

# Cybersecurity Challenges in Critical Infrastructure: A Perspective on Regulations and Competence in Luxembourg

Maxime Naval, Erik Perjons<sup>a</sup> and Simon Hacks<sup>b</sup>

*Department of Computer and System Sciences, Stockholm University, Stockholm, Sweden  
maxime.naval@protonmail.com, {perjons, simon.hacks}@dsv.su.se*

**Keywords:** Critical Infrastructure, Cyber-Security Challenges, Luxembourg, Thematic Analysis.

**Abstract:** Critical infrastructure (CI) faces a growing threat of cyber-attacks as digitalization expands across industries, necessitating robust cyber-security measures. This study focuses on the challenges of securing CI in Luxembourg, exploring both regulatory and organizational aspects. Semi-structured interviews with chief information security officers (CISOs) within Luxembourg's CI sectors were conducted to gather insights. Thematic analysis revealed six key challenge themes: Regulatory Compliance, Industry Landscape and Adaptation, Resource Management, External Collaboration and Support, IT Infrastructure Management, and Operational Governance. The findings underscore the need for a comprehensive, multi-faceted approach involving international regulation alignment, streamlined reporting, enhanced national cyber-security support, government initiatives, and ongoing harmonization efforts across nations to address cyber-security challenges in critical infrastructure effectively.

## 1 INTRODUCTION


Critical infrastructure (CI) can be defined as “the body of systems, networks, and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public’s health and/or safety” (Grigalashvili, 2022). Examples of CI are systems, networks, and assets in energy supply, telecommunications, transportation, water and wastewater management, healthcare, finance, emergency and security services, and digital infrastructure. Cyber-attacks targeting CI can devastate nations and their citizens (Riggs et al., 2023). Therefore, ensuring CI security against cyber threats is paramount.


Recent trends indicate a rise in cyber-attacks on critical infrastructure (Serpanos and Komninos, 2022), prompting various sectors of society to enhance their cybersecurity measures for defense. While larger European countries have been dealing with significant cyber-attacks on CI for many years, Luxembourg, which is in focus in this study, has only recently been the victim of such targets (Creos, 2022; Kollwelter, 2022).

Governments and international organizations have

proposed new legislation and regulations for securing CI. For instance, the recently adopted NIS2 directive by the EU mandates all EU member states to integrate its provisions into national law (European Parliament and the Council of the European Union, 2022). As a result, all EU member states are required to implement this new directive into national law. The new legislation builds on the first NIS directive, adopted in 2016 (European Parliament and the Council of the European Union, 2016). Further, NIS2 broadens the definition of CI sectors, thus increasing the number of societal actors affected by these changes. Challenges may arise during implementation in various CI sectors under this new legislative environment due to the added complexity of coordinating efforts between organizations and government agencies (Kshetri, 2015; Peters, 2018; Laegreid et al., 2015).

Digitalization has increased the interconnections between IT systems across industries, escalating the complexity of managing IT assets. However, the human resources required to oversee IT infrastructure have not always kept pace with this growing demand (Gurpreet et al., 2019). Today, nearly every employee interacts with some form of IT system to perform their work tasks, which amplifies overall vulnerabilities. Consequently, organizations are increasingly focusing on training personnel to mitigate cyber incidents. The effectiveness of these efforts, however,

<sup>a</sup>  <https://orcid.org/0000-0001-9044-5836>

<sup>b</sup>  <https://orcid.org/0000-0003-0478-9347>

largely depends on the available resources and the internal business culture (Sohrabi Safa et al., 2015).

Within an organization, these challenges are usually managed by the chief information security officer (CISO). The CISO is tasked with devising and executing the organization's information security strategy and overseeing its cyber-security operations (Maynard et al., 2018). In the rapidly evolving technological landscape impacting CI, CISOs face new challenges involving managing increasing IT assets and implementing regulatory requirements. Adequate financial and human resources are crucial for CISOs to successfully fulfill this mission, representing the primary constraints to achieving robust information security (Johnson and Goetz, 2007).

Accordingly, this paper investigates cyber-security vulnerabilities and regulations in CI and issues related to human competence, focusing on Luxembourg. Therefore, we will answer the following research question: *What are the challenges associated with implementing cybersecurity measures in critical infrastructure, and which are the potential solutions to address them?*

The rest of the paper is structured as follows. First, we overview common cybersecurity vulnerabilities in CI. Next, we examine EU legislation addressing these vulnerabilities. Then, we present a qualitative analysis of interviews with Luxembourg's CI CISOs, highlighting challenges and solutions for implementing cybersecurity measures. Finally, we discuss the results' implications and suggest future research directions.

## 2 BACKGROUND

### 2.1 Cyber-Security Vulnerabilities in Critical Infrastructure

Most industries have fully embraced digital transformation in recent years, making the business world increasingly reliant on a highly intricate network of interconnected technologies. This digital transformation has also extended to CI, where information and communication technologies (ICT) have enhanced efficiency and flexibility. Integrating advanced computing and industrial automation has contributed to increased output. Additionally, these advancements enable predictive and remote maintenance, addressing issues before they escalate into more costly problems that could lead to severe outages (Antova, 2020).

Implementing ICT has brought numerous benefits to daily operations in CI, including real-time remote

maintenance and monitoring, system interconnectivity, and enhanced communication with external networks. However, these advancements have also introduced new attack vectors (Stergiopoulos et al., 2020). Recent trends show a concerning rise in cyber-attacks on CI, with significant implications for affected states. For example, in Germany, the Federal Office for Information Security (BSI) reported 452 cyber-security incidents affecting CI in 2022. However, many incidents are believed to go unreported due to concerns about reputational damage (Bundesamt für Sicherheit in der Informationstechnik, 2022). The estimated damage from cyber-attacks on CI in the same year amounted to over 200 billion euros in Germany (Beil, 2023).

