European Journal of Economic and Financial Research
ISSN: 2501-9430
ISSN-L: 2501-9430
Available on-line at: http://www.oapub.org/soc

DOI: 10.46827/ejefr.v8i4.1790 Volume 8 | Issue 4 | 2024

CYBERSECURITY AND THE AUTOMOTIVE SUPPLY CHAIN IN MOROCCO: EXPLORATORY STUDY

Raissouni Kenza[1i],
Errabih Zakia[2],
Raissouni Rajaa[3],
Raissouni Mohammed Rabih[4],
Charroud Soukaina[1],
Bourkkadi Salmane[5]

[1]PhD Student,
Laboratory: Technologies and Industrial Services,
Sidi Mohamed Ben Abdelah University (EST),
Fez, Morocco
[2]Lecturer,
Laboratory: Technologies and Industrial Services,
Sidi Mohamed Ben Abdelah University (EST),
Fez, Morocco
[3]PhD,
Centre for Doctoral Studies in Economics and Management and Sustainable Development,
Abdelmalek Essaadi University,
Tetouan, Morocco
[4]PhD,
Team Science Teaching and Issues of Multilingualism and Diversification of Learning Modalities in the Digital Era,
Regional Center for Education and Training,
Tangier, Morocco
[5]Lecturer, Poitiers University,
France – Ibn Tofail University,
Morocco

Abstract:
Technological evolution exposes the Moroccan automotive supply chain to cyberattack risks, which could potentially lead to interruptions detrimental to operational continuity. In order to better understand the security measures currently in place to address these potential threats, an exploratory study was conducted within companies in the Moroccan automotive sector. This research was conducted through structured interviews, guided by specific questionnaires, with four carefully selected companies. The sample included two small and medium-sized enterprises (SMEs) as well as two large companies in the

[i] Correspondence: email raissounikenza@gmail.com

automotive sector in Morocco. The results obtained from these interviews reveal significant differences in the level of awareness and security approach towards cyberattack risks among the different companies interviewed.

JEL: L91, L62, O33, D80, M15, R41

Keywords: cyberattacks, cyber risk management, automotive supply chain, automotive sector in Morocco, cybersecurity related to the supply chain

1. Introduction

The global automotive supply chain, a complex network spanning multiple continents, is a crucial element for the smooth operation of the industry. From design to final distribution to consumers, this chain involves various actors, such as automotive manufacturers, as well as three categories of suppliers at different levels (Hugo et al, 2004; Benaini, 2020):

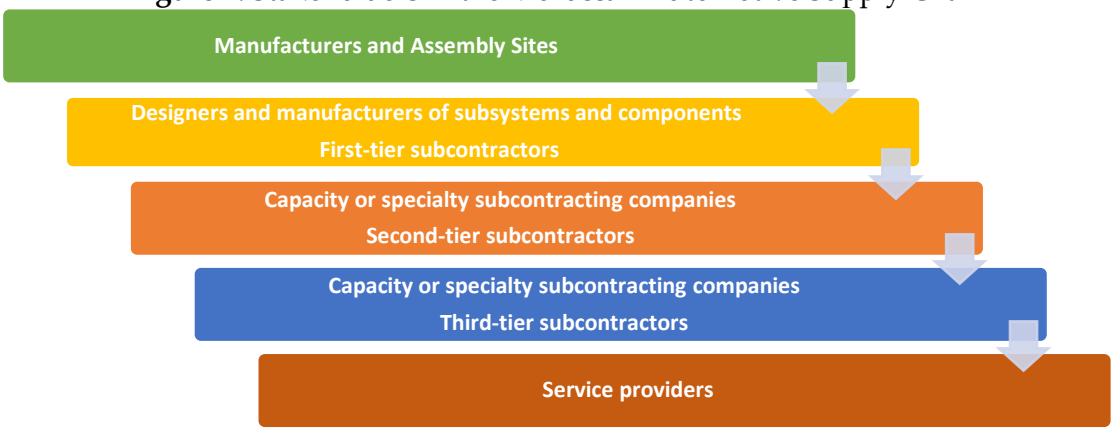
- Automotive manufacturers, who are the major brands and the order givers.
- Tier 1 suppliers, who are key partners of the manufacturers and focus on producing equipment or modules for vehicles. Their role is crucial to the industry's economy, and they make continuous efforts in terms of internationalization and innovation to meet the needs of manufacturers.
- Tier 2 suppliers, who act as subcontractors and provide subassemblies, parts, or equipment.
- Tier 3 suppliers, who are capacity subcontractors and provide components that are integrated into subassemblies, which are then assembled by Tier 2 suppliers.

