Cyber-attack crisis management in the context of energy companies

Kenza RAISSOUNI[1], Zakia ERRABIH[1], Salmane Bourekkadi[2], Rajaa RAISSOUNI[2]

[1] Industrial Technologies and Services Laboratory, Higher School Of Technology, Fez, Morocco
[2] University of Poitiers, France - Ibn Tofail University, Morocco

Abstract. The aim of this research is to present and analyze a set of public or private energy companies that have been victims of cyber-attacks, while identifying various lessons that can guide other companies towards effective crisis management in response to this risk. To achieve this, we have adopted an exploratory approach that involves utilizing, in an original manner, the raw material derived from a collection of published articles and other documents that have addressed and presented the phenomenon of cyber-attacks on private and public energy companies. The main findings of this study demonstrate that, for effective management of a cyber-attack crisis, legislation must serve as a catalyst for anticipating and managing the crisis through innovative and ambitious draft texts. Additionally, companies must possess the necessary skills and expertise to respond to cyberattack crises, including the technical infrastructure and software required to counter cyber incidents. Furthermore, fostering a collaborative and multi-disciplinary team-building capacity led by a pilot with a comprehensive and unified vision, along with the ability to make prompt decisions, is of paramount importance.

keywords — Crisis management, Cyber-attack, Cyber crisis, Cyber Crisis management, cyber risk, Energy compagnies, Types of cyber-attacks.

1 Introduction

The cyber-attack represents a crisis of unparalleled severity that weighs on companies. The very foundations of crisis management are often challenged due to the cyber-specificity of these attacks. The attack on a computerized information system has taken on a new dimension since the advent of the World Wide Web in 1990, further intensifying with the evolution of a society where the exponential generation of information remains uninterrupted [1]. The challenges inherent in this situation are compounded by the growing fragility of information systems, accentuated by the massive and diversified flow of data to be processed, as well as its speed of circulation. Given the global reach of the Web, no industry, type, or size of company is immune to cyber-attacks [2]. In the energy sector, the unprecedented deployment of information and communication technologies in infrastructure exposes these systems to potential vulnerabilities and unprecedented risks related to data security and cyber-attacks [3]. The critical nature of operations in the energy industry makes them particularly enticing targets for cybercriminals and hackers, all driven by the desire to exploit these weaknesses to inflict considerable damage. Faced with a cyber-attack, energy companies must be able to respond quickly and appropriately. That is why it is important to decide in advance how to handle certain situations rather than waiting

to be confronted with them for the first time during an incident, and then developing a plan to mitigate damage, reduce costs and recovery time, and communicate with internal and external stakeholders becomes crucial.
Research importance: Attacks on energy infrastructure can have devastating consequences on the economy, society, and public health. Therefore, effective crisis management of cyber-attacks is essential to ensure continuous availability of energy and prevent major disruptions that could result from these attacks.
Research objective: The presentation and analysis of a set of cases of public or private energy companies that have been victims of cyber-attacks, can nevertheless identify various lessons, and draw the attention of managers to the problem, Additionally, it is important to raise awareness about the reality and magnitude of the threat in a society where Big Data serves as a source of knowledge but also vulnerability. This awareness can help companies improve their crisis management strategies to effectively respond to the risks posed by cyber-attacks.
Research methodology: We adopted an exploratory approach that involved utilizing the raw material derived from a collection of published articles and other relevant documents addressing the phenomenon of cyber-attacks against public and private companies. This approach allowed us to offer an original perspective on the subject matter.

