Cybersecurity in the Context of Moroccan Energy Companies

K. RAISSOUNI[1], Z. ERRABIH[1], S. CHARROUD[1], R. RAISSOUNI[2], M. R. RAISSOUNI[3], S. BOUREKKADI[4]

[1]Laboratoire Technologies et Services Industriels, École Supérieure de Technologie, Université Sidi Mohamed Ben Abdellah, Maroc
[2]Centre des études doctorales en sciences économie et gestion et développement durable de l'Université Abdelmalek Essaadi, Maroc
[3]Materials and Subatomic Physics Laboratory, Faculty of Sciences, Ibn Tofail Université, Morocco
[4]EuRSED, O2 scientific production France

Abstract. The aim of this research is to assess the level of maturity of Moroccan companies in the energy sector in terms of cybersecurity and to identify the factors influencing their abilities to implement effective security measures to address the risks associated with cyber-attacks. To achieve this, we have adopted an exploratory approach. A questionnaire was sent to energy sector companies in Morocco to investigate their cybersecurity practices. This entails examining the current security measures in place, security policies and procedures, as well as employee training programs. Furthermore, we are exploring the human and financial factors that can influence the ability of energy companies to implement effective security measures against cyber- attacks. The results clearly indicate that most of these companies demonstrate a high level of maturity in terms of cybersecurity. However, several significant factors influence their ability to implement effective security measures. Among these factors, the lack of qualified personnel, the high costs associated with acquiring and implementing security technologies, as well as expenses related to training and awareness, can be mentioned.

Index Terms— Cyber-attack, Cyber risks, Cybersecurity, Energy sector, Maturity level, Moroccan energy companies, Security measures.

1 Introduction

Cybersecurity has become a crucial global issue due to the growing significance of information and communication technologies in our daily lives [1]. Indeed, digital transformation has impacted all sectors of a country's economy, rendering them vulnerable to cyber-attacks that can result in severe and costly consequences for individuals, companies, and governments [2]. Furthermore, they can also have an impact on the global economy by affecting the competitiveness of companies and disrupting supply chains [3]. This is why cybersecurity has become a crucial component of economic security. It is directly linked to a country's digital sovereignty. It adopts a comprehensive approach that goes beyond mere protection and attack of computer systems, aiming to monitor and take control of them. This can potentially result in reputation damage, theft of sensitive data, and digital hacking actions [4]. It encompasses computer networks, satellite links, cloud

systems, data and their exchanges, connected devices, mobility, and the development of medications [5] [6]. Cybersecurity also encompasses legal risks, both on an industrial and political level. It encompasses all laws, policies, tools, devices, concepts, and security mechanisms, as well as management methods. The means used to ensure cybersecurity can be of a technical, legal, methodological, or human nature [7].

In Morocco, cybersecurity has become an essential topic in political, economic, and social debates. Indeed, considering the stakes and risks associated with the envisioned openness and development outlined in the "Maroc Numeric 2013" plan, our country is now faced with the imperative of establishing mechanisms to protect and defend the information systems of governmental administrations, public organizations, and infrastructures of vital importance. Among these infrastructures, energy companies are of paramount importance, as they are considered critical actors for national security and the continuity of essential services, such as the production, transportation, and distribution of electricity and gas. Indeed, the digitization of energy systems has paved the way for new security threats, including cyber-attacks [8]. However, as a critical infrastructure for the country, this sector cannot afford any downtime or disruption due to a cyber-attack [9] [10]. Aware of these risks, Morocco is stepping up its efforts and demanding better risk management, hoping to ensure improved protection and an appropriate response in the event of a major incident. Indeed, the government has already taken a number of measures for the development of cybersecurity and the establishment of digital trust [11], including strengthening the legal framework through various laws such as Law 09-08 for the protection of personal data (12), Law 53-05 on electronic exchange of legal data, Law No. 43-05 on the security of computer systems, Law No. 05-20 on cybersecurity, aiming to strengthen the legal arsenal in the fight against cyber-attacks and cybercrime [13], and Decree No. 2.21 which defines measures for the protection of information systems in government administrations, public institutions and enterprises, as well as infrastructures of vital importance and private operators. One of the strengths of cybersecurity in Morocco is the adoption of standards by most organizations, as evidenced by the International Telecommunication Union. However, despite the legal arsenal available in Morocco, and as in all countries, the level of maturity in cybersecurity varies greatly depending on the sector of activity or the size of the company. Hence, our research problem is as follows: What is the level of maturity of companies in the energy sector in Morocco in terms of cybersecurity? And what are the factors that influence their ability to implement effective security measures to address the risks associated with cyber-attacks?