Many studies emphasize the increasing importance of the globalization of supply chain links and assert that their integration is essential to ensure the success of these chains (Mustafa Kamal & Irani, 2014).

With the rise of global production, Morocco has positioned itself significantly in the global automotive industry's value chain. The country emphasizes both the production of components and other inputs, as well as automotive assembly, which has experienced remarkable growth, while also developing its capabilities in distribution and other related activities. Indeed, the Moroccan automotive sector has seen notable expansion due to the establishment of major manufacturers such as Renault and PSA, and the rise of suppliers (Jalila, 2022). This evolution in the sector is not limited to vehicle assembly alone but also extends to the local production of components and subassemblies (Khadija et al, 2015). Renowned companies such as Valeo, specializing in cable manufacturing, Delphi, the American group linked to General Motors, which has expanded its harness and automotive component manufacturing activities to Tangier, Labinal, and Yazaki have established their presence, according to data from the Moroccan Association of the Automotive Industry and Trade (AMICA, 2013), thus contributing to the diversification and complexity of the automotive supply chain. In developing

countries like Morocco, this supply chain typically involves automotive manufacturers, component suppliers (ranging from Tier 1 to Tier 3), distributors, dealers (retailers), and customers. Figure 1 below illustrates the number of entities involved in this chain.

Figure 1: Stakeholders in the Moroccan Automotive Supply Chain



Source: AMICA.

Effective management of the supply chain in the Moroccan automotive industry is of particular importance for both upstream operations (supplying factories) and downstream operations (distribution of finished products to customers) (Momoh, 2016). The complexity of this supply chain, covering stages from design through procurement, production, and up to distribution to customers, requires constant monitoring of management systems. Additionally, rapid technological growth in the automotive sector has introduced elements such as automation, IoT, and connectivity, transforming how the supply chain is managed (My Brahim, 2021).

However, this technological evolution also exposes the automotive supply chain to cybersecurity risks. Electronic interconnections between the different links in the chain create potential vulnerabilities to cyberattacks (Kache & Seuring, 2014). Indeed, data exchanges between manufacturers, suppliers, distributors and other actors in the chain are essential to ensure smooth coordination. Yet, increasing levels of cooperation and integration can introduce their own risks (Yoon et al, 2017), by increasing the number of potential access points for cyberattacks (Garvey et al, 2015).

Companies in the automotive sector often use integrated management systems to oversee their entire supply chain and promote integration among the different stakeholders in the chain (Moukadem & Elkharraz, 2019). These centralized systems are attractive targets for cybercriminals, as compromising a single point can lead to widespread repercussions. The inadequate security of some companies in the automotive sector against cyberattacks thus becomes a concerning issue that requires special attention to safeguard the integrity, confidentiality, and availability of critical data within the Moroccan automotive supply chain.

The need to guarantee the continuity of operations within the Moroccan automotive industry's supply chain makes the protection of IT systems and the management of cybersecurity risks crucial priorities (Pandey et al, 2020). This

requirement underscores the importance of a holistic approach to risk management within supply chains (Ghadge et al, 2012), raising the central question: what security measures are adopted by companies in the Moroccan automotive sector to counteract cyberattack threats targeting their supply chain?

The answer to this research problem allowed us to fill several significant gaps:

- Lack of information regarding the perception of supply chain managers in the automotive sector in Morocco towards cybersecurity.
- Lack of information on the specific cybersecurity practices adopted by companies in the Moroccan automotive sector to address cyberattack risks within the supply chain.

The objective of this research is to examine and understand the security measures currently implemented within certain companies that are part of the automotive supply chain in Morocco in response to cyberattack risks resulting from technological advancements.

The main aspects of this objective are as follows:

- Assessment of Security Measures: The study aims to evaluate the security measures implemented by certain companies in the automotive supply chain in Morocco to counter cyberattack risks.
- Comparative Study: The inclusion of varied samples, encompassing both small and medium-sized enterprises (SMEs) and large companies, suggests a desire to understand differences in security approaches based on company size. This could help identify specific needs for different types of businesses.