2 Cyber- attacks

2.1 Definitions and conceptualization of cyber-attack

The term "computer network attack" has been replaced by "cyber-attack," referring to acts of aggression in cyberspace. Cyber-attacks target different aspects of the digital realm, combining the concepts of "cyberspace" and "attack." This term acknowledges the evolving threats in the digital domain and emphasizes the need for a comprehensive understanding of these attacks [4]. In the military domain, a cyber-attack is defined in the 2010 U.S. Department of defense lexicon as "a hostile act that utilizes computers, computer networks, or computerized systems to modify or destroy the critical cyber systems, assets, or functions of an adversary" [5]. According to [6], a cyber-attack can be compared to a modern act of piracy with the primary objective of stealing or destroying information through unauthorized network access. It represents a criminal act and, in its most severe forms, can even be considered a terrorist action. According to [7], cyber-attacks exploit one or more vulnerabilities in information system security, such as inadequate protection, weak security coding, human negligence regarding security protocols, technological flaws, unknown viruses, and identity deception. Another definition characterizes cyber-attacks as targeted attacks on the computerized information systems of companies or organizations [8]. Additionally, [5] mentions that cyber-attacks can circumvent existing protections to gain access to strategic information, hold the company for ransom, damage its reputation, or even completely obliterate it. According to [9], a cyber-attack is a purposeful intrusion into computer systems with malicious intent, targeting various computing devices such as computers, servers, printers, and communication devices. It is important to note that damage to the computer system can also result from errors or negligence, not just malicious acts. Another source [10], a cyber-attack is defined as "a deliberate individual or collective action aimed at compromising the integrity of a person's, enterprise's, organization's, or state's computerized information system, utilizing all or part of the Internet network."
Cyber-attacks pose a significant and often underestimated threat to both public and private companies. When targeted by these attacks, companies experience enormous financial losses and reputational damage [11]. According to [12], certain companies are more

susceptible to cyber-attacks, particularly those in the e-commerce industry that handle sensitive user data.
We can say, Cyber-attacks have diverse definitions across countries, NGOs, international organizations, cybersecurity experts, and authors. In summary, a cyber-attack is a deliberate and malicious action carried out in cyberspace to harm information systems. It can lead to damaging consequences like identity theft, unauthorized access, system infiltration, widespread information system degradation, and exploitation of web browsers.

2.2 Motivation of cyber-attack

There are several motivations behind cyber-attacks, and it is important to note that these motivations can vary depending on the situation. Attackers may have multiple motivations simultaneously. Here are some of the most common reasons:
• Financial Gain: Cybercriminals target financial resources and sensitive information, which can be sold on the black market. Ransomware, a malicious software that infects numerous computers, is commonly utilized for these purposes. Notable instances of such attacks include the WannaCry and NotPetya ransomware attacks in May and June 2017, respectively.
• Ideology-driven cyber-attacks: Hackers with specific ideological beliefs, like libertarian hackers, may target news agencies in response to perceived attacks on freedom of expression. An example of this occurred with a pro-Russian news agency in Ukraine, which was subjected to cyber-attacks with the intention of shutting it down.
• Coercion (blackmail, threats, etc.): Cybercriminals may resort to coercion by threatening to disclose private data or inflict harm on a computer system unless a ransom demand is fulfilled.
• Curiosity or personal pleasure: Some individuals reveal vulnerabilities in systems to showcase their talent to the hacker community, while others launch attacks for recreational purposes or amusement.

2.3 Anatomy of a successful cyber-attack

Although attacks utilize various methods, they generally follow a series of common steps.
Most successful attacks adhere to a standardized process, as depicted in Figure 1.
To defend against cyber-attacks, it is crucial to comprehend the typical pattern of these steps:
• Cyber Scanning: Hackers identify a vulnerable target and plan their attack by determining the best method to exploit it. The initial target can be anyone within a company, from administrators to directors. With an entry point secured, attackers launch their assault, often utilizing targeted phishing emails to introduce malware.
• Exploration: After identifying the target, hackers search for vulnerabilities to infiltrate the company's network. They utilize easily accessible internet tools to explore the network and find entry points. This step can be time-consuming, sometimes spanning several months, as criminals work to identify vulnerabilities.
• Access and elevation: After identifying network vulnerabilities, attackers aim to gain privileged access and escalate their privileges in the targeted system. This allows them to move freely within the environment. Rainbow Boards and similar tools are used to steal credentials and elevate privileges to the admin level, granting attackers control over accessible network systems. Once attackers have acquired elevated privileges, they can exploit the compromised network at will, as outlined in the Microsoft STRIDE model.
• Exfiltration: With unrestricted access to the network, attackers can enter systems that house the organization's most sensitive data, which they can extract at their discretion.