The answer to this research problem has allowed us to address several of the most significant gaps:

• A lack of knowledge about cybersecurity practices in the energy sector companies in Morocco,

• A lack of information on the human and financial factors that influence the ability of energy companies to implement effective security measures.

The objectives of our research are to assess the level of cybersecurity maturity of companies in the energy sector in Morocco, identify the factors that influence the ability of companies to implement effective security measures to address the risks associated with cyber- attacks, and propose recommendations to enhance the security posture of companies in the energy sector in Morocco. By studying this topic, we could help raise awareness among energy companies in Morocco of the importance of implementing effective security measures to protect their IT systems, data and critical infrastructures, and identify areas where improvements are needed, providing a solid foundation for future research on cybersecurity in the energy sector in Morocco and elsewhere.

2 Methodology

In this research, we adopted a quantitative approach to comprehensively collect data on the studied companies. This methodology allowed us to obtain measurable and quantifiable data, thus facilitating an objective analysis. With this approach, we were able to obtain accurate and relevant information to assess the level of maturity of companies in the energy sector in terms of cybersecurity and identify factors influencing their ability to implement adequate security measures. Based on this, we formulated concrete recommendations aimed at enhancing their resilience against cyber- attacks. In this regard, we developed a survey questionnaire that was validated by two information systems specialists. This questionnaire is structured into three main sections. The first section focuses on the professional profile of the participants as well as the characteristics of the energy companies they belong to, including their location and size. The second section focuses on evaluating the maturity of energy sector companies in terms of cybersecurity by exploring their security framework. This framework encompasses a range of organizational resources related to cybersecurity, such as regulations, policies, specialized workforce, processes, practices, and technologies. It also includes an incident response plan aimed at assessing and mitigating cyber-attacks. The third section examines various factors that influence the ability of energy companies to implement effective security measures to address the risks of cyber-attacks. Once our questionnaire was developed using the Google Forms tool, we distributed it to the various stakeholders through two distinct communication channels. Initially, we sent out the questionnaires via email, accompanied by a concise introduction explaining the purpose of the study and emphasizing the importance of their participation. Participants were then able to fill out the questionnaire online at their convenience. Additionally, we also utilized WhatsApp to share the questionnaire with contacts identified within the relevant companies. This multi-channel approach allowed us to maximize the chances of participation and obtain representative responses. The data collection period extended over four months, from February 1, 2023, to the end of May 2023, ensuring ample participation and ensuring the relevance of the obtained results. The data collected from the respondents were subjected to statistical analysis using Microsoft Excel software. The results will be presented in a clear and concise manner, utilizing graphs and tables to facilitate the understanding and interpretation of the findings. The questionnaire was administered to a variety of players within companies, with respondents including senior executives, information systems security managers, information systems directors, as well as key employees involved in cybersecurity operations, such as IT security engineers and IT technicians. The study was conducted in different regions of Morocco, with a specific focus on the Tanger-Tétouan-Al Hoceïma region, Rabat-Salé-Kénitra, and the Casablanca-Settat region, targeting energy sector companies present in these locations. Most of the companies that responded to the questionnaire were large, which can be attributed to the fact that large companies generally invest more in cybersecurity, followed by medium-sized and small companies.

3 Data collection and analysis

3.1 Cybersecurity Framework and Intervention Plan

The first questions that we consider crucial in our questionnaire are the adoption of security standards and the monitoring of compliance with standards. The responses to these questions are highlighted in the following diagrams:

Fig. 1. Adopted Security Standards.

