ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA
CESENA CAMPUS

Department of Computer Science and Engineering - DISI
Master's Degree in Digital Transformation Management
LM-91 - Methods and Techniques for the Information Society

On the CISO and the necessity of this role in a data-driven era

Graduation thesis in
Cybersecurity

Supervisor
Gabriele D'Angelo

Co-Supervisor
Dott. Alessandro Leone

Defended by
Myriam Pollaccia

V Session
Class of 2023

Abstract

As we are currently living in the era of digital transformation, the security of our data is increasingly becoming a necessity and not just a small function of a business or a government.

The role of the Chief Information Security Officer might be the key to face this challenge in the proper way and with the right awareness.

This thesis aims to understand the current state of the art of the role by exploring literature on a CISO's right competencies, the relevant standards and certifications they should refer to, the right position for them in the organizational chart and the specific responsibilities they should face.

Would it be possible to find a universal standard for the role?

A mio nonno Carlo,
che per primo ha saputo cogliere
la mia curiosità e il mio spirito:
coltivandoli ha, inconsapevolmente,
dato forma al mio futuro.

Contents

Introduction

A **Chief Information Security Officer** (CISO) is a professional responsible for the information technology security of an organization.
This role, which may be assumed immediately to be a technical one, is, in fact, the clear representation that **cybersecurity is a multidisciplinary topic**. Cybersecurity is a wide discipline that encompasses many aspects that go beyond technology, therefore the interesting thing about this role is that it is difficult to exactly define it because it stands between technical and managerial expertise.
It is a relatively new role, and literature on it, as we will see in the following chapters, is scarce.

During my internship work with Bernoni Grant Thornton, I directly observed the work of a CISO, in order to understand the key areas to investigate. This helped to form the structure and chapters of this thesis: **Competencies**, **Standards**, **Hierarchy** and **Duties**.

At the end of my internship, I had the possibility of interviewing CISOs from different industries to understand the current state of the art, grasp common best practices and try to outline the role as much as possible by investigating the four main areas mentioned above.
The respondents, throughout the entire thesis, will be named by their industry: *Advisory*, *Wholesale*, *Services*, *Retail* and *Healthcare*.

Below I'll summarise the questionnaire that served as a guideline for the interviews, by listing the main questions that permitted to structure the thesis:

- *What are the main competencies a CISO must have?*
- *Do you think a CISO is a technical role or a managerial role?*
- *How is the company's organizational structure composed?*
- *Who are the actors involved in the IT infrastructure?*

- *In which hierarchical position is the CISO?*
- *Where do you think the CISO should be in the hierarchical structure?*
- *Have the CISO's tasks been formally defined in a policy or procedure?*
- *Which do you think are the most important standards that a CISO must know?*
- *Which certifications would you recommend to a CISO?*
- *How is the top management involved in cybersecurity decisions, activities and possible incidents?*
- *How do the management and the CISO communicate?*
- *What are the main activities of the CISO?*
- *Is the CISO in charge of developing awareness training in the company?*

The questionnaire was flexible, and I adapted the questions to the specific context of the organization of the CISO I was interviewing and to how the conversation flowed.

We are living in a new era where technology is not only an instrument of help for companies anymore, but a crucial aspect of the organization, so firms need CISO expertise. Firms rely on Big Data, personal data is a concern, and security must not be an option anymore, but a requirement in the era of Digital Transformation.

To understand the issue, I will briefly reference some statistics exposed by Cobalt (Fox, 2023) about the future trends in cybersecurity:

- Cybercrime damage costs are estimated to grow by 15% per year and hit 10 trillion dollars annually by 2025, worldwide.
- 75% of security professionals observed an increase in cybercrime.
- 45% of insurance experts state that cyber incidents are more feared than energy concerns.
- 53% of organizations are implementing cybersecurity in strategic business initiatives.

- 44% of business leaders recognise the importance of CISOs.
- In the last four years there has been an increase of 239% in cybercrimes that targeted healthcare.

The statistics mentioned above reference specific sources that can be directly accessed from the Cobalt article I am referring to.

The purpose of this thesis is not only to understand the current state of the art of this role but also to answer a question that I asked myself at the start of this project: *"Can the role be standardised?"*

Chapter 1

Competencies

To effectively succeed in their role, CISOs must possess a comprehensive set of competencies, spacing from **technical knowledge** to **managerial knowledge** and soft skills. What are these competencies, the degree to which a CISO should possess them, and the **balance** between technical and managerial skills is the object of this chapter.
Specifically, it was interesting to understand if the role of the CISO should be considered as a very technical one (so a CISO should be a technician with deep IT and cybersecurity knowledge) or as a managerial one, with CISOs being first and foremost proficient in business issues, with the role of being a bridge between top management and the team of IT and cybersecurity competent technicians that accompany them.

During the interviews held during the internship, one of the questions was "*Is the CISO a manager or a technician?*"
Advisory, *Wholesale* and *Services* answered that the role should be managerial, accompanied by a team of technicians; *Retail* and *Healthcare* answered that, instead, it should be technical.

To the question "*Which competencies do you think are essential to a CISO?*" all of them answered that being proficient in certification requirements (or actually being certified) is essential, except for *Wholesale*, who actually thought certifications were not essential, at least not as the capability of building awareness inside the company and the ability to build an organizational culture that had information security as its foundation.