2. Research Methodology

2.1 Epistemological Positioning

Our research is primarily positioned within an exploratory perspective, an approach adopted when existing studies are limited, as highlighted by Martine Hlady (Martine Hlady, 2002). This context applies to our research, as our study focuses on risk management related to cyberattacks in the automotive supply chain in Morocco, a relatively unexplored area in the existing literature.

2.2 Empirical Approach

Our empirical approach is developed according to a qualitative methodology which favors the acquisition of detailed and substantial information. Indeed, the adoption of a qualitative study allows an in-depth exploration of the phenomena associated with the management of risks generated by cyberattacks within the automotive supply chain.

Information was collected through semi-structured individual interviews conducted with two information systems security managers from two large Moroccan automotive companies, as well as with two supply chain managers from two small and medium-sized automotive enterprises. To this end, we designed an interview guide to conduct the interviews appropriately.

The selection of these four studied companies was carried out in a non-arbitrary manner to allow for a comparison of the level of awareness and security approaches regarding cyberattack risks within these different entities interviewed. The table below provides a brief description of the companies and the interviewees, along with their main tasks within the automotive supply chain.

Table 1: Presentation of the Exploratory Study Sample

Company	Activity	Person interviewed	Main tasks
A	Automotive Manufacturer	Information Systems Security Manager (ISSM)	Monitoring the implementation of standards, procedures, and tools related to the security of the information system and the company's informational assets; providing training and advice on information systems security issues; and handling incidents related to the information system in use.
B	Manufacturing of electrical harnesses	Information Technology Manager (ITM)	Development, implementation, and maintenance of the company's IT systems
C	Manufacturing of automotive equipment	Supply Chain Manager	Coordination between different logistics departments and control of production
D	Production of wiring and electrical harnesses	Procurement Manager	Overseeing and supervising procurement operations and stock management

The choice of the Tangier-Tétouan-Al Hoceima region as a study area stems from its status as a central hub for automotive industrial production, particularly due to the iconic presence of the Renault factory, around which a pool of automotive industrial SMEs has developed.

3. Presentation of Results

Through the semi-structured interviews, we obtained information on the questions we had planned in advance. The main themes of the survey are: Awareness of Cybersecurity and the Security Measures Implemented.

3.1 Results Concerning Cybersecurity Awareness

For the theme of cybersecurity awareness, the managers from the two large companies (ISSM and ITM) view cybersecurity as an essential strategic component, receiving strong support from their management. This recognizes the critical importance of security for maintaining operational continuity and the company's reputation. Additionally, there is a shared understanding within the management of both companies regarding the need to maintain a robust security posture against emerging threats.

> *"The management is actively involved in developing security policies, aware of the crucial role of protecting the IT systems underpinning our supply chain. Regular communication channels are established with management to ensure mutual understanding of the challenges and ongoing support for cybersecurity initiatives."* (Excerpt from the ISSM's response)

For the SMEs in the automotive sector interviewed on the same topic, the first company acknowledges the growing importance of cybersecurity in the current context of Industry 4.0. However, it does not engage in advanced security measures, considering them to be an unnecessary additional cost.

On the other hand, for the second SME, according to the procurement manager, the management is starting to become aware of the importance of cybersecurity in its supply chain. However, it has not yet fully invested in establishing robust security policies. This company uses basic IT systems for inventory and order management, but its integrated digital technologies remain relatively basic. 'Cyberattack risks are not considered a major concern at the moment,' excerpt from the procurement manager's response at the automotive SME.

3.2 Results Concerning the Security Measures Implemented

The second theme of our interview addresses the security measures implemented. We asked a series of questions to delve deeper into this topic and gather more information. In fact, regarding the question of cyber risk assessment methods used throughout the supply chain, the responses varied between the two groups of companies. The large companies interviewed rely on a structured and comprehensive approach to assess cyber risks in the supply chain.