Although tools are essential to a cyber-security strategy within CI, human resources remain the most crucial security component (Alessandro et al., 2020). In a security context, human error can be defined using the insider anomaly concept, distinguishing unintentional, intentional, and malicious human errors. Unintentional human error arises from a lack of organized information or operational skills, which can lead to inadvertent mistakes. This type of error may persist as unintentional or evolve into intentional or malicious actions. Intentional human error occurs when a user knowingly engages in risky activities or misuses resources. While these actions may not immediately impact the organization, they can potentially violate privacy rights or other regulations. The most severe form of human error involves deliberate actions aimed at causing harmful consequences (Ait Maalem Lahcen et al., 2020). The level of exposure to IT systems varies according to each role. Still, in today's highly digitalized work environment, every employee poses a potential vulnerability within the overall cyber-security strategy.

Different reports estimate that 82 % to 95 % of organizational data breaches can be attributed to human error (Verizon, 2022; Tessian, 2020; World Economic Forum, 2022). The most common vectors involving a human factor in cyber-security incidents are phishing attacks, misuse of credentials, and scans and exploits (IBM Security, 2023). Another crucial aspect of human error is evident in incident response. Upon discovering an incident, executing a well-defined response plan that adheres to internal cyber-security policies and procedures is essential. The absence of such policies can result in delayed responses to alerts, inadequate adherence to incident response protocols, or errors during the investigation phase, all of which increase security risks.

## 2.2 European Cyber-Security Legislation

The **NIS2 directive** (European Parliament and the Council of the European Union, 2022) broadens objectives and scope of applicability compared to NIS1. NIS2 imposes new cyber-security obligations on companies, state-owned enterprises, and public authorities in critical sectors across the EU, which are vital to the economy and society. Additionally, NIS2 extends coverage to include medium-sized and large institutions that NIS1 does not fully cover. The directive mandates enhanced requirements for cyber-security risk management measures and reporting obligations in response to online attacks and resulting data breaches. This includes audit requirements, risk assessments, and timely installation of updates and certifications.

The **Cyber-security Act** (European Parliament and the Council of the European Union, 2019) was introduced in 2017 as part of a comprehensive package of measures to enhance cyber-security and strengthen resilience against cyber-attacks by the EU. It poses an EU framework for IT security certification of products, services, and processes while considering their criticality.

The **Cyber Resilience Act** (European Commission, 2022) aims to complement the NIS2 directive by regulating connected devices, which have garnered attention due to their security vulnerabilities. Many manufacturers of these products have been found to prioritize cost, or lack sufficient expertise in cyber-security. This could lead to vulnerabilities that expose sensitive personal data to malicious hackers or facilitate other cyber attacks too easily.

## 2.3 Cyber-Security in Luxembourg

ENISA, the European Union Agency for Cybersecurity, serves as a coordinator at the European level. ENISA provides expert network and information security advice to national authorities and EU institutions. It also acts as a forum for exchanging best practices and facilitates communication between EU institutions, public authorities, and organizations.

On a national level, Luxembourg established the High Commission for National Protection (HCPN) in 2016, effectively serving as the National Agency for Information Systems Security. The HCPN’s primary mission includes issuing recommendations for implementing information security policies and guidelines to government agencies. It also plays a crucial role in supporting the implementation of the State’s general information security policy. Upon request, the HCPN

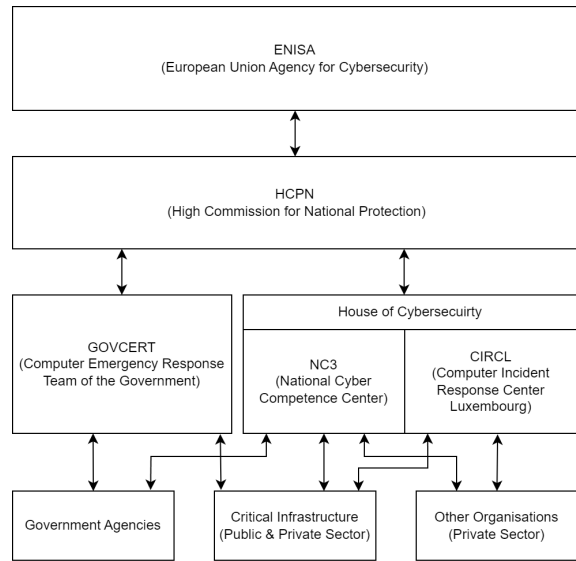


Figure 1: Hierarchical Model of the Coordination between Entities in Luxembourg.

advises public agencies and critical infrastructure (CI) institutions on network and information system security and associated risks (Haut-Commissariat à la protection nationale, 2023).

Figure 1 illustrates the organizational structure of cyber-security entities in Luxembourg. Under the HCPN, the Governmental Computer Emergency Response Team (GOVCERT) manages incidents for government agencies and selected CI institutions within both public and private sectors (CERT governmental Luxembourg, 2023). The Computer Incident Response Center Luxembourg (CIRCL) handles incidents from non-CI private sector entities. Both CIRCL and the National Cyber Competence Center (NC3) operate under the Luxembourg House of Cybersecurity, serving as a cornerstone for advancing cyber resilience in Luxembourg. The Luxembourg House of Cybersecurity fosters innovation, enhances competencies, and promotes collaboration across all societal levels (Luxembourg House of Cybersecurity, 2023).

