Salvador: *IEEE*, pp. 1–6. Available at: https://doi.org/10.1109/ICMLANT56191.2022.9996456.

Nygård, A. R., Katsikas, S., (2022) SoK: Combating threats in the digital supply chain, in *Proceedings of the 17th International Conference on Availability, Reliability and Security*. *ARES 2022: The 17th International Conference on Availability, Reliability and Security*, Vienna Austria: *ACM*, pp. 1–8. Available at: https://doi.org/10.1145/3538969.3544421.

Oullada, O. *et al.* ,(2023) Model for measuring the impact of good pharmacovigilance practices of COVID-19 patients on hcp reactivity: Morocco case study. *Statistics in Transition new series*, 24(5), pp. 63–88. Available at: https://doi.org/10.59170/stattrans-2023-064.

Pandey, S. *et al.*, (2020) Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, 13(1), pp. 103–128. Available at: https://doi.org/10.1108/JGOSS-05-2019-0042.

Pandey, S., Singh, R. K. and Gunasekaran, A., (2021) Supply chain risks in Industry 4.0 environment: review and analysis framework. *Production Planning & Control*, pp. 1–28. Available at: https://doi.org/10.1080/09537287.2021.2005173.

Politeknik Mukah Sarawak, Sarawak, Malaysia *et al.*, (2021) Cyber security in supply chain management: A systematic review. *Logforum*, 17(1), pp. 49–57. Available at: https://doi.org/10.17270/J.LOG.2021555.

Salem, I. E., Al-Saedi, K. H., (2023) Intensive Malware Detection Approach based on Data Mining. *Journal of Applied Engineering and Technological Science (JAETS)*, 5(1), pp. 414–424. Available at: https://doi.org/10.37385/jaets.v5i1.2865.

Sassi, A. *et al.*, (2021) The relation between Industry 4.0 and Supply Chain 4.0 and the impact of their implementation on companies. *International Journal of Innovation and Applied Studies*. performance: State of the Art', 31(4), p. 820-828.

Sassi, A. *et al.*, (2024) Model for Assessing the Impact of Internet of Things on Supply Chain 4.0: Moroccan Case, in Y. Mejdoub and A. Elamri (eds) *Proceeding of the International Conference on Connected Objects and Artificial Intelligence (COCIA2024)*. Cham: Springer Nature Switzerland (Lecture Notes in Networks and Systems), pp. 252–258. Available at: https://doi.org/10.1007/978-3-031-70411-6_39.

Sassi, A. *et al.*, (2025) A causal model to assess the influence of supply chain 4.0 on Moroccan companies' performance. *International Journal of Advances in Applied Sciences*, 14(1), p. 111. Available at: https://doi.org/10.11591/ijaas.v14.i1.pp111-122.

Serhane, A., Hamzaoui, E.-M. and Ibrahimi, K., (2023) IA Applied to IIoT Intrusion Detection: An Overview, in *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM). 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Istanbul. Turkiye: *IEEE*, pp. 1–6. Available at: https://doi.org/10.1109/WINCOM59760.2023.10323032.

Tamy, S. *et al.*, (2020) Cyber security based machine learning algorithms applied to industry 4.0 application case: Development of network intrusion detection system using hybrid method. *Journal of Theoretical and Applied Information Technology*, 98(12), pp. 2078–2091.

Tatt*, D. Y. B., Ganesan, Y. and Fernando, Y., (2019) 'The Effects of Cyber Supply Chain Risk Management in Financial Industry'. *ICBSI 2018 - International Conference on Business Sustainability and Innovation*, pp. 512–521. Available at: https://doi.org/10.15405/epsbs.2019.08.51.

Zhang, Y. *et al.*, (2019) 'PCCN: Parallel Cross Convolutional Neural Network for Abnormal Network Traffic Flows Detection in Multi-Class Imbalanced Network Traffic Flows'. *IEEE Access*, 7, pp. 119904–119916. Available at: https://doi.org/10.1109/ACCESS.2019.2933165.