In his research study, Cotton (2022) wanted to find the specific competencies that

hiring managers should look for in a CISO to consider them qualified.
Specifically, the research aimed to find the best practices and expertise for CISOs, considering "an examination of available CISO literature indicated **no consensus** about the experience level and qualifications required for a CISO" (p. 17).

At the end of the research, after interviewing 10 CIOs (*Chief Information Officers*) who hired CISOs in their company, and after reviewing the literature (similar to the work done for this dissertation), four principal themes came out:

- **Theme 1: Hard skill credentials are a must to serve successfully as a CISO.**

  The research highlighted a series of hard skills, such as:

  > "possessing the wisdom to **discern** the possibility of a risk occurring and the potential damage the risk could cause or is the risk of insignificance to where if the risk occurred, the organization is willing to accept the potential damage the risk could cause [...] the ability to **connect cybersecurity to the organization's mission**, knowledge of cloud infrastructure and services, program management, incident handling, the knowledge and understanding of cybersecurity policies and governance, and knowledge of networks architecture, security, operations, and infrastructure" (p. 97-98).

- **Theme 2: Soft skills are essential to protecting organizational data and networks.**

  The soft skills highlighted included:

  > "the ability to coordinate with other security agencies [...] communicate effectively [...] understand business operations [...] understand what elements require security protection [...] manage resources, budget, time, and people [...] think critically [...] problem-solving [...] the ability to translate technical to non-technical language" (p. 99).

- **Theme 3: CISOs are seasoned professionals with several years of cybersecurity experience.**

  Members of the research group considered as relevant years of experience between 10 to 15 years. No participant considered less than 5 years of experience to be sufficient to apply for this role and successfully do a proper job.

- **Theme 4: Specific certifications are essential for a successful CISO.**

  The majority of the research group members stated that certifications are an indicator of the CISO possessing the skills required to perform their job. Specifically, the certifications indicated included CASP (*CompTIA Advanced Security Practitioner*) and CISSP (*Certified Information Systems Security Professional*).

This specific research served as a base for the following paragraphs and served as a sort of summary of the different skills CISOs should have.

Technical expertise

The main foundation of the set of technical expertise is, clearly, a strong understanding of cybersecurity principles and the security domain.
For this matter, current cybersecurity standards give out a guideline.

An important one comes from the CISSP certification, which encompasses eight domains:

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

The *CISSP Exam Outline* provides a further and more in-depth guideline of the requirements, but the scope of this dissertation is an overview of the state of the art of the role of the CISO and not a cybersecurity procedures tutorial, therefore I consider more appropriate to only develop these points briefly.

Analysing point by point will allow a reader who does not have background knowledge of cybersecurity to get a better understanding of the technical expertise a CISO could need to have and will also permit them to grasp the domain of application of this *C-Suite* role that is being analysed now.
With “C-Suite” I am referring to the company’s top management positions.
The term groups together all the Chiefs, so, for instance, the CIO, the CEO (*Chief Executive Officer*), the CFO (*Chief Financial Officer*), or, of course, the CISO.

I will now proceed to expand on the points listed above:

Security and Risk Management:
Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (Office of the Federal Register, National Archives and Records Administration, 2017), states that:

“Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents” (p. 22391).

The process of recognizing threats that the business could potentially encounter, analysing and correctly classifying them by understanding their likelihood of happening and impacting the systems and implementing correct mitigation strategies by appropriately balancing them and continuously assessing the situation is one of the main pillars of the technical aspects the CISO must encounter.

Asset Security:
Asset security refers to the process of managing an organization’s assets by continuously monitoring them and acknowledging potential security threats they might be affected by. Assets include traditional devices such as computers, servers, and IoT devices, as well as databases and domains since each of these assets could be a door for a breach in the system.
Being aware of the characteristics of different types of assets and their potential threats, as well as recovery practices like patches, is an important skill for an information security expert. *NIST Special Publication 1800-5* (NIST, 2018) on IT Asset Management offers an important guideline for asset management.
This won’t be discussed in detail for the same reasons expressed before.

Security Architecture and Engineering:

"Security architecture is the design and organization of the components, processes, services, and controls appropriate to reduce the security risks associated with a system to an acceptable level. Security engineering is the implementation of that design. The goal of both security architecture and security engineering is primarily to protect the confidentiality, integrity, and availability of the systems or business in question." (Warsinkse, 2019, p. 213)

This is a phase that normally follows the risk assessment phase.
As stated by Warsinkse, the principles for engineering a system to reduce risk have been proposed for years in many ways, with the leading being ISO/IEC (*International Standardization Organization / International Electrotechnical Commission*) standards (discussed in detail in the next chapter) and *Saltzer and Schroeder's Principles.*

Saltzer and Schroeder (1975) set out eight examples of design principles for security systems.
Since these design principles are essential in cybersecurity, they will be explained briefly for the same purpose discussed before:

- **Economy of Mechanism**: a simple system results in fewer errors and therefore fewer possible breaches. It is better to focus on simpler, well-tested mechanisms than complicated ones that could lead to complexities.