The coordination among these cyber-security agencies and stakeholders in Luxembourg is articulated in the current 4th national cyber-security strategy, covering the period up to 2025 as published by the Luxembourgish Government. This strategy outlines guidelines and initiatives to enhance cyber-space security through coordinated efforts among stakeholders (Cybersecurity Luxembourg, 2020).

## 2.4 Related Work

(Teixeira et al., 2019) conducted a systematic literature review of 32 studies to identify critical success factors in implementing GDPR. Their findings reveal that GDPR compliance is frequently intricate and subjective, leading to extensive and time-consuming processes. The study underscores the substantial financial and human resources required for effective implementation, highlighting challenges stemming from a lack of privacy knowledge and expertise.

Another relevant literature review by (Hussain et al., 2020), analyzed 33 articles to delineate cyber-security challenges and emerging threats. The review emphasizes the significance of comprehending how these challenges are perceived and tackled, especially within cyber-security. Identified challenges encompass cyber-security governance, robust risk management practices, and promoting a culture of awareness. Effective governance is essential for organizations handling critical global data, providing a secure operational framework.

While raising awareness is crucial in cybersecurity, the effectiveness of training can vary significantly depending on its format and approach. (Chowdhury and Gkioulos, 2021) analyzed 68 articles to assess the effectiveness of cyber-security training in CI sectors. Their findings indicate that hands-on training in team-based scenarios, often using simulation and virtualization platforms, is among the most effective methods. However, they also noted a lack of consensus among researchers regarding the optimal training solutions. A significant barrier to implementing cyber-security training is the insufficient allocation of resources, and the associated costs (Chowdhury and Gkioulos, 2021).

The results of these literature review studies were also found in more focused research papers examining CI. In the water sector, incidents often stem from inadequate security skills and insufficient training (Amin et al., 2020). Similarly, the healthcare sector faces cybersecurity challenges exacerbated by limited budget allocations for cyber-security measures (Javaid et al., 2023). Additionally, the lack of support from executive management, who control budgets and policies, poses a critical obstacle (Chaudhary et al., 2023).

(Rawindaran et al., 2023) explore the cyber-security challenges of Wales's small and medium enterprises (SMEs). They highlight that government cybersecurity policies and regulations often cater more to large organizations, leaving SMEs struggling to properly adopt policies within their sector or comply with regulatory requirements. Given that the Luxem-

bourgish government and its critical infrastructure organizations can be classified as SMEs, this study aims to extend Rawindaran et al.'s research by providing an international perspective.

Makrakis et al. (Makrakis et al., 2021) provide an in-depth analysis of vulnerabilities and attacks targeting critical infrastructures, highlighting the increased risks introduced by integrating operational technology with modern IT frameworks. Their work emphasizes the complexities of defending aging systems against modern cyber threats. In a complementary study, Kampourakis et al. (Kampourakis et al., 2023) conduct a systematic review of wireless security testbeds in cyber-physical systems (CPS), addressing the dual challenges of leveraging wireless technologies for flexibility and mitigating the expanded attack surface they create. Their findings underscore the need for modular and robust testbed architectures to enhance CPS security research.

The contribution of this article is distinguished from the other works mentioned in related research by its focus on the specific context of Luxembourg's critical infrastructure (CI) cybersecurity challenges, particularly from a regulatory and organizational perspective. Unlike previous studies, such as (Teixeira et al., 2019), which examined the broader challenges of implementing GDPR across multiple sectors, or (Hussain et al., 2020), which explored general cybersecurity challenges and governance issues, this study provides a localized and detailed analysis of Luxembourg's unique cybersecurity landscape. It builds on existing frameworks but dives deeper into how regulations like the NIS2 directive are being interpreted and applied in Luxembourg's CI sectors, and how the country's smaller size and resource limitations affect the ability of CISOs to implement cybersecurity measures effectively. The article further expands on (Rawindaran et al., 2023) by offering insights into the international and European harmonization challenges faced by Luxembourg, a country with a comparatively lower IT maturity level, adding valuable localized insights to the global discourse on CI cybersecurity.

## 3 METHOD

We opted for a survey research strategy (Denscombe, 2021) to answer the research question. The survey allowed for the exploration of the perceptions of CISOs in various CI sectors across Luxembourg, providing rich insights into their perspectives on regulatory and organizational challenges related to cybersecurity. The semi-structured interview approach was selected to enable participants to share their experiences

and opinions flexibly and in-depth, capturing the nuances of cybersecurity implementation.

Participant selection involved purposive sampling, where CISOs from different CI sectors defined by the NIS2 directive were contacted. The goal was to ensure representation from sectors such as financial, healthcare, energy, communications, and wastewater treatment. Seven CISOs agreed to participate, offering a diverse yet focused sample size. Despite the limited number of participants, including key sectors, valuable insights into the cybersecurity challenges specific to Luxembourg's CI landscape were provided.

The data collection process involved semi-structured interviews conducted via Zoom and MS Teams, lasting between 30 and 45 minutes to accommodate the busy schedules of CISOs. Interviews were conducted in English, French, and Luxembourgish, depending on the participant's preference, which necessitated translation and transcription. The questions (cf. Appendix) were designed around two main areas: organizational aspects, which included collaboration and external partnerships, and regulatory aspects, focusing on compliance, legislation, and resource management.

Data analysis was conducted using thematic analysis (Denscombe, 2021). This method involved multiple stages, including familiarization with the data, coding, and theme development. In the initial coding phase, 197 codes were identified. Through an iterative process, redundant or overlapping codes were refined and rephrased, resulting in 165 codes. These codes were then grouped into broader themes aligned with the study's focus on regulatory compliance, resource management, industry landscape adaptation, and external collaboration.