> "*We regularly conduct vulnerability assessments, perform penetration testing, and continuously monitor threats.*" (Excerpt from the response of the ISSM of the first large company)

> "*We primarily use the NIST Cybersecurity Framework as our reference framework, integrating its guiding principles: identification, protection, detection, response, and recovery. Consequently, we have established a detailed inventory of assets, considering their essential contribution to logistics operations and their potential impact in the event of a compromise.*" (Excerpt from the response of the IT Manager (ITM) of the second large company)

The statements from the managers of the SMEs interviewed highlight divergent approaches to assessing cyber risks along the supply chain. Indeed, the first SME is in the initial stages of a risk assessment process. They hold regular meetings to discuss potential threats and assess their impact. On the other hand, the second SME appears to adopt a more informal and operational approach.

In the absence of a dedicated risk assessment unit, they involve various departments of the company in risk management, focusing on the practical logistics aspects of their supply chain. This suggests a lower awareness of cyber risks and a stronger focus on daily operations.

For questions relating to security protocols aimed at ensuring the confidentiality and integrity of communications and data exchanged within the supply chain, as well as for measures guaranteeing the security of the management systems of this chain, in particular with regard to concerns the software used, and when it comes to managing access and identities of actors throughout the supply chain to avoid unauthorized access, responses varied. Indeed, information systems managers within the two large companies have implemented robust security measures. In this regard, one of these managers stated:

> "*We have implemented a series of robust security protocols to ensure the confidentiality and integrity of communications and data within our supply chain. Initially, we use secure connections, including TLS/SSL protocols, to encrypt data transmitted between different links in the chain.*"

Additionally, they enforce strict access management policies for communication systems. "*We have implemented a centralized identity management system with a role-based approach*". Each user is assigned privileges based on their responsibilities and operational needs.

Access rights are regularly reviewed to ensure they remain aligned with user needs. Additionally, regular IT security training is provided to raise awareness among users about risks and best practices regarding identity and access management.

Another response from the IT Manager (ITM) of the second company highlighting the high level of security within this company:

> "*We have implemented robust security protocols, including the use of secure connections via protocols such as SSH (Secure Shell). SSH is used to establish secure remote connections, providing a means to encrypt data exchanged between systems*".

Thus, access management in this company is rigorously controlled, with regular audits and security training sessions to maintain a high level of vigilance. The security of supply chain management systems is an absolute priority for the two IT security managers.

> "*We have implemented multilayered security measures to protect these critical systems. First, access to these systems is strictly controlled, with permissions granted on a need-to-know basis. Real-time monitoring mechanisms are in place to detect any suspicious activity or unauthorized access.*" (Extract from the ITM response)

These companies also implement regular software updates to address known vulnerabilities and conduct periodic security tests, including penetration testing, to assess the robustness of their systems.

> "*Regarding the SMEs, it is evident that their level of security is lower compared to the two large companies surveyed. Indeed, the responses reflect this observation: « We have not yet developed specific cybersecurity policies and procedures. Our efforts are primarily focused on the physical management of components. Although we use basic antivirus software, we have not yet invested in more advanced security solutions*." (Extract from the response of the supply chain manager of the first SME interviewed)

> "*We pay special attention to our supply chain management systems, focusing on enhancing our shipment tracking software and inventory systems. However, improvements are underway concerning access and identity management*." (Excerpt from the response of the procurement manager of the second SME interviewed)

Regarding questions related to specific business continuity plans in the event of a cyberattack affecting the supply chain, as well as the speed of operational recovery and collaboration with supply chain partners in the event of a cyber-incident, the responses reveal once again that large companies are better prepared to handle cyberattacks, while the interviewed SMEs are less prepared. Indeed, according to the ISSM's response concerning the business continuity plan in the event of a cyber-attack, he states that the business continuity plan has been drawn up to ensure a rapid and effective response, thereby minimising the impact on the supply chain. According to the same manager:

> "*In the event of an incident, our incident response team is activated immediately. The initial measures include isolating the threat, containing the spread, and assessing the extent of the damage. Simultaneously, internal communications are initiated to inform key stakeholders, including management, supply chain personnel, and other concerned parties*."

To ensure a rapid resumption of operations, the ISSM states that they have put in place frequent backups. Operational teams are trained to switch to manual processes, if necessary, while affected systems are restored from healthy versions. At the same time, post-incident analyses are carried out to understand the vulnerabilities and reinforce security measures where necessary.