- **Fail Safe Defaults**: the default access is lack of access, so it is not based on exclusion but on permission. If and only if certain conditions are verified, access is granted. A design that grants access as default, in case of a mistake will allow access even if the conditions are not met.

- **Complete Mediation**: every access to every object must be checked for authority.

- **Open Design**: the protection mechanism can't rely on the secrecy of its design and the presumption that attackers won't know about it. This also allows for the design to be reviewed properly over time.

- **Separation of Privilege**: compartmentalizing access and allowing only the necessary permissions leads to fewer potential breaches. No user should be able to access the entire system.

- **Least Privilege**: every user of the system should have the least set of access privileges necessary for its purpose. It is clearly strongly correlated to the principle enounced before.

- **Least Common Mechanism**: the number of mechanisms common to more than one user should be minimized, reducing the attack surface.

- **Psychological Acceptability**: protection mechanisms must be humanly acceptable and aligned to user expectations in order to actually be implemented correctly and expect users to be compliant with it.

Communication and Network Security:

“Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment” (Fruhlinger, 2018).

CISOs might be responsible for implementing network security measures such as VPNs (*Virtual Private Networks*), intrusion detection and firewalls.

Identity and Access Management:
IAM (*Identity and Access Management*) is a comprehensive approach to user identity management and asset access control that encompasses various processes, policies and techniques, including the ability to control physical and logical access to assets and manage authorization mechanisms.

Security Assessment and Testing:
Security Assessment and Testing is a component of information security risk management which aims to identify current vulnerabilities by testing and developing corrective measures.

Software Development Security:
Software Development Security refers to the process of ensuring security from the development stage of a software, to reduce the risk of vulnerabilities in the later stages of the operations. CISOs might be held accountable for assuring security in *DevOps* contexts.
To be clear, ”DevOps” is a term that combines Software Development and Operations. It is a methodology for the development of software.

Managerial expertise

CISOs have the hard work of translating a crucial problem such as cybersecurity into a business need, therefore they must possess good interpersonal skills, to enable them to effectively communicate (and possibly convince others of the importance of their subject and the need for investment in it) to clients and managers on top levels. The need is to appropriately translate and be able to explain technical concepts to a variety of audiences, with the purpose of building a bridge over the gap between cybersecurity and the business domain.

Possessing financial acumen in order to convince top management that it is a good idea to spend money on security issues since it can be difficult to demonstrate a Return On Investment in this case, is another good skill of a professional security officer, as well as leadership, essential for decision-making, creating awareness in the company and gaining consensus when explaining the security approaches implemented.

Smit et al. (2021), in their research study, aimed at gaining more information about the soft skills demanded by a CISO, since those are not studied in depth compared to other roles in different industries. One of the aspects they explored was information security awareness and its importance for the information security program. Weishäupl et al. (2018), cited by Smit et al., state:

> "Awareness is a complex issue that has not yet been discovered entirely. Influencing the behavior of 200,000 employees is a challenging task. In addition, **IT security tends to be managed by technicians who are more knowledgeable in technology rather than in human behavior**" (p. 812).

Policies are essential to build information security awareness because they get people to better comply with security approaches and rules, which is supported by the answers of *Advisory*, *Wholesale* and *Services* during the interviews.

At the end of their research, which combined literature and results from the Delphi survey they conducted, some soft skills were highlighted.
The following soft skills identified by the authors are the ones that positively influence the CISO leadership role (in order of importance): Communication, Leadership, Interpersonal skills, Professionalism, Integrity, Work ethics, Responsibility, Teamwork skills, Positive attitude, Flexibility, Courtesy.
The research does not go more in-depth and in the end, it is suggested to do more research on the way the CISOs develop these skills.

Anderson (2014), exam developer and reviewer of the CISSP certification, defines CISOs as hybrid professionals, defined by Morello (2008) as “people with varied experience, professional versatility, multidiscipline knowledge and technology understanding”. In Anderson’s opinion, CISOs must possess a set of qualities diverse enough to be adaptable to different contexts and circumstances, which is essential for a dynamic environment like the digital world.

She then proceeds to list a series of managerial skills and soft skills that are necessary for CISOs to achieve this versatility, including:

- **Being open to the ideas of others**: CISOs need to collaborate with different professionals who can be better proficient in solving certain issues. Building and maintaining a diverse network is essential to be a better problem solver.
- **Being proficient in different domains**: With proficiency, Anderson does not mean having full knowledge in every possible subject but maintaining a good knowledge by collaborating with different domain practitioners, reinforcing what was stated before.
- **Lateral thinking**: Being able to develop innovative strategies to face issues and see things from different perspectives. This skill is also useful considering the digital world is constantly evolving with new technological possibilities and consequent transformation inside society.
- **Understanding business needs**: CISOs need a holistic view of the organization, in order to “achieve a balance between performance efficiency and security” (p. 315). Information security must always be applied to the existing business culture and to the business objectives.
- **Acknowledge budgeting**: CISOs need to have the “ability to present a solid business justification to a budget committee and receive funding” (p. 315), and this resonates even more if we take into consideration that not every CISO has procurement. Three out of the five CISOs interviewed during the internship actually had no procurement possibilities and had to depend on somebody else for budgeting. CISOs should have the capability of exploring different budgeting strategies for implementing security.
- **Being a strong leader**: Leadership is learnt like any other skill, and it is essential for the role of the CISO. Like other requirements, it should be coherent with the context in which the CISO is operating and “must take into

consideration the leader, organizational maturity, required tasks, and other situational factors" (p. 319). Good leaders also ensure good teamwork, by making sure there is appropriate communication between staff members and the CISO and inside the team as well.