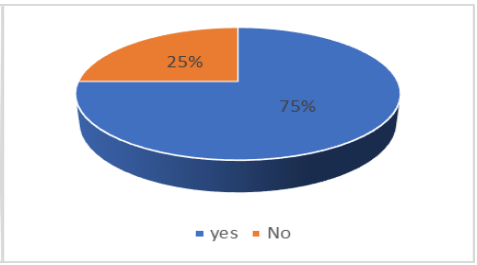

Fig. 2. Standards compliance monitoring.

We have also shown a keen interest in matters related to the implementation of a cybersecurity program within energy companies, as well as the main security systems used. The answers to these inquiries are clearly presented in the following tables:

Table 1. Possession of a cybersecurity program.

Possession of a cybersecurity program	Percentage%
Yes	80
No	20

Table 2. Main security systems used.

security systems used	Percentage%
Endpoints	90
Network security	75
Data protection	40
data traceability	60
Other	15

Furthermore, the responses regarding the identity of the person responsible for the cybersecurity function, the number of employees dedicated to cybersecurity, and the employee training and awareness programs in cybersecurity are highlighted in the following diagrams:

Table 3. Cybersecurity manager.

Cybersecurity manager	Percentage %
(ISSR)	70
(ISD)	55
Director	15
Other	5

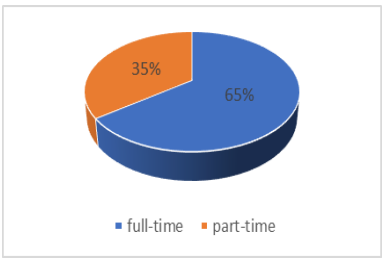

Fig. 3. employees assigned to cybersecurity.

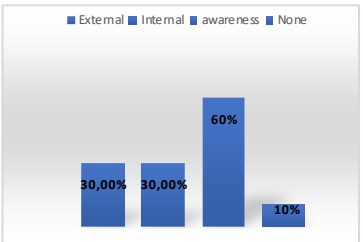

Fig. 4. Training and Awareness.

In addition, the following figures depict the responses regarding energy companies' possession of the key elements of an intervention plan:

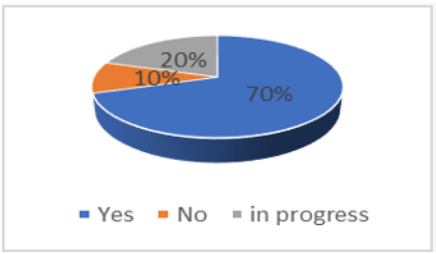

Fig. 5. Possession of an Incident Response Plan.

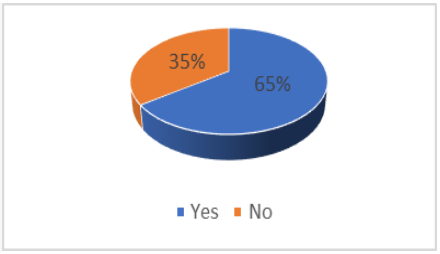

Fig. 6. Cyberattack Simulations.

3.2 Factors Influencing the Ability of Energy Companies to Implement Effective Security Measures

The responses to the corresponding questions have been presented in two separate tables for ease of analysis:

Table 4. Human Factors.

Human factors	Percentage%
Lack of qualified employees	75
Organizational culture	60
High salaries	55

Table 5. Financial Factors.

Financial factors	Percentage %
High security technology costs	85
High training and awareness costs	55
High regulatory compliance costs	65

4 Results

4.1 Cybersecurity Framework and Intervention Plan

4.1.1 Cybersecurity Framework

Among the surveyed energy sector companies, it is noteworthy that 85% of them have adopted one or more security standards. The most adopted standard is Law 09-08, which represents 75% of the cases. Next, the ISO 27100 standard is adopted by 65% of the companies, and the DNSSI standard by 60% of them. Furthermore, 20% of the companies mentioned other security standards, such as the Moroccan CNDP regulation or the European GDPR (Figure 1).
In addition, it is important to note that among the companies that have adopted standards and regulations, 75% of them regularly perform checks to ensure compliance, while 25% stated that they do not do it periodically (Figure 2).
Moreover, it is also noticeable that 80% of the surveyed companies claim to have implemented a cybersecurity program incorporating security protocols to address incidents