## 4 RESULTS

The thematic analysis resulted in six main themes and their sub-themes (cf. Figure 2), which will be explained below. Moreover, challenges and, in some cases, solutions were identified for each sub-theme. Cited statements have been paraphrased and translated into English.

### 4.1 Regulatory Challenges and Compliance

**Different National Transpositions:** The European Directives NIS1 and NIS2 require implementation into national legislation. However, participants noted that interpretations of these directives can vary

among member states. Differences in the expertise of national regulatory bodies significantly influence these interpretations. One participant highlighted that Luxembourg generally has a lower IT maturity level than Anglo-Saxon countries, impacting various sectors and organizations, and posing challenges in interactions with regulatory bodies. Two participants also mentioned that varying business process requirements complicate collaboration with international partners. For example, one participant stated, "... we have partners in Germany or France, which have different processes, which make collaboration difficult."

**Extra-European Markets:** While most participants advocated for greater harmonization within the European market, two participants highlighted challenges related to operations outside the European Market, the so-called extra-European markets. This can lead to significant resource constraints because companies operating in extra-European markets must ensure compliance with diverse regulatory requirements across multiple jurisdictions. One participant stated, "Since we operate in the EU and US markets, we sometimes find ourselves running compliance audits for different regulatory entities in both markets, which requires a lot of time and effort." Therefore, two participants expressed a desire for more international harmonization of regulation.

**Cloud-Related Compliance Issues:** The adoption of cloud solutions continues to rise across all sectors, driven by their potential to enhance operational efficiency and increase value generation. However, one participant highlighted a significant concern: "There are not many players around, and the biggest ones are all American and do not meet all the regulatory requirements imposed by the EU." A prominent example is the recently enacted Cloud Act by the US (115th Congress of the United States, 2018), which requires US companies to grant US intelligence agencies access to their data. This mandate contradicts EU privacy laws and prohibits personal data transfer from EU users to the US. As the EU and the US negotiate new agreements, European organizations may face challenges where they cannot avoid using certain business solutions without compromising regulatory compliance: "If you take Office365 or M365 as an example, most organizations have no way around these solutions, yet these cloud solutions are not completely GDPR compliant."

**Financial Penalties:** Financial penalties can be imposed on organizations for non-compliance with

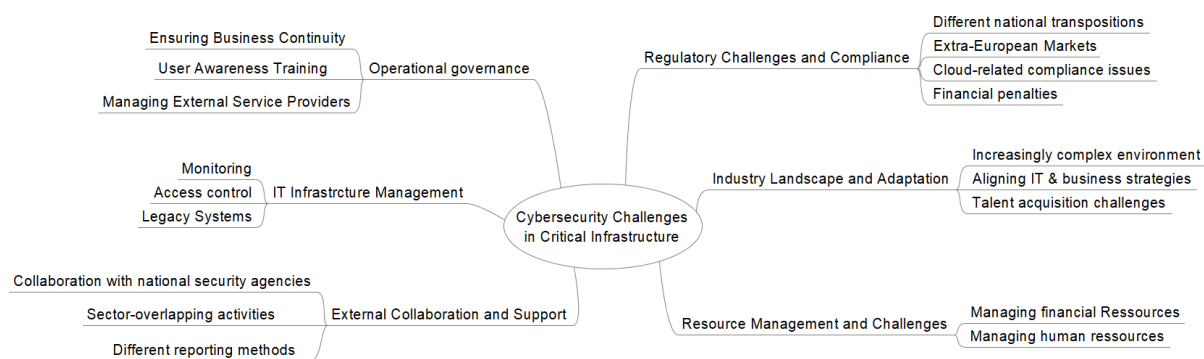


Figure 2: Thematic Analysis Results.

regulations, adding extra pressure on cyber-security and compliance teams, according to two participants, and is expressed in the following way by one of them: "The risk of being fined add pressure to decision-makers, which ultimately is passed on to the team and increases the stress." Another participant noted that this enforcement of regulations is "unfortunately necessary as it is sometimes the only way to compel decision-makers within an organization to take appropriate action."

## 4.2 Industry Landscape and Adaptation

**Increasingly Complex Environment:** Two participants highlighted a growing concern over cyber-attacks targeting infrastructure, stressing the urgency as malicious actors exploit vulnerabilities. These threats are becoming more sophisticated, using advanced techniques that require constant vigilance. CI systems have also become increasingly interconnected, facing greater complexity in cyber-security, exposing them to multiple threat vectors. Additionally, two participants noted the rapid introduction of new regulations, which demand significant resources for assessment and implementation. The interconnected nature of CI sectors also raises the risk of cascading disruptions. Therefore, operators must balance the imperative to modernize their systems with the need to secure them effectively, ensuring the stability and resilience of essential services.

**Aligning IT and Business Strategies:** Aligning IT with business strategies presents significant cyber-security challenges. Both areas must work closely to ensure that technology projects align with overall organizational objectives, as stressed by two participants. Two participants also mentioned difficulties in gaining organizational decision-makers' support for such alignment, although one did not face this issue. One participant emphasized the need to foster

a collaborative culture and improve communication to secure support from decision-makers. Furthermore, two participants highlighted the importance of conducting regular risk assessments and integrating security measures into strategic planning. This helps to ensure that IT and business strategies work together effectively.

**Talent Acquisition Challenges:** Two participants highlighted that the IT industry's growing complexity and rapid adoption of new technologies necessitate organizations to recruit new personnel for project management and robust cyber-security operations. Furthermore, investments in training and upskilling existing staff are crucial to adapt to the evolving threat landscape. However, the participants identified three key challenges in talent acquisition. First, specific technologies require rare skill sets that are challenging to find in the market. Secondly, the field of cyber-security is expanding rapidly, leading to a general shortage of professionals. Thirdly, even when talent is available in the Luxembourg job market, organizations struggle to meet or sustain competitive salary expectations, making it difficult to attract and retain skilled professionals. As stated by one participant: "Some experts are very hard to come by, and even when you find them, it is not easy to make them an offer that they accept." Another participant claimed that the lack of new talent needs to be tackled on a national basis.