- **Being comfortable with compromise**: Security solutions and approaches might not be the best globally but be the best locally considering the context and situation, since they have to be implemented in processes that are already established and have to be accepted by people who might be reluctant to follow them. Being balanced and accepting compromise is also essential for evaluating risk correctly, avoiding the implementation of security approaches that are too harsh for areas that might need lighter strategies, being low risk. This hybrid approach should be adopted as a continuous strategy for information security management.

Finding the right balance

A question that arose during the research was about how these diverse types of knowledge should be balanced and what is more important.
Certainly, different industries have unique needs and therefore the balance could vary based on that, and this is supported by the different answers provided during the interviews. However, it is clear that, in order to truly understand the various issues of information security, CISOs must have a minimum of technical knowledge even if they do not come from a technical background.

Kayworth and Whitten (2012) interviewed information security executives from 11 organizations of various industries (similar to the work done for this dissertation). Based on Siponen (2005), cited by the two authors, "Historically, companies have followed a technically focused information security strategy that emphasizes the primary role of technology in designing effective security solutions"(p. 163) and "The lack of integration between the security group and the business may result in security policies and budgets not reflecting the needs of the business"(p. 164).
The view that comes from their research is that the emphasis must be both on technology and socio-organizational context, making the information security officers competent on both sides.

They identified three fundamental issues in the information security strategy that are positively affected by a balanced approach:

- **Balancing Information Security and Business Needs**: More conservative approaches to security might hinder business operations, so it is necessary for every security decision to be business-driven. They also argue that risk management is not a responsibility of the security officer but a responsibility of the business. However, they also noted that “an effective security strategy is not “one-size fits all”; rather, it takes into account the varying risk factors that may be associated with different industries, product lines, or geographic locations” (p. 165).

- **Ensuring Compliance**: Security approaches must ensure compliance with legislation (data privacy regulations, financial regulations, etc.)
- **Maintaining Cultural Fit**: It is essential to find approaches that match organizational culture and values, and that do not interfere too much with regular operations, in order to avoid cultural conflict and ensure compliance by every member of the firm. The same point was suggested by one of the CISOs interviewed during the internship.

Death (2019), at the end of a description of essential skills a CISO must have, says “the specific success factors may also be determined by the needs of their respective organizations and the prevailing security culture within them” and that “these skills are necessary to effectively lead the integration of technology with the business and mission of the organization, and aligning the security program with the needs, targets and priorities of the people within” (p. 13).

It seems that **a definite answer is difficult to find** and that the right balance is truly a matter of the organization’s unique needs and the context in which the CISO is operating.

A CISO who is first and foremost a manager might be able to better convey the need for cybersecurity inside the company and create the necessary awareness; they are financially aware of the risk/cost decisions and are good communicators, but they could lack the knowledge necessary to properly understand the information security need and properly communicate with the technical team, and vice versa. A grouping could be done, for instance, on industry.

The balance is supported by most of the sources found during the research, and even authors of articles online with titles that suggest a strict position, like the one from Espinosa (n.d.), in the end, suggest a balanced vision of the role.
Where the balance is shifted depends on the specific needs of the firm.

Chapter 2

Standards

One of the themes identified by the research conducted by Cotton was that "Specific certifications are essential for a successful CISO." This principle, as said in the previous chapter, is reinforced by the answers of four out of the five CISOs interviewed, who stated that standards and certifications are important to support the job.

There is a plethora of different information security standards, frameworks, and certifications. This chapter aims to understand their effective relevance and whether it is necessary for a CISO to own a certification.

The ones named by the security officers interviewed are various. Grouping them by typology, they included:

Standards:

- ISO/IEC 27001 "*Information security, cybersecurity and privacy protection – Information security management systems – Requirements*"

- ISO 22301 "*Security and resilience – Business continuity management systems – Requirements*"

- ISO 9001 "*Quality management systems – Requirements*"

- SSAE 18 (*Statement on Standards for Attestation Engagements*) by AICPA (*American Institute of Certified Public Accountants*), developed from ISAE 3402 (*International Standard on Assurance Engagements*)

Frameworks:

- NIST (*National Institute of Standards and Technology*) Cybersecurity Framework
- COBIT (*Control Objectives for Information and related Technology*) by ISACA (*Information Systems Audit and Control Association*)
- OWASP (*Open Web Application Security Project*) Cyber Defense Framework
- ITIL (*Information Technology Infrastructure Library*)

Certifications:

- CISM (*Certified Information Security Manager*) by ISACA
- CISA (*Certified Information Systems Auditor*) by ISACA
- CRISC (*Certified in Risk and Information Systems Control*) by ISACA
- C—CISO (*Certified Information Security Officer*) by EC-Council
- CISSP (*Certified Information Systems Security Professional*) by ISC2 (*International Information System Security Certification Consortium*)
- COMIT (*Certification in Outsourcing Management for IT*)

Standards are documents that determine specific procedures for ensuring the consistency, reliability and integrity of the organization's services, assets, products, and systems. This transforms information security into a quantifiable set of information, which can be measured and, therefore, periodically monitored.