However, in addition to stealing private data, they can also modify or delete files on compromised systems.
• Wait: Once attackers gain unrestricted access to the targeted network, their goal is to remain undetected by deploying covert malware such as rootkits. This enables them to regain access in the future and freely navigate the compromised network with elevated privileges.
• Assault: During this stage, cybercriminals have the capability to manipulate or disable the victim's hardware. A notable example is the Stuxnet attack on critical infrastructure in Iran. However, the duration of the assault phase is typically short-lived.
• Obfuscation: Obfuscation techniques, including log file cleaning, spoofing, disinformation, zombie accounts, and Trojan horse commands, are employed to impede legal investigations, create confusion, and mislead investigators.

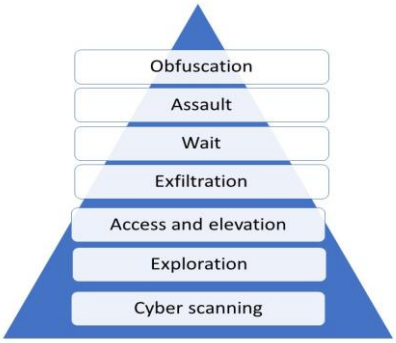

Fig. 1. Anatomy of a typical cyber-attack.

2.4 The most common types of cyber-attacks

In general, there are several types of cyberattacks, with the most common ones including:
• Denial of service (DoS) and distributed denial of service (DDoS): In a denial-of-service attack, access to a computer or network is intentionally blocked or degraded by a malicious user. This is typically done by disrupting network connections or overwhelming the targeted system until it becomes overloaded and ceases to function [13]. A distributed denial of service (DDoS) attack, on the other hand, targets a system's resources, but it is carried out from numerous other infected host machines controlled by the attacker. Due to their simplicity, DDoS attacks are often considered "low-end" by hackers, yet they are still commonly employed [11].
• Phishing and spear phishing attacks: Phishing is a technique that aims to deceive users into revealing sensitive information, such as passwords or credit card numbers, by sending them emails that appear to be from trusted sources. This method combines social engineering and technical deception. It may involve an email attachment that installs malware on the recipient's computer or a link to a fraudulent website designed to trick users into downloading malware or disclosing personal information. A spear phishing attack typically involves the impersonation of a sender and utilizes strong social engineering to link the subject of the email and the body of the message to the targeted person's or organization's activities.
• A password attack: Because passwords are the most frequently used mechanism for authenticating users of IT systems, acquiring passwords is a common and effective attack method. A person's password can be obtained through various means, such as searching their physical office, monitoring network connections to acquire unencrypted passwords, using social engineering techniques, accessing a password database, or simply guessing.

• Attack by malicious software: Malware can be described as unwanted software installed on your system without your consent. It can attach itself to legitimate code, spread, hide in useful applications, or replicate itself on the Internet.
• Ransomware attacks: These attacks aim to encrypt company files and demand a ransom for decryption, leading to disruptions in business operations and significant financial losses. Attackers disable the victim's computer or information system and use cryptographic techniques to render the data inaccessible. They then send an encrypted message offering decryption in exchange for a ransom payment [14].

3 cyber crisis

3.1 Definition: What is a cyber crisis?

Each field develops its own definitions, and different authors and researchers may have their own interpretations, none of which are inherently less valid than others. When it comes to cyber crises, they can be characterized by their ability to initiate without detection by the involved individuals, often through a passive cyber-attack that plans to transition into an active phase. The ANSSI Guide explains that referring to a "cyber crisis" is inappropriate and suggests that it is more accurate to discuss "crises originating from a cyber- attack." According to the guide, a cyber crisis occurs when one or more malicious actions on the information system (IS) result in a significant destabilization of the entity. The guide defines a cyber crisis as a rare event with a strong impact [15]. However, it is important to note that not every event arising from cyberspace and causing damage to information systems is automatically classified as a cyber- attack. Additionally, the statement that a cyber crisis is a "rare event with a strong impact" implies that rarity is no longer a defining characteristic of a crisis.