In addition, the ISSM adds that collaboration with their supply chain partners in the event of a cyber-incident is an essential component of their risk management strategy.

> "*We have established shared communication and incident management protocols with our key partners. We activate these protocols immediately, enabling a rapid exchange of information on the nature of the attack, the measures taken, and the anticipated impact.*

This promotes a common understanding of the situation and facilitates a coordinated response".

"*We have detailed business continuity plans to deal with cyber-attacks. These plans include specific procedures for isolating the threat, restoring critical systems from back-up, and communicating effectively with internal and external stakeholders. Regular exercises are carried out to test the effectiveness of these plans*", declares the ITM of the second large company.

As for the responses from the SMEs' managers regarding these points, they are as follows:

"Currently, we have not yet developed a specific business continuity plan for cyberattacks. Our focus has primarily been on the operational and logistical aspects of our company. Developing a dedicated cybersecurity business continuity plan will be a priority in the future to ensure the resilience of our supply chain in the event of a cyber-incident", declares the supply chain manager.

According to the procurement manager:

"Continuity plans in the event of a cyberattack are being developed. Collaboration with our supply chain partners is a challenge, given our current level of integrated technologies. We are working on communication and incident management protocols, but progress is slow."

4. Discussion of Results

The results of these interviews reveal significant differences in the level of awareness and security approach to the risks of cyber-attacks within the different companies interviewed. The large companies interviewed, deploying substantial resources to secure their operations, demonstrate a keen awareness of potential threats, resulting in robust security measures. In contrast, the SMEs interviewed, though aware of the risks, show a lower level of preparedness against cyberattacks, highlighting a crucial need for increased awareness and the implementation of appropriate security measures within these smaller structures.

Indeed, the comparative analysis between the two large companies and the two SMEs interviewed reveals significant differences in terms of cybersecurity awareness, security measures implemented, and preparedness against cyberattacks.

4.1 Cybersecurity Awareness

- The managers interviewed from the two large companies consider cybersecurity as an essential strategic component, with strong support from management. They share an understanding of the challenges and maintain a robust security posture.
- The SMEs interviewed also recognize the importance of cybersecurity, but they are not as committed to advanced security measures, often due to budget constraints or a lack of resources.

4.2 Security Measures Implemented

- The two large companies surveyed have implemented robust security protocols, using secure connections, strict access and identity management policies, as well as regular audits and training on cybersecurity.
- The surveyed SMEs tend to have less advanced security measures, focusing more on the physical management of components or specific aspects of their supply chain. They are in the early stages of implementing risk assessment processes and strengthening security, but they are progressing more slowly.

4.3 Preparation for Cyberattacks

- The two large companies interviewed have detailed continuity plans for cyberattacks, including specific procedures for isolating the threat, restoring critical systems, and communicating with stakeholders. They also have shared communication and incident management protocols with their supply chain partners.
- The two SMEs are still developing their continuity plans. They acknowledge the need to collaborate with their supply chain partners in the event of an incident, but this can be a challenge due to their current technological level.

5. Conclusion

The automotive supply chain in Morocco plays a crucial role in the national economy as a driver of growth and development. Companies that make it up, whether large companies or SMEs, must recognize the strategic importance of effectively securing their operations against cyber threats. This recognition is all the more crucial in a context where cybersecurity has become a major concern with the advent of Industry 4.0.

Securing the automotive sector supply chain in Morocco against cyber threats is essential to guarantee the continuity of operations, protect the reputation of companies and maintain competitiveness in the global market. Investments in cybersecurity, collaboration between supply chain players (Sara & Khalid, 2022) and increased awareness of these issues are essential elements to meet this challenge (Abhijeet et al, 2020) and ensure a prosperous future for the automotive industry.

Conflict of Interest Statement

The authors declare no conflicts of interest.