Frameworks are more general and flexible guidelines covering a variety of domains, whose purpose is to provide some best practices to reduce the risk of cyber threats, making them applicable to various contexts and needs.

Certifications are obtained after passing tests, and therefore formally demonstrate the proficiency of professionals in information security domains.

As for other concepts inside this dissertation, the three categories won't be discussed any further.

This chapter aims to explore the reasoning behind some of the suggestions, and the ways information security officers can benefit from the following.
Specifically, I will discuss ISO/IEC 27001:2022 and the NIST Cybersecurity Framework, which are a gold standard in information security guidance, and some of the most mentioned certifications, by the respondents of the interviews and the most seen during my bibliographic research.

ISO/IEC 27001

ISO/IEC 27001 is an international standard for information security management, belonging to the ISO/IEC 27000 family of standards on the creation and administration of ISMSs (*Information Security Management Systems*).
With a global growth rate of 20% (Mohan, 2023), and over 70000 certificates reported in 150 countries (according to ISO's website) it is now the reference standard for organizations from different industries, from agriculture to manufacturing, since it proves to customers that they are effectively able to protect their information with proper policies and procedures and that the compliance to the standard is regularly supervised by the accreditation bodies.
It consists of requirements for the creation and administration of an ISMS that is a proper tool for cyber-resilience and enterprise risk management, by promoting a 365° approach to security.

The structure of the standard, as Kosutic (2022) describes in his article for Advisera (the standard itself is proprietary content and therefore it is not possible to directly consult it for free), consists of two major components.

The first component is a series of clauses, following the PDCA (*Plan-Do-Check-Act*) model:

- **Plan**: Covering clauses from 4 to 7, refers to the set of steps to define and achieve an objective.

- **Do**: Covering clause 8, refers to the action on what is planned.

- **Check**: Covering clause 9, refers to the set of steps to identify any gaps between what was planned and what has been achieved.

- **Act**: Covering clause 10, refers to the set of steps to address the gaps identified and improve the efficiency of what is in place (Watkins, 2022, p. 17).

Covering briefly all the clauses:

- **Clauses 0 to 3 - Introduction, Scope, Normative references** and **Terms and definitions**.
- **Clause 4 – Context of the organization**: Understand external and internal issues, regulatory issues and interested parties of the organization.
- **Clause 5 – Leadership**: Establish objectives for the top management, according to the organization's strategy, as well as a top-level policy.
- **Clause 6 – Planning**: Consider risks and opportunities for the ISMS environment and establish a risk treatment plan, based on controls from Annex A of the standard.
- **Clause 7 – Support**: Evaluate the resources, awareness, and competence of the employees on security matters, and produce proper documentation for it, including a communication plan.
- **Clause 8 – Operation**: Plan, implement and control information security processes, in order to put into action the risk assessment and treatment plan.
- **Clause 9 – Performance evaluation**: Identify the proper KPIs (*Key Performance Indicators*) to monitor, measure, analyse and evaluate the ISMS. Conduct internal audits that are properly documented.
- **Clause 10 – Improvement**: Address nonconformities by eliminating their causes.

The second component is Annex A, which consists of 93 security controls that can be used as a checklist, covering four themes:

- **Organizational**: 37 controls on important processes and documentation on expected behaviour from users, systems, and equipment.
- **People**: 8 controls on the management of human resources by the provision of education and awareness training.
- **Physical**: 14 controls on physical asset protection.
- **Technological**: 34 controls on hardware and software and other components added to the systems of the organization.

Companies can be certified after an audit performed by an accreditation body. A lead auditor, in conjunction with a team, will perform an assessment based on a systematic risk management approach, covering all the aspects of the standard. By being ISO/IEC 27001 certified, companies demonstrate their ability to maintain a robust ISMS, and are therefore more credible to their customers, in terms of data protection.

If the company decides to undergo the certification process, it could be appropriate for its CISO and security officers to not only have a deep knowledge of the standard but to actually be certified as ISMS Lead Auditors themselves. By doing so, having a deep understanding of the specifics that auditors will look for and operating preliminary internal audits (as well as continuous ones to monitor compliance), they can make sure the auditing process to get the company certified goes smoothly from the beginning, by ensuring compliance. Also, this helps the company not only to get the accreditation but to maintain it in time, creating a culture of continuous improvement of information security practices and governance inside the organization.
Aside from this, it offers a framework and a clear checklist of security operations that a CISO should follow, even if the company decides to not be officially certified.

NIST Cybersecurity Framework

NIST Cybersecurity Framework was created through collaboration between industry and the U.S. Government and consists of standards, guidelines, and practices, based on a flexible and repeatable approach and existing cybersecurity standards.

The framework consists of three main components:

- **Core**: Provides activities and expected outcomes to guide organizations in cybersecurity risk management, complementing existing processes.
  The Core delineates the *Functions*, which are essential cybersecurity activities to operate inside an organization.

- **Implementation Tiers**: Provide context to help organizations understand to which degree they should apply the suggested approaches to their specific situation.