3.2 Examples of cyber-attack crisis in Energy companies

There are many examples of cyber-attack crisis over the years:
• Saudi Aramco (2012): The hacker group "Cutting Sword of Justice" orchestrated a ransomware attack against Saudi Arabia's oil giant, the world's largest oil producer with a daily output of 10.5 million barrels. The attack occurred during the holy month of Ramadan. As a result, all operations, except for industrial activities, were brought to a halt, rendering sales impossible.
• Energy companies in the United States and Western Europe (2014): They were infected by a virus like Stuxnet, called Energetic Bear. The malware primarily targeted electricity producers, electricity and oil distribution network operators, and equipment manufacturers. It allowed attackers to take control of industrial equipment. The group behind the virus allegedly first infected three industrial control system equipment manufacturers, who then transmitted the virus to their energy clients during update operations.
• Norsk Hydro (2019): The root cause of the cyber-attack, as well as the solution to mitigate it, were identified with valuable assistance from Microsoft and other IT security partners. Furthermore, due to a robust backup policy, the company was confident in its ability to recover the data without having to pay the ransom.
• SolarWinds (2020): A massive cyber espionage attack targeting software provider SolarWinds has been uncovered, impacting multiple U.S. government entities and companies. The attack exploited a vulnerability in SolarWinds infrastructure management software, allowing unauthorized access to sensitive network and confidential data.

• Colonial Pipeline (2021): Colonial Pipeline, the largest supplier of petroleum products in the United States, has been targeted in a ransomware attack. The hackers gained access to the pipeline system by utilizing a stolen VPN account and password belonging to one of the employees, subsequently encrypting the data. To prevent a potential industrial disaster, Colonial Pipeline made the decision to shut down its industrial system. Despite paying the ransom in bitcoins, panic buyers exacerbated the situation, resulting in a widespread gasoline shortage.

These examples illustrate the severe consequences that cyber-attacks can have on companies and governments. The impacts can be diverse, encompassing legal, regulatory, business, organizational, HR, financial, reputation, and technical aspects. Therefore, it is crucial to take proactive and effective measures to manage minor security incidents and build resilience in preparation for major crises. The journey towards resilience involves implementing the fundamental principles of cyber-attack crisis management, which will be outlined below.

3.3 Managing Cyber-attack Crises

The key to a company's success lies not only in anticipating crises but also in continuously preventing, managing, and mitigating small incidents along with their cumulative effects. By being prepared for major crises and emerging stronger and better equipped, companies can achieve resilience.

The path to resilience inevitably involves following the fundamental principles of cyber crisis management:

• Legislation as a Tool for Anticipating and Managing Cyber Crises;
• Technologies and Governance;
• The skills and expertise of reaction;
• The piloting at the heart of the crisis.

3.3.1 Legislation as a Tool for Anticipating and Managing Cyber Crises

Legislation serves as a reminder that there are no voids or lawless zones in cyberspace. Recognizing this is crucial for anticipating threats and avoiding engaging in illegal activities when in doubt, as well as being able to identify oneself as a victim if necessary [16]. Furthermore, in the event of a crisis, it is essential to have a solid grasp of the legal dimension to effectively manage the potential consequences.

Legislation on cybersecurity and cybercrime varies significantly from country to country. Some nations have not yet enacted specific laws to address online crime, while others have stringent legislation in place to regulate online activities. In the United States, the Computer Fraud and Abuse Act (CFAA) is a significant law that criminalizes illicit online activities such as hacking, online fraud, and unauthorized transmission of protected data. The European Union has implemented the General Data Protection Regulation (GDPR), which sets forth regulations for safeguarding personal data online.

In Morocco, the legislation on cybercrime and cybersecurity aims to protect both citizens and companies from the risks associated with cyber-attacks. Several relevant laws and regulations have been implemented to achieve this objective:

• Law 09-08 targets computer crimes against companies, including theft of confidential information and computer sabotage.
• Law 30-13 establishes obligations for companies to protect the personal data of employees and customers.
• ISO 27001 information security standard offers a framework for managing information security in organizations and includes measures to safeguard against online threats.