## 4.3 Resource Management

**Managing Financial Resources:** Financial constraints pose a significant challenge in achieving complete cyber-resilience for CI operators. One participant explained that limited budgets, influenced by various operational and economic factors, often hinder their ability to upgrade IT infrastructure or implement comprehensive protection strategies: "If you look at the regulatory requirements, you often

find yourself wanting to revise your entire infrastructure, but are limited by budget constraints.” Despite these constraints, CI operators rely on rigorous risk assessments to prioritize security initiatives based on the criticality of assets and potential impact. According to one participant, balancing investments in security technologies with maintaining operational efficiency is an ongoing struggle, exacerbated by the continuous updates required to defend against evolving cyber threats, further stretching already tight financial resources.

**Managing Human Resources:** Two participants emphasized that the CISO role should be part of senior management, enabling easier collaboration with department supervisors and better integrating cybersecurity strategies into overall business planning. This structure is common in larger organizations with dedicated departments for specific tasks due to their larger staff numbers. However, smaller organizations cannot create dedicated departments for operations. Therefore, the individual responsible for cybersecurity in these organizations often handles additional roles and remains closely involved in daily IT operations, not solely focused on security tasks: “We are a small team, where it is not feasible to dedicate the supervision of information security to a single role.”

#### 4.4 External Collaboration and Support

**Collaboration with National Security Agencies:** The level of guidance from national security agencies varied significantly. Participants wanted more information sharing from agencies for assistance with new regulations and security processes. CIRCL was the most frequently mentioned partner, cited by six participants, while GovCert, HCPN, and ENISA were each named by four. The amount and frequency of information exchanged also varied. CIRCL was noted for its assistance with security processes and best practices. One participant received regular vulnerability updates from CIRCL without direct collaboration. GovCert and ENISA were praised for providing relevant cybersecurity information, with one organization participating in an ENISA-led emergency simulation. Two organizations regularly exchanged information with HCPN, which oversees process implementations. Next to the four cybersecurity agencies mentioned above, the Institut Luxembourgeois de Régulation (ILR) was also named a frequent exchange partner by six organizations. As the main regulatory body, the ILR has been described as overseeing compliance with

regulations and providing some guidance towards implementation strategies.

**Sector-Overlapping Activities:** A common concern among participants was the unclear scope of each agency. While GovCert handles the public sector and CIRCL the private sector, both interact with organizations in both areas. Some organizations are state and privately owned, making it unclear which agency to contact for assistance: “Since we are partly public, partly private, it is not always clear if we fall into the CIRCL’s or GovCert’s scope, which sometimes feels like being a second class client for both of them.”

**Different Reporting Methods:** Six participants reported having to file reports to at least one agency and facing challenges due to differing reporting methods. One participant noted that HCPN and ILR require different risk management approaches, leading to multiple reports for the same event. Additionally, those operating in multiple sectors must report to various regulatory bodies using different methods and deadlines. This process is time-consuming and resource-intensive. Participants expressed a need for more harmonization in reporting methods to alleviate these burdens.

#### 4.5 IT Infrastructure Management

**Monitoring:** All participants emphasized the necessity of continuous IT infrastructure monitoring to detect abnormal behavior. This is challenging due to the complexity of CI operators’ IT environment. Participants noted that various systems require unique monitoring approaches and custom adaptations: “We have legacy systems that cannot be integrated into modern monitoring solutions.” Hiring specialized experts might be necessary but is not always feasible, often resulting in outsourcing monitoring to external partners, adding another layer of complexity.

**Access Controls:** Most participants stated that they had implemented access controls to prevent unauthorized users from taking unwanted actions on their systems. The most common methods for access control were 2FA authentication, role-based access control, and data encryption. Participants emphasized that managing these controls is an ongoing process, necessitating regular updates. Additionally, two participants utilized private intranet networks to shield internal communications from external interference. A significant challenge mentioned was the resistance from end-users, who often viewed these measures as overly restrictive.

**Legacy Systems:** Legacy systems pose significant challenges due to their susceptibility to modern threats. They often lack essential security features, have unpatched vulnerabilities, or use weak authentication methods. Participants also noted that monitoring these systems is not always feasible. However, migration projects are complex, costly, and sometimes impractical, making it difficult for organizations to comply with regulatory requirements.

#### 4.6 Operational Governance

**Ensuring Business Continuity:** Most participants emphasized the need for a business continuity plan, noting that the constantly changing environment requires frequent risk re-evaluations. Additionally, testing and training are crucial for validating a plan's effectiveness. Two participants mentioned recent resilience tests simulating large-scale attacks to assess the crisis management team's response and process robustness, with one test conducted in coordination with ENISA. Four participants stated they were using the ISO/IEC 27000 international standard, while one mentioned employing the ISA/IEC 62433 standard within their organization.

**User Awareness Training:** All participants reported using user awareness training. A common strategy involves targeted phishing campaigns, where a user's failure to detect a phishing email leads to mandatory training for the user. Participants also discussed other training methods designed to raise awareness of cybersecurity threats, often tailored to specific organizational roles. Various training formats include group seminars, individual conversations, and e-learning platforms. A common challenge is that not all users are comfortable with technology, and cybersecurity can be perceived as dull, making it difficult to motivate staff to learn best practices. One participant mentioned that gamification techniques helped engage users in cybersecurity training. Another emphasized the importance of explaining the reasons behind certain restrictions and processes to users, noting that transparent and open communication enhances acceptance of cybersecurity practices within the organization.