- **Profiles**: Used to identify and prioritize opportunities for improvement.

The *Functions* mentioned are the following and are the pillars of the framework:

- **Identify**: Helps in determining current risk inside the organization.
- **Protect**: Suggests the implementation of safeguards to prevent and try to reduce risk.
- **Detect**: Suggests ways to analyse possible attacks.
- **Respond**: Helps in taking action towards a detected security incident.
- **Recover**: Provides approaches to restore assets impacted by the incident.
- **Govern**: Helps in monitoring and assessing the existing cybersecurity risk strategy of the organization and its policies. It was added with the last update of the framework, released in the August of 2023. This last update also updates some critical aspects, such as the applicability to all organizations of every industry and size.

Yvon (2020) explored literature evidencing a lack of implementation of the NIST Cybersecurity Framework from the security experts of many U.S.-based companies, specifically from small and medium enterprises. Their research specifically aimed to understand the reasons, factors, and insights for this phenomenon, by interviewing a number of security officers. From the research, several themes emerged.

Many participants judged the framework as too complex to implement, or, at the same time, so open to interpretation that it was difficult to find a way to properly implement it. Many highlighted that the framework was “not being designed with small businesses in mind” (p. 112), but this was managed by the last framework update of 2023. They also judged the implementation of the framework as too expensive, for a multitude of reasons, especially not being able to understand the cost against risk.
Another major theme that emerged, which is the reason for the last point mentioned, was the lack of competent cybersecurity professionals in the US territory.

Even if the study is dated 2020, multiple sources still highlight this problem, not only in the US territory but worldwide. There is still a big gap between the number of cybersecurity experts needed and the ones available, especially with the right skills. If companies find competent professionals, they lack the budget to pay them (Hill, 2023).

Relevant certifications

From the *ECSO CISO Survey Analysis Report* (2021), we can grasp some of the certifications suggested for CISOs of various industries. The work is similar to what has been done for this dissertation during my internship: 24 questions on a variety of topics such as the work of a CISO, crisis management, certifications suggested, liability and regulatory aspects were written down on a survey that received a total of 101 responses by CISOs coming from different sectors.

Below I summarize the survey's findings:

- **Energy**: ISO/IEC 27001 was the most mentioned by respondents. However, "companies/operators choose to get certified as a measure of compliance. [...] certification is not considered as a priority in their organization" (p. 14). The security officers in this sector seem to prefer a risk-based approach, with a focus on vulnerability assessments and penetration testing as security measures, instead of a "compliance mentality that provides a false sense of security" (p. 15).
- **Finance**: The respondents consider certifications to be less valuable than standards. As a framework to follow, the NIST Cybersecurity Framework was mentioned.
- **Food**: The respondents again indicated that certifications are not seen as necessary, and they do not apply them in their company.
- **Health**: Certifications are not considered a priority or even a representation of the state of information security. The certifications applied are usually not related to cybersecurity.
- **Manufacturing**: The respondents indicated that certifications should be considered by CISOs to be involved in various processes. The security of the company is not based on the presence of certified CISOs or certifications, but these are seen as an aid.
- **Public sector**: Certification aspects are impacted by a lack of budget for allowing employees to be certified.
- **Telecommunications**: This sector relies on certifications, with the aim of merging the requirements with business needs.
- **Transportation**: The respondents answered that there is a need for a balance between agile processes and certifications. The companies are certified, but it is not mentioned if the security officers are as well.

- **Utilities**: The answers were split in half between respondents who did not consider certifications important and those who did and suggested even more visibility on the matter.

Unfortunately, in the research, it is never mentioned if the certifications the respondents were referring to were company certifications or information security officers specific. Also, there are no suggestions about which certifications, in particular, they are referring to, not even the type. If they were referring to company certifications, were they referring specifically to information security ones or other types?

A question that arose during the research and during the interviews was about the necessity for CISOs to own information security certifications and the current state of the art among information security professionals around the world.

A volume from the Computer Fraud & Security magazine (2006) stated that according to a government report:

> “the reason for the lack of IT security certifications was down to CISOs having skills that are **learned on the job**. ≪Generally, those state CISOs who do not hold certifications have gained their IT security expertise through years of “hands-on” work in IT security or closely related fields≫ the report stated”.

The article is dated 2006, but the purpose of this dissertation is to explore the *current* state of the art.
The benchmark data provided by a survey conducted by *IANS Research* with Artico Search (2023) highlighted that out of all the CISOs that participated in the survey, 36% “have completed or are currently engaged in a leadership development program with a certification” and that 33% is in a 1-1 executive coaching program. However, even in annual reports on the role of the CISO, it is difficult to quantify the number of security professionals investing not only in specific certifications like the ones on leadership just mentioned, but also CISO-tailored ones like C—CISO and CISSP.

The EC-Council, which is a cybersecurity technical certification body that operates in 145 countries globally and is the owner of certifications such as the ECSA (Certified Security Analyst) and C—CISO, states that, to this day, they have trained 300,000 information security professionals globally.
Evdokimov (2018), the then head of information security of Kaspersky Lab’s, after a CISO survey conducted by his colleagues, stated that 46% of the CISOs inter-

viewed had a CISSP certification and 37% had a CISM certification.
However, it is difficult to find more general statistics that are valid globally, to grasp more reasoning behind these numbers.