In conclusion, legislation plays a significant role in managing cyber-attack crises by creating legal frameworks for protecting computer systems and sensitive data, establishing security standards, and defining liability for companies and governments in case of a cyber-attack. This encourages the adoption of stricter security practices and provides avenues for justice and recovery for cyber-attack victims. However, it is crucial to understand that legislation alone is not sufficient for effective management of cyber-attack crises.

3.3.2 Technical and governance

Collaboration and synergy between the multidisciplinary crisis management team and governance are vital for effective management of a cyber-attack crisis. Pre-planning by governance enables faster and integrated crisis management, involving the right stakeholders promptly. Governance also plays a crucial role in establishing internal escalation processes with predefined communication channels and clear roles and responsibilities.
During a crisis, governance provides strategic information and guidance to direct the actions of technical teams, offering them a set of "rules of engagement". Therefore, it is crucial for companies to establish a governance structure that defines clear roles and responsibilities for various stakeholders involved in cyber crisis management. Additionally, comprehensive security policies and procedures that apply organization-wide should be implemented.

3.3.3 The skills and expertise of reaction

Several essential elements contribute to effective cyber-attack crisis management, enabling companies to prepare for and respond to cyber-incidents:
• The first crucial element is to have a well-trained organization with adequate resources. [17] highlights the importance of having highly skilled employees who are not only responsive to cyber risks but also possess the necessary abilities to prevent such risks.
• Next comes governance, specifically the establishment of procedures that form a crisis management intervention plan. This plan aims to ensure data protection, preserve the company's reputation, and reduce costs.
• Lastly, the company must have the necessary technical resources, including infrastructure and software, to effectively counter cyber- incidents.

as a final point, to ensure effective cyber-attack crisis management, conducting a cyber-attack simulation is crucial. This simulation enables the testing of crisis management procedures in a near-realistic scenario. It is considered one of the most comprehensive methods to engage the entire company in responding to a cyber-attack, identifying vulnerabilities at the organizational, technical, and procedural levels. This helps raise awareness and prioritize computer security measures based on the specific needs of the company.

3.3.4 the piloting at the heart of the crisis

The growing complexity of cyber-attacks, which can impact multiple facets of a company, necessitates a holistic and synchronized approach from the organization. The crisis pilot assumes a pivotal role in this endeavor, ensuring efficient coordination among various departments and prompt implementation of appropriate responses [18]. The crisis pilot plays a crucial role in coordinating various departments, including information systems, incident response, and security management. They possess technical expertise, collaborate

with teams for digital investigations, advise on cybersecurity solutions, and effectively communicate with the management committee. Their ultimate objective is to empower managers with the information and tools needed to make informed decisions during uncertain situations.

4 Discussion

The management of cyber-attack crises in the context of energy companies is a crucial topic that requires special attention. In our study, we examined the most common types of cyber-attacks faced by energy companies, providing concrete examples of companies that have fallen victim to such attacks. By analyzing these examples, we found that the key to successfully addressing these risks lies not only in anticipating the crisis but primarily in continuous prevention to manage, or even eliminate, small incidents and their cumulative effects. This approach aims to prepare for a potential major crisis while emerging stronger and better prepared. This approach can be referred to as "resilience" [19]. The path to resilience in cyber crisis management inevitably involves the following fundamental aspects: legislation through clear laws and regulations; technology and governance; skills and expertise in response; and the strong leadership. These findings partially align with those of other studies on cyber risk management in companies [20].

5 Conclusion

Cyber crises are complex, and it is crucial to be prepared, considering the uniqueness of each crisis. Cyber-attack crisis management is intricate and constantly evolving, requiring meticulous preparation and strategic planning. To effectively prepare for cyber-attacks, organizations must have a comprehensive understanding of legal frameworks and enforce strict compliance with laws, regulations, and standards [21]. Additionally, establishing a governance structure that clearly defines roles and responsibilities for all stakeholders involved in crisis management is crucial. Developing well-defined crisis management plans and ensuring that professionals are trained and proficient in their respective roles are essential for swift and efficient responses to cyber-attacks. Therefore, it is vital for companies to adopt an integrated approach to cyber crisis management that encompasses legislative, technical, governance, process, and communication elements. This comprehensive approach equips organizations with the readiness and capability to effectively handle cyber- attacks.