affecting information security. However, a small group of approximately 20% of the companies do not have it (Table 1).
Regarding the security technologies used, it appears that in the surveyed companies, Endpoint access protection and network security are widely implemented. The adoption rates are (90%) and (75%) respectively. The utilization rate of data protection solutions is (40%), data traceability solution is at 60%, and 15% use other systems (Table 2).
In terms of cybersecurity management, 70% of companies have entrusted cybersecurity to an Information Systems Security Responsible (ISSR), 55% have entrusted this responsibility to the Information Systems Director (ISD), 15% have delegated it to the company's director, and 5% have opted for other approaches, such as internal IT technicians or external service providers (Table 3).
Regarding the cybersecurity team, the majority of the surveyed companies affirm that they have two or fewer employees assigned to cybersecurity. Specifically, (35%) of companies state that they have one part-time employee dedicated to cybersecurity, while (65%) of companies state that they have two full-time employees dedicated to cybersecurity (Figure 3). When it comes to employee cybersecurity training, 30% of the surveyed energy companies provide external training, 30% offer internal training, and 60% have implemented awareness programs. However, 10% of the companies do not offer any cybersecurity training programs (Figure 4).

4.1.2 Intervention Plan

The cybersecurity intervention plan is a vital tool to ensure a consistent, coordinated, and effective response to security incidents [14]. The results show that 70% of the surveyed companies have an Incident Response Plan (IRP). 20% state that the implementation of IRPs is currently underway. The companies without an IRP represent a percentage of 10% (Figure 5). For cyberattack simulations, the graph shows that 65% of companies maintain their Incident Response Plan (IRP) by conducting cybersecurity defense exercises or penetration testing, while 35% do not perform any simulations. Regarding the frequency of these tests, the majority of companies conduct these exercises annually (Figure 6).

4.2 Factors Influencing the Ability of Energy Companies to Implement

The survey results reveal two key factors that impact the ability of energy sector companies in Morocco to implement effective security measures: human factors and financial factors. Regarding the former, the data indicates that 75% of companies identified the lack of qualified employees as the main factor influencing their ability to implement effective security measures. Additionally, 60% emphasized the importance of organizational culture as a determining factor in this capacity. Furthermore, 55% of companies mentioned that high salaries for cybersecurity professionals constitute a factor influencing their ability to implement effective security measures. (Table 4).
Regarding the financial factors, the survey results show that 85% of the surveyed companies identified high costs associated with acquiring and implementing security technologies as the primary factor influencing their ability to implement effective security measures. Additionally, 55% of companies highlighted that high costs associated with training and awareness pose a barrier to implementing effective security measures, while 65% of companies indicated that regulatory compliance costs were a factor influencing their ability to implement adequate security measures (Table 5).

5 Discussion

Our research question is relevant in the current context of cybersecurity for companies, which is a timely topic due to the increasing global cyberattacks. Energy companies are particularly vulnerable to cyberattacks because they rely on critical systems for energy production, distribution, and management.

Through a comprehensive analysis of the cybersecurity framework and the cybersecurity intervention plan, we have gained a deep understanding of the proactive and reactive approach adopted by energy companies to manage cybersecurity risks. This assessment has allowed us to evaluate the maturity level of energy companies in Morocco regarding cybersecurity. Through our meticulous survey, we have accurately identified the key factors that influence the ability of energy companies to implement effective security measures.

The results obtained reveal that Moroccan energy companies display a high level of maturity in cybersecurity. This observation can be attributed to the majority of these companies being large in size. However, there are factors influencing their ability to develop adequate security measures. The strong adherence of companies, at a rate of 85%, to one or more national or international standards is clear evidence of this advanced maturity. This highlights the full commitment of energy sector companies to cybersecurity and underscores the crucial importance of regulatory frameworks for these entities. Additionally, the fact that 80% of surveyed companies affirm having implemented a cybersecurity program may indicate a certain level of cybersecurity maturity. This suggests that the majority of companies recognize the importance of cybersecurity and have taken measures to protect their systems, data, and infrastructure against cyber threats. However, it is important to note that a significant 20% of companies have not yet set up a cybersecurity program, and this mainly concerns small and medium-sized businesses. It is therefore imperative for these companies to reassess their strategic approach to cybersecurity as the consequences of a successful cyberattack targeting their systems and infrastructure could result in significant disruptions in energy supply, substantial material damages, and even pose risks to public safety [15].