In the previous chapter, I already introduced the CISSP certification, since its eight domains could be used to understand the technical competencies that a CISO should possess. The exam outline offers a valid guideline for cybersecurity knowledge, but I will not delve more into that. What I want to mention, instead, is the fact that in order to be eligible to take the exam, an important, limiting requirement has to be met: five years of cumulative experience in at least two of the eight domains. Having a master's degree between the ones approved by ISC2 might be enough to cover only one year of the requirement (CISSP Experience Requirements, n.d.). This means this certification can certainly be obtained only by professionals who are already advanced in their careers.

Compared to CISSP, C—CISO certification not only validates a security expert's technical and managerial skills but also their leadership skills, because as stated by EC-Council itself, it was designed as a subsequent step to the CISSP certification, helping security experts move to executive roles. It covers the CISSP's eight domains from a business executive perspective and also covers concepts such as strategic planning and procurement (Richardson, 2022).

Another certification of relevance is CRISC, a certification focused on ERM (*Enterprise Risk Management*), which is one of the information security officers' duties, as we will see later in this dissertation. Being CRISC certified shows that the CISO is able to properly do a risk assessment, quantify risk, understand which is the organization's tolerance to it and respond adequately. Compared to other certifications, it is focused on a specific area, just like CISA with auditing skills. CRISC seems to be a credential pursued by security professionals who are advanced in their careers and who are already certified by other certification bodies (Fruhlinger, 2021a).

Not everyone believes that security experts should always be certified. Oltsik (2016) states:

"cybersecurity certifications may be worthwhile in esoteric cybersecurity areas or for individuals looking to explore new career directions. That said, **certifications should be thought of as supporting rather than replacing real-world experience**".

He believes some certifications are worthwhile, but the “industry” of certification bodies tried to do “a **marketing push** with a consistent message that more certifications equate to more money, knowledge and opportunities for cybersecurity professionals”.

Oltsik was part of a research report from ESG (*Enterprise Strategy Group*) in collaboration with ISSA (*Information Systems Security Association*), which highlighted several aspects of the different qualifications of a cybersecurity expert. First of all, the report showed percentages of different certifications obtained by CISOs, highlighting that more than half of the respondents had achieved a CISSP. Aside from CISSP, the percentages dropped (19% for CompTIA, 17% for CISM and 16% for CISA). Out of all the CISOs owning a certification, only 55% claimed that CISSP provided the knowledge, skills, and abilities necessary for their job. Other than the CISSP, only the CompTIA was said to provide them as well (but only for 13% of the respondents), indicating that certifications might not really be useful to be better proficient in the job and that probably “Cybersecurity acumen comes from experience, mentoring and hands-on training rather than book knowledge”.

Making a comparison with the most recent version of this research report, percentages are absolutely similar, and to the question “*Which of the following actions do you believe would be the most helpful for you in the advancement of your cybersecurity career?*”, out of 301 respondents, only 42% answered “*Pursuing more security certifications*” (Oltsik, 2023).

However, besides any discussion about the necessity for a CISO to own a certification or not, being certified does have a cost. CompTIA Security+ costs $392; CISSP is even higher (justifiable, considering it is the gold standard of information security officers certifications), with a price of $749; CISA costs $760, same for CISM and CRISC (but no renewal fees are expected, compared to the other ones) (StationX Team, 2024).

Yes, being a certified CISO not only shows objective capabilities and offers credibility to their companies and their clients but also spikes their career and salary. However, should it be a CISO duty to be certified, or **should the companies invest more in their professionals?**

The relevance of certifications depends on the specific organizational context, but users are becoming increasingly aware of cybersecurity matters. Organizations might benefit from a high return on investment by demonstrating to their clients that they are able to securely manage their data.

Chapter 3

Hierarchy

During the interviews, one of the questions I asked the CISOs interviewed was about the hierarchical position of the CISO in the organizational chart.
The CISO reports to the CIO in two out of five cases (for *Advisory* and *Retail*) and reports directly to the board in two cases (*Wholesale* and *Services*). In *Healthcare*, the CISO and CIO roles are the same (in this case, the information security officer role is taken by the system administrator), and the C-suite roles are not present, so the analysis cannot be applied.

Specifically, for each of the companies interviewed, I will list the information about the organizational structure and hierarchy and the type of communication between the different roles:

- **Advisory**: The CISO is properly defined in a policy and is below the CIO in the organizational hierarchy. In case of an incident, the CISO reports directly to the board of directors and the DPO (*Data Protection Officer*) in a crisis committee. The CIO approves the policies written by the CISO and has procurement, so the security budget is not in the hands of the CISO.

- **Wholesale**: The CISO is in the top management, at the same level as the CIO. The communication follows a top-down approach in which the CISO can act promptly in case of an attack without necessarily reporting to the board. The reporting happens only after the decision has been taken. The CISO has procurement.

- **Services**: The CISO is delegated by the CEO, and reports directly to the board of directors, specifically through security committees in which, quarterly during the year, initiatives, advancement, and policies are discussed.

- **Retail**: The CISO refers to the CIO, but information security projects are discussed directly with the board of directors. Communication with the board is also expected in case of risks, the possibility of a security breach and for project approval. The procurement is on the CIO.