References

1. H. Chen, R.H. Chiang, V.C. Storey, Business intelligence and analytics: from big data to big impact, M I S Q, **36**, 4 (2012)
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. P. Sanders, c. Bronk, MD. Bazilian, Critical energy infrastructure and the evolution of cybersecurity, E J **35**, Issue 10 (2022)
4. D. ventre. *Cyberattaque et cyberdéfense*, Collection cyberconflits et cybercriminalité, La voisier, Paris (2011)
5. Joint Chiefs of Staff, *joint terminology for cyberspace operations*, DoD, Etats-Unis, (2010).
6. O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel, The law of cyber-attack. C L R **100**, 4 (2012)

7. F. Pasqualetti, F. Dörfler, F. Bullo, Attack detection and identification in cyber-physical systems, IEEE T A C, **58**, 2715-2729, (2013)
8. C. Lala, B. Panda, Evaluating damage from cyber-attacks: a model and analysis, IEEE T S, 31, 4 (2001)
9. CLUSIF, Club de la sécurité de l'information français, Fiches Incidents Cyber SI Industriels, (2017), Available from: https://clusif.fr/publications/fiches-incidents-cyber-industriels-2017/ [Accessed 08/05/23].
10. J. M. Lehu, Cyberattaque :la gestion du risque est-elle encore possible ? Analyse et enseignements du cas Sony Pictures, R S G, 291-292, 41-50. (2018)
11. Imrani, O.E.et al. , Impact of industrial free zones on the business environment of emerging countries , cta Logistica, 2023, 10(1), pp. 105–110
12. A. De Mereuil, A.M. Bonnefous, Anatomie d'une cyber-attaque contre une entreprise: comprendre et prévenir les attaques par déni de service, A M - G C, 123, 5-14 (2016)
13. M. Warren, W. Hutchinson, Cyber-attacks against supply chain management systems: a short note, I J P D & L M, **30**, 710-716 (2000)
14. J.K. Deane, C.L. Rees, W.H. Baker, Assessing the information technology security risk in medical supply chains, I J E M R, **3**, 145-155 (2010)
15. ANSSI, Agence Nationale de la Sécurité des systèmes d'information, *Attaques par rançongiciels : comment les anticiper et réagir en cas d'incident*, Collection Gestion de Crise Cyber, (2020)
16. ANSSI, Agence Nationale de la Sécurité des Systèmes d'information, *Cris d'origine cyber, les clés d'une gestion opérationnelle et stratégique*, Collection Gestion de Crise Cyber, (2021)
17. L. Raimondo, *les fondamentaux de la gestion de crise cyber*, Editions Ellipses, paris, (2022)
18. A. Khursheed, M. Kumar, M. Sharma, Security against cyber-attacks in food industry, I J C T A, **9**, 17, 8623-8628 (2016)
19. L. Schaedler, L. Graf-Vlachy, A. Konig, Strategic leadership in organizational crises: A review and research agenda, L R P **55** (2022)
20. C. Kuffner, M. Kopyoto, A.J. Wohlleber, E. Hartmann,The interplay between relationships, technologies and organizational structures in enhancing supply chain resilience: empirical evidence from a Delphi study, I J P D & L M **52**, 8, 673-699 (2022)
21. Kassou, M., Bourekkadi, et al. (2021) . Blockchain-based medical and water waste management conception. E3S Web of Conferences, 2021, 234, 00070
22. El imrani, O. et al (2022). The consumer price index and it effect in the new ecosystems and energy consumption during the sanitary confinement: The case of an emerging country. IOP Conference Series: Earth and Environmental Science , 975(1), 012006
23. A. Tajer, O. Araban, F. E. Belfatmi, S.M. Rigar, Gouvernance et résilience des PME à l'ère de la crise sanitaire du COVID 19. R I S G 5, 3 (2022)
24. ANSSI, Agence Nationale de la Sécurité des Systèmes d'information, *Panorama de la Cybermenace*, Collection Gestion de Crise Cyber, (2022)