About the Author(s)

Kenza Raissouni is a PhD student at the Industrial Technologies and Services Laboratory, Fez, Morocco.
ORCID: https://orcid.org/0009-0000-3167-6941
Errabih Zakia is a research professor and Head of the Management Techniques Department. Research laboratory: Industrial Technologies and Services (LTSI). Higher School of Technology. Sidi Mohamed Ben Abdellah University (USMBA) - FES – Morocco.
Raissouni Rajaa is a PhD in economics and management at the Centre for doctoral studies in economics and management and sustainable development, Abdelmalek Essaadi University, Tétouan, Morocco.
ORCID: https://orcid.org/0009-0003-1739-8975
Raissouni Mohammed Rabih PhD in didactics of physical sciences Department of Physics, Faculty of Sciences, Ibn Tofail University, Kénitra, Morocco. Teacher of physical sciences and their didactics, Centre régional des métiers de l'éducation et de la formation de Tanger, Tangiers, Morocco. Research interests: didactics of physical sciences and training of science teachers.
ORCID: https://orcid.org/0000-0002-6221-3736
Charroud Soukaina is a PhD student at the Industrial Technologies and Services Laboratory, Fez, Morocco.
Bourkkadi Salmane is a research professor at Poitiers University, France - Ibn Tofail University, Morocco.
ResearchGate : https://www.researchgate.net/profile/Salmane-Bourekkadi

References

Abhijeet G, Maximilian W, Nigel D C and Richard W, 2020. Managing cyber risk in supply chains, Supply Chain Management: An International Journal 25: 223–240. DOI 10.1108/SCM-10-2018-0357.

AMICA Association Marocaine pour l'Industrie et le Commerce de l'Automobile, 2013. L'industrie automobile au Maroc, opportunités et perspectives.

Benaini N, 2020. Intégration du Maroc dans les Chaînes de Valeur Mondiales : Cas du secteur de l'automobile, Revue Internationale du chercheur 1: 44-71.

Chaine Logistique Globale : Étude Exploratoire Auprès des Entreprises De L'industrie Automobile Au Maroc. European Scientific Journal. Doi:10.19044/esj.2019.v15n34p367.

Garvey, M.D., Carnovale, S. and Yeniyurt, S, 2015. An analytical framework for supply network risk propagation: a Bayesian network approach, European Journal of Operational Research 243: 618-627.

Ghadge A., Dani S. and Kalawsky R, 2012. Supply chain risk management: present and future scope, The International Journal of Logistics Management 23: 313-339.

Hugo WMJ, Badenhorst-Weiss JA, Van Biljon EHB, 2004. Supply chain management: logistics in perspective. 3rd edition, Pretoria, South Africa.

Jalila C, 2022. L'industrie de l'automobile au Maroc, réalités du présent et défis futurs -; Revue des Sciences Humaines et Sociales de l'Académie du Royaume du Maroc 1: 2820-7254.

Kache, F. and Seuring, S, 2014. Linking collaboration and integration to risk and performance in supply chains via a review of literature reviews, Supply Chain Management: An International Journal 19: 664-682.

Khadija R, Hicham Ji, Atmane B, 2015. Analyse et évaluation de la chaîne logistique automobile marocaine. https://hal.science/hal-01260703/document. Accessed 14 April 2024.

Martine Hlady R, 2002. La méthode des cas Application à la recherche en gestion. Collection : Perspectives marketing. Éditeur : De Boeck Supérieur. https://doi.org/10.3917/dbu.hlady.2002.01

Momoh, O, 2016. Supply chain attack, disponible à l'adresse : Accessed 14 April 2024

Moukadem K, & Elkharraz A, 2019. Systèmes D'information et Résilience De La

Mustafa Kamal, M. and Irani, Z, 2014.Analysing supply chain integration through a systematic literature review: a normative perspective", Supply Chain Management: An International Journal 19:523-557.

My Brahim I, 2021. Transformation digitale et industrie 4.0 : impact sur les PME du secteur automobile au Maroc. Revue internationale d'economie numérique, international journal of Digital Economy. ISSN : 2665-8151. Volume 3, N 2.

Pandey S. Singh R.K. Gunasekaran A. and Kaushik A, 2020. Cyber security risks in globalized supply chains: conceptual framework, Journal of Global Operations and Strategic Sourcing 13: 103-128.

Sara B L., & Khalid H, 2022. Collaboration in Supply Chain of the automotive industry in Morocco: Theoretical framework. International Journal of Accounting, Finance, Auditing, Management and Economics 3: 1-23. https://doi.org/10.5281/zenodo.6390278.

Yoon, J., Talluri, S., Yildiz, H. and Ho, W, 2017. Models for supplier selection and risk mitigation: a holistic approach", International Journal of Production Research, pp. 1-26.