Literature review on possible hierarchy structures

In my bibliographic research, I found different sources with some current and past statistics about the different reporting structures, other sources with explanations of different drivers for the choice of the hierarchy inside the organization and the pros and cons of each possibility, and sources talking about the conflict of interest that might arise between the CISO and the CIO. The bibliographic resources mentioned space from 2006 to 2023.

The hierarchy position of a CISO inside the organizational chart can vary depending on various factors, such as the industry in which the organization is operating, how the C-suite is composed and the size of the organization.

Hitch Partners published a *CISO Survey Report* for 2023, which collected answers from more than 650 information security officers coming from the U.S. The authors call "CISO" professionals who hold this title but also CSOs (*Chief Security Officers*), and the reporting structure evidenced is divided into privately held companies and publicly traded companies. The former usually shows the CISO reporting to the CEO (more than half of the respondents), while the latter shows more than half of the CISOs reporting to the CIO. For both types of companies, the information security officer **reports to the board at least quarterly for more than 40%** and does not report at all to it for less than 15% (Hitch, 2023).

According to Puetz and Abdelkader (2022), the benefits of the CISO reporting to a C-suite executive between CEO, CRO (*Chief Risk Officer*) or CFO or, instead, to the CIO, are different.
The benefits of the former option are, for instance, the increased CISO authority and influence over the board, the increased perception of cybersecurity as a problem that does not solely belong to IT, and the possibility for the CISO to stop a CIO's decision that is just too risky in terms of information security. On the other side, the benefits of the latter are an increased proximity to the first line infrastructure, which can allow to better highlight potential issues for the second line (risk management) and the third line of defense (internal audit).

With “lines”, I am referring to the “*Three Lines Model*”, previously known as the “Three Lines of Defense”. This model gives a structure that helps organizations with risk management and governance and defines “first line roles” as those who provide products or services to clients, “second line roles” as those who monitor and manage risk and “third line roles” as those who ensure the achievement of objectives by independently overseeing the processes in place (The Institute of Internal Auditors, 2020).

According to Fruhlinger (2021b), in a 2020 report on the state of the art of CISOs, we can see that **in 24% of cases, the CISO reported to the CEO** and **in 33% they reported to the CIO**.
Looking at the same report from 2023, it is not possible to make a comparison because the same percentages are not available. It is only stated that 48% of security leaders meet with the board one or more times a month and that 25% report directly to the board of directors (compared to 20% in 2022) (Foundry, 2023, p. 6).

The **conflict of interest between the CIO and the CISO** starts from their main objectives: the CIO, being responsible for the management of Information Technology inside the organization, aims to plan ways to use the technological assets inside the organization to aid the digital evolution in it, or to invest in new assets. At the same time, they also must consider the organization’s budget, in terms of time and money, which can translate into prioritising features, functionalities and flexibility over information security, which is the job of the CISO. Where the CISO is positioned in the organizational hierarchy therefore heavily influences the relationship between the two roles.

If the CISO role is under the CIO in the organizational chart, then cybersecurity will be seen solely as a technological matter. As we started to understand in the previous chapter, and as we will see better in the next chapter about the duties of a CISO, cybersecurity is so much more than a technological issue.
Having the CISO report directly to the board of directors or to a C-level role higher than the CIO will permit to see cybersecurity as “embedded into the overall risk management of the enterprise” (Brody, 2021).

As we see from the same article written by Brody for CISCO, the 2014 version of the FISMA (*Federal Information Security Modernization Act*), which is a U.S. federal government law, designates CIOs as the first responsible for the development, documentation and implementation of the information security programs, therefore formally determining the placement of the CISO in the organizational chart under the CIO.

Brody states that the position of the CISO depends on the enterprise's perspective on risk management. If this is embedded into the culture of the organization and continuously overseen by the CEO, then the CISO cannot be placed under the CISO in the hierarchy. If, instead, the main core of the organization is information technology (and therefore the protection of the resources is the only cybersecurity obligation to its stakeholders), then the CISO needs to be under the control of the CIO. In general, he concludes, that when the CISO is placed under the CIO, cost management is considered more important than risk management, and vice-versa.

Bittianda (2018), analysed possible reporting structure solutions and their pros and cons, by interviewing diverse people from various information security responsibility positions.

Reporting to the CIO, states Bittianda, is the most typical reporting structure. He considers the communication between a CISO and a CIO to be easier compared to the one between a CISO and the rest of the C-suite or the board of directors. This is because the CIO typically fully understands cybersecurity matters immediately. This, anyway, could also mean focusing on technological solutions rather than solutions that include more holistic solutions like, for instance, information security awareness between employees of every level of the organization, also taking into consideration the fact that most vulnerabilities come from the weak element of the chain: humans. Conflict of interest is considered, again, as another possible issue with this solution.

Some financial services firms have started to place the CISO under the CRO. This can make sense considering the role of the Chief Risk Officer is to oversee risk in general, not just in financial terms. This could also move the CISO too far away from the board if the CRO does not report to it directly.

CISOs could report to the CFO, which could give a better possibility for the CISO to better administer the budget towards cybersecurity projects. This also means that CFOs will probably seek a clear and direct return on investment, which sometimes is difficult