**Managing External Service Providers:** Organizations face significant challenges managing cybersecurity risks from third-party service providers. The primary approach is written contracts, including data protection clauses and sometimes detailed processes to ensure cyber resilience. A major challenge is the

limited control over external providers' security practices. Three participants implemented screening or auditing processes to mitigate risks, though these can be time-consuming. One participant noted that while robust contracts are essential, they can be challenging to execute due to disagreements over responsibilities, prolonging negotiations, and increasing costs.

## 5 DISCUSSION

This section discusses the findings from six themes presented in the previous section and relates the findings to previous research. The first theme, the regulatory challenges and compliance, focused on the complex regulatory landscape for CI operators in Luxembourg due to varying interpretations and compliance requirements of European Directives like NIS1 and NIS2 across member states. Participants noted that some regulatory bodies excel in specific domains but not necessarily in IT, leading to inconsistent compliance and confusion. This issue aligns with previous research by Rawindaran et al., suggesting sector-specific support from government entities for cybersecurity strategies (Rawindaran et al., 2023). The globalization of IT infrastructure, including cloud solutions, further complicates compliance, exposing organizations to varied requirements that can conflict with European and foreign regulations. This necessitates international agreements to harmonize regulations.

The second theme, industry landscape and adaptation, emphasized the constantly evolving cyber threat landscape, posing significant challenges to CI operators. Increased sophistication of attacks and interconnected systems require continuous vigilance and adaptation. This underscores the need for costly cybersecurity measures to ensure the resilience of essential services. Participants highlighted the difficulty in aligning cybersecurity initiatives with business priorities and gaining decision-makers support, emphasizing the need for enhanced cybersecurity awareness within organizations and society. Government initiatives and campaigns can also help increase public awareness and build a cyber-resilient society. Chaudhary et al. previously highlighted the challenges in gaining decision-makers support for cybersecurity initiatives (Chaudhary et al., 2023). Moreover, Luxembourg's high cost of living has made talent acquisition difficult despite traditionally high salaries attracting global talent. Participants noted the struggle to find cybersecurity experts due to unmatched salary expectations.

The third theme, resource management, relates to the challenges in managing internal resources. Lim-



ited budgets and operational constraints necessitate careful resource allocation, balancing investment in advanced security technologies with maintaining operational efficiency. Human resource management is also critical, with varying degrees of CISO detachment from daily IT operations. Larger organizations favor more detachment, while smaller ones face limited personnel and operational demands. These findings correlate with previous research on resource constraints and the need for strategic allocation (Hussain et al., 2020; Javaid et al., 2023; Chaudhary et al., 2023).

The fourth theme, external collaboration and support, concerns collaboration with national cybersecurity agencies and other entities. Collaboration is vital but varied, with overlapping responsibilities between agencies like CIRCL and GovCert creating confusion and hindering efforts. Different reporting methods imposed by agencies lead to inefficiencies, highlighting the need for harmonization. Previous research supports these findings, noting that new regulations have increased administrative work (Gonçalo et al., 2019). Overall, improved communication from national security agencies is needed to support CI operators effectively.

The fifth theme addresses the challenges in managing IT infrastructure. Effective management is essential for detecting anomalies and safeguarding critical systems, but the complexity of CI IT environments and resource constraints pose significant challenges. Customized monitoring solutions and the need for specialized expertise often lead to outsourcing, increasing costs. Centralizing monitoring operations in the public sector could reduce the resource burden on individual organizations and improve efficiency.

The last theme, operational governance, is the evolving threat landscape, necessitating regular re-evaluation of risks and resilience strategies, including implementing business continuity plans. Participants strive to adhere to cybersecurity standards like ISO/IEC 27000 or ISA/IEC 62433. User awareness training is also crucial, with tailored programs and transparent communication enhancing engagement and understanding. While previous studies suggested government-provided training for the general population, such initiatives are already in place in Luxembourg. Participants emphasized explaining new decisions and processes to all end-users to increase awareness and satisfaction, fostering a healthy cybersecurity culture. Managing external service providers through contracts and agreements is common, but ensuring alignment with organizational standards remains challenging. Screening and auditing processes could mitigate risks but can also be

resource-intensive.

This analysis highlights the multifaceted challenges CI operators face in Luxembourg and the need for strategic approaches to enhance cybersecurity resilience.

## 6 CONCLUSIONS

Revisiting the research question *“What are the challenges associated with implementing cybersecurity measures in critical infrastructure, and what potential solutions exist to address them?”*, we identified six distinct challenges. Addressing these requires a multifaceted approach, including regulation harmonization, talent development, resource optimization, streamlined reporting methods, and a continuous commitment to enhancing cybersecurity practices.

A short- to medium-term solution involves reducing the impact of new regulations on already overstretched CI operators. This can be achieved by streamlining reporting to a single method used by all regulators and increasing support from national cybersecurity agencies. Redefining the precise scope of activities for these agencies and improving their ability to assist CI operators would enhance collaboration, reduce resource strain, and increase efficiency. Additionally, recognizing that organizations and regulatory agencies alone cannot solve national cyber-resilience. Therefore, government initiatives must address labor market challenges and increase public cybersecurity awareness.

At the European and international levels, regulators should gather feedback on regulatory challenges faced by CI operators to revise and adapt legislation as necessary. Continued efforts to harmonize regulations across nations will simplify operational activities for CI operators.