Furthermore, it is observed that the protection of Endpoint access points and network security are widely deployed aspects in the surveyed companies. Indeed, the respective implementation rates of these measures are 90% and 75%. These percentages demonstrate that these companies have taken significant measures to secure their network connections in order to prevent cyberattacks.

Regarding cybersecurity management, it is interesting to note that 70% of companies have chosen to entrust this responsibility to an Information Systems Security Responsible (ISSR), and 55% of companies have decided to assign this task to the Information Systems Director (ISD), demonstrating the importance attached to this function within the company and a willingness to entrust this responsibility to competent experts. This also indicates a positive sign of maturity in terms of cybersecurity.

In terms of employee training in cybersecurity, the results indicate that the majority of surveyed companies recognize the importance of training and awareness in cybersecurity. Awareness programs can help strengthen the security culture within the company and educate employees about risks and best practices in cybersecurity. However, the presence of a significant percentage (10%) of companies not offering any cybersecurity training program may indicate a lack of maturity or awareness in some energy sector companies, particularly smaller ones.

So far, we have focused the discussion on the proactive elements of a cybersecurity plan. Another essential aspect of cybersecurity is the reactive intervention plan. The results indicate that the majority of surveyed companies have an incident response plan (IRP). The availability of this plan demonstrates preparedness and the ability to respond to security

incidents in an organized manner. Additionally, 65% of companies conducting cyber-attack simulations indicate a willingness to regularly test and evaluate the implemented security measures [16], ensuring their effectiveness and adaptability to new threats. However, the fact that 10% of companies do not have such a plan, 20% are in the process of implementing IRPs, and 35% do not conduct any simulations highlights the need for further improvement in cybersecurity, particularly for small and medium-sized enterprises. It is crucial for all energy companies in Morocco, regardless of their size, to adopt a collective approach that emphasizes collaboration in the implementation of prevention, detection, and incident response strategies, the adoption of advanced security technologies such as external cloud storage [17], and the sharing of information on threats and cybersecurity incidents. This collaboration will strengthen the resilience of the entire sector and enable a more effective response to cyber-attacks.

Regarding the factors influencing the ability of energy companies to implement effective security measures, the survey results indicate that 75% of the companies have identified a lack of qualified employees as the primary human factor influencing their ability to implement effective security measures. This finding is supported by the fact that there is an insufficient number of cybersecurity specialists within these companies. Indeed, having two full-time employees dedicated to cybersecurity can be considered a reasonable approach for some small or medium-sized enterprises, especially if they do not have a large IT infrastructure or operate in a sector particularly sensitive to cyber threats such as the energy sector. Furthermore, respondents indicate that organizational culture has a significant impact on their cybersecurity capabilities. A company culture that values security, encourages continuous learning, and promotes individual and collective accountability strengthens the company's commitment to security, and vice versa [18].

For the financial factors, the majority of surveyed companies identified the high costs associated with acquiring and implementing security technologies as the main factor influencing their ability to implement effective security measures. The financial investment required to obtain advanced security technologies can pose a challenge for some companies with budget constraints [19]. Furthermore, the obligation for energy companies to comply with national and international cybersecurity standards and regulations can also result in significant expenses, greatly impacting their ability to adopt adequate security measures. The high costs associated with training and awareness programs also pose a challenge to implementing effective security measures, as these programs require substantial financial resources.

Finally, despite the promising results obtained in this study, it is essential to consider the limitations of our research. First, collecting reliable and accurate data poses a challenge in this field, especially when companies are reluctant to share information about security incidents or the security measures they have implemented. Additionally, this research focused on a limited sample of energy companies in Morocco, which may limit the generalization of the findings to the entire sector.