One can argue that the interviewee’s statements are “common sense.” However, they provide a localized and context-specific understanding of Luxembourg’s critical infrastructure cybersecurity challenges. While certain observations, such as the importance of regulatory compliance or the need for adequate resources, may seem self-evident, they are still relevant in Luxembourg’s unique regulatory and organizational landscape. The insights from the interviews help illustrate how general cybersecurity principles manifest in real-world scenarios, particularly in smaller nations with limited resources and complex international regulatory demands. By contextualizing “common sense” observations within the specific challenges faced by CISOs in Luxembourg, the study bridges the gap between theoretical knowledge and

practical implementation, offering valuable lessons for policymakers and CI operators, particularly in similar-sized nations or regions navigating similar cybersecurity landscapes.

The study's validity depends on accurate data collection, but the subjective nature of thematic analysis introduces the possibility of interpretation bias. Despite using techniques like member checking, the findings may be influenced by participants' articulation and the researcher's interpretation. Participants received copies of their transcripts for validation.

Interpretation subjectivity challenges qualitative research reliability. Efforts were made to ensure that the inherent subjectivity of qualitative analysis hinders accurate translations but perfect consistency. The study's findings, limited by sample size and participant demographics, may not be broadly applicable. Replicating interview conditions precisely is difficult due to the dynamic nature of human interactions. Extending results to diverse populations should be done cautiously, recognizing these limitations for future research.

Future research could expand into more detailed analysis by studying an entire strategy implementation process within a selected organization, identifying internal challenges more precisely through interviews or questionnaires at various hierarchical levels. Another valuable area of research would be to investigate national cybersecurity agencies in more detail to identify national coordination problems. Replicating similar research in other European countries could reveal common challenges and potentially offer new solutions for foreign organizations or governments to implement.

## REFERENCES

- 115th Congress of the United States (2018). Clarifying Lawful Overseas Use of Data (CLOUD) Act. Public Law No: 115-141. <https://www.congress.gov/bill/115th-congress/house-bill/4943>.
- Ait Maalem Lahcen, R., Caulkins, B., Mohapatra, R., and Kumar, M. (2020). Review and insight on the behavioural aspects of cybersecurity. *Cybersecurity*, 3(10).
- Alessandro, A., Fabio, N., and Giulia, P. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering*, 149:1–18.
- Amin, H., Amin, R., Stefano, G., Mohsen, A., Riccardo, T., Avi, O., and Katherine, B. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, 146(5).
- Antova, G. (2020). Wie können wir die digitalisierung der kritischen infrastrukturen sicher gestalten? <https://digitaleweltmagazin.de/wie-koennen-wir-die-digitalisierung-der-kritischen-infrastrukturen-sicher-gestalten/>. Accessed: 2024-04-12.
- Beil, L. (2023). Kritische infrastruktur in gefahr? <https://www.tagesschau.de/wissen/technologie/infrastruktur-cybersicherheit-cyberattacken-101.html>. Accessed: 2024-04-12.
- Bundesamt für Sicherheit in der Informationstechnik (2022). Die lage der it-sicherheit in deutschland 2022. Technical report, Bundesamt für Sicherheit in der Informationstechnik, Berlin.
- CERT governmental Luxembourg (2023). Govcert. <https://www.govcert.lu/en/>. Accessed: 2023-05-11.
- Chaudhary, S., Gkioulos, V., and Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, 50.
- Chowdhury, N. and Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40.
- Creos (2022). Le Groupe Encevo victime d'une cyberattaque. <https://www.creos-net.lu/actualites/actualites/article/le-groupe-encevo-victime-dune-cyberattaque.html>. Accessed: 2023-05-28.
- Cybersecurity Luxembourg (2020). National cybersecurity strategy iv (ncss iv). <https://www.cybersecurity.lu/strategy>. Accessed: 2023-05-11.
- Denscombe, M. (2021). *The Good Research Guide*. Open University Press, New York.
- European Commission (2022). Proposal for a regulation of the european parliament and of the council on horizontal cybersecurity requirements for products with digital elements (cyber resilience act). [https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF). Accessed: 2024-04-12.
- European Parliament and the Council of the European Union (2016). Directive concerning measures for a high common level of security of network and information systems across the union. Official Journal of the European Union. Directive (EU) 2016/1148.
- European Parliament and the Council of the European Union (2019). Regulation (eu) 2019/881 of the european parliament and of the council of 17 april 2019 on enisa (the european union agency for cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (eu) no 526/2013 (cybersecurity act). <https://eur-lex.europa.eu/eli/reg/2019/881/oj>. Accessed: 2024-04-12.
- European Parliament and the Council of the European Union (2022). Directive on measures for a high common level of cybersecurity across the union, repealing directive (eu) 2016/1148. Official Journal of the European Union. Directive (EU) 2022/2555.
- Gonçalo, A. T., Miguel, M. d. S., and Ruben, P. (2019). The critical success factors of gdpr implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, 21(4).
- Grigalashvili, V. (2022). The essence of critical infrastructure in the european union, nato and g7 countries.

- International Journal of Innovative Technologies in Economy*, (1(37)).
- Gurpreet, D., Smith, K., and Hedström, K. (2019). *Ensuring Core Competencies for Cybersecurity Specialists*, volume 7, pages 121–133.
- Haut-Commissariat à la protection nationale (2023). Agence nationale de la sécurité des systèmes d'information (anssi). <https://hcupn.gouvernement.lu/fr/service/attributions/missions-nationales/anssi.html>. Accessed: 2023-05-13.
- Hussain, A., Mohamed, A., and Razali, S. (2020). A review on cybersecurity: Challenges & emerging threats. In *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, pages 1–7.
- IBM Security (2023). *Ibm security x-force threat intelligence index 2023*. Technical report, IBM Security.
- Javaid, M., Haleem, A., Singh, R. P., and Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, page 100016.
- Johnson, M. E. and Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, 5(3):16–24.
- Kampourakis, V., Gkioulos, V., and Katsikas, S. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. *Computers & Security*, 126:103383.
- Kollwelter (2022). Cyberattack op 25 wandrieder vunder firma soler. <https://www.rtl.lu/news/national/a/1876775.html>. Accessed: 2023-05-28.
- Kshetri, N. (2015). Recent cybersecurity policy initiatives: Challenges and implications. *Computer*, 48(7):64–69.
- Laegreid, P., Randma-Liiv, T., Rykkja, L. H., and Sarapuu, K. (2015). Emerging coordination practices of european central governments. *International Review of Administrative Sciences*, 81(2):346–351.
- Luxembourg House of Cybersecurity (2023). Luxembourg house of cybersecurity. <https://lhc.lu/#PageHomeAboutLHC>. Accessed: 2023-05-11.
- Makrakis, G. M., Koliass, C., Kambourakis, G., Rieger, C., and Benjamin, J. (2021). Industrial and critical infrastructure security: Technical analysis of real-life security incidents. *IEEE Access*, 9:165295–165325.
- Maynard, S. B., Onibere, M., and Ahmad, A. (2018). Defining the strategic role of the chief information security officer. *Pacific Asia Journal of the Association for Information Systems*.
- Peters, B. G. (2018). The challenge of policy coordination. *Policy Design and Practice*, 1(1):1–11.
- Rawindaran, N., Jayal, A., Prakash, E., and Hewage, C. (2023). Perspective of small and medium enterprise and their relationship with government in overcoming cybersecurity challenges and barriers in wales. *International Journal of Information Management Data Insights*, 3(2).
- Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., and Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, 23(8).
- Serpanos, D. and Komminos, T. (2022). The cyberwarfare in ukraine. *Computer*, 55(7):88–91.
- Sohrabi Safa, N., Sookhak, M., Von Solms, R., Furnell, S., Abdul Ghani, N., and Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53:65–78.
- Stergiopoulos, G., Gritzalis, D. A., and Limnaios, E. (2020). Cyber-attacks on the oil&gas sector: A survey on incident assessment and attack patterns. *IEEE Access*.
- Teixeira, G. A., da Silva, M. M., and Pereira, R. (2019). The critical success factors of gdpr implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, pages 402–418.
- Tessian (2020). The psychology of human error. <https://www.scribd.com/document/621516208/Tessian-Research-The-Psychology-of-Human-Error>. Presentation.
- Verizon (2022). 2022 data breach. <https://www.verizon.com/business/resources/reports/dbir/>. Accessed: 2023-03-02.
- World Economic Forum (2022). The global risks report 2022. Technical report, World Economic Forum.

## APPENDIX

Table 1.

Question	Motivation	Hypothesis
<b>Introduction</b>		
Tell me about yourself, what is your background? How many years of experience do you have in the industry? What are your tasks and mission in your current role?	Introduction question to warm-up and get some more detailed background information about the participants.	All participants have more than 10 years of experience.
<b>Organisational aspects</b>		
How many people work in IT & in what roles? Do you have enough personnel? If not, what would the ideal distribution look like?	This question aims to address the 12 profiles presented in the ECSF framework, for which different skills synergies and interdependencies are presented. These questions aim to see how organizations are set up compared to the framework's examples.	Given the rapidly changing environment, organizations have difficulties filling positions and organizing themselves adequately.
In your opinion, what are the most significant organisational challenges that organizations face when it comes to implementing cybersecurity policies?	This question sets out to investigate where inner hurdles are faced and what participants regard as the most challenging aspect.	Many companies lack financial and human resources to implement policies properly as demonstrated in relevant literature.
How do you navigate those challenges within your organization?	Gather the most significant aspects for a successful implementation from a CISO's point of view and see if the same aspects are mentioned between participants.	Given that the NIS2 directive has a larger scope than NIS1, it is assumed that already previously affected organizations have a more mature approach to implementing policies.
How do you keep informed? What resources do you use?	Find out what communication channels and networks exist to communicate on these issues and see how many and what type of sources provide insights to professionals.	National cybersecurity entities inform organizations on a regular basis and help keep track of ongoing changes and contextualize events.
How do you mitigate human error within your organization? Are there specific policies, trainings, access management rules, etc. you can talk about?	Given that human error plays such an important part in most incidents, this question aims to address what measures organizations specifically put in place to mitigate it and to whom they apply within the organization.	The assumption is that most organizations offer cybersecurity awareness training to all employees to some extent.
<b>Regulatory aspects</b>		
What regulations and standards are currently implemented or in the process of being implemented?	NIS1 has already been implemented, but since NIS2 is currently in the national implementation phase, this question addresses which legislations are primarily being focused on and if they overlap with the literature review findings.	Organizations are aware of the upcoming NIS2 directive and are already discussing implementation strategies for the upcoming NIS2 or other legislation.
What are your thoughts on the current state of cybersecurity regulation in Luxembourg?	Examine how cybersecurity professionals evaluate the current state of legislations and regulations and how it impacts their work.	Some regulations might overlap and create confusion, and some regulations might be difficult to implement.
How do you ensure that third-party vendors and partners comply with relevant cybersecurity regulations when working with your organization?	GDPR, NIS2, and other regulations all require data confidentiality, integrity, and availability. This question explores how organizations handle third-party involvement.	Choosing partners who have ISO certifications, extended background checks, and NDAs signed depending on operations.
What changes would you like to see in regulations? What do you expect in the future?	Bring forward some key changes that would benefit CISOs' daily work and gain insights into how the industry might change in the future (new challenges, new possibilities).	Possibly more support from government entities in decision-making and strategy implementation.