6 Conclusions

Based on the results obtained to address our research question regarding the maturity level of energy sector companies in Morocco in terms of cybersecurity and the factors influencing their ability to implement effective security measures against cyberattacks, it is clear that the majority of these companies demonstrate a high level of cybersecurity maturity. Furthermore, the survey results indicate that the lack of qualified employees, organizational culture, and high salaries for cybersecurity professionals are significant human factors that influence companies' ability to implement effective security measures. Alongside, the high costs associated with acquiring and implementing security

technologies, training and awareness costs, as well as regulatory compliance costs, have been identified as significant financial factors that affect this capability. The identification of these factors has enabled us to formulate targeted recommendations to enhance cybersecurity in the Moroccan energy sector:

- Implement attractive recruitment and retention programs;
- Conduct a salary benchmarking analysis to understand market standards and ensure competitive compensation;
- Promote a security culture that encourages individual and collective responsibility in cybersecurity;
- Invest in effective security technologies;
- Consider cloud-based security solutions;
- Develop internal training and awareness programs;
- Find more efficient and cost-effective ways to comply with regulations.

References

1. A. Barichella, Cybersécurité des infrastructures énergétiques. Regards croisés Europe /Etats Unis, Ifri (2018)
2. Li. Yuchong, Liu. Qinghui, A comprehensive review study of cyber-attacks and cyber security ; Emerging trends and recent developments, E R 7 (2021)
3. A. Ghadge, M. Weiß, N. D. Caldwell, R. Wilding, Managing cyber risk in supply chains: a review and research agenda, Supply Chain Management, A I J **25**, 2 (2020)
4. A. S. Zaidoun, *Sécurité informatique Concepts et outils*. ISTE, Londres (2023)
5. D. Ventre, *Intelligence artificielle*, *cybersécurité et cyberdéfense*, ISTE, Londres (2020)
6. L. Basset, Compte rendu de [Cyberattaque et cyberdéfense, Daniel Ventre, 2011, Paris, Lavoisier, 312 p.] Études internationales, **43**, 3 (2012). https://doi.org/10.7202/1012824ar
7. J. P. Damiano, La cybersécurité : contexte, enjeux, constats et perspectives Cybersecurity, IESF (2023)
8. I. Onyeji, M. Bazilian, C. Bronk, Cyber Security and Critical Energy Infrastructure, T E J, **27**, 2 (2014)
9. G. Desarnaud, cyberattaques et systèmes énergétiques : faire face au risque, Étude de l'Ifri, (2017)
10. P. Sanders, c. Bronk, M. D. Bazilian, Critical energy infrastructure and the evolution of cybersecurity, E J **35**, 10 (2022)
11. Administration de la Défense Nationale, Stratégie Nationale en matière de Cybersécurité, Royaume Du Maroc (2012) www.dgssi.gov.ma
12. H. Kounaidi, Y. Mazouz, M. Kounaidi, Impact de la loi 09-08 sur la gouvernance des systèmes d'information des administrations publiques marocaines, R C C A, **7** (2018)
13. M. K. MISSAOUI, A. ELHILA, Criminal law and ethics put to the test of cybercrime. JEMED, **4**, 2, (2021)
14. Guide pratique pour les entreprises, *Gestion des risques liés à la cybersécurité*, Version 3 (2017)
15. A. Bendovschi, Cyber-Attacks – Trends, Patterns and Security Countermeasures, P E F, **28,** 24 – 31, (2015)

16. Z. Errabih, Crisis Management and Business continuity: Luxury or Necessity? Case of large and medium-sized companies in the Rabat – Casablanca. R I S G. 2, (2019)
17. S. Cale, M. Chaveyriat, S. Lenco, Cloud externe : les meilleures pratiques pour assurer son utilisation en toute sécurité. S S, **25**, 48-58, (2017). https://doi.org/10.3917/sestr.025.0048
18. M.I. Al-Ghamdi, Effects of knowledge of cyber security on prevention of attacks, J B A S, (2021)
19. D. ULAS, Digital Transformation Process and SMEs. P C S, **158**, 662-671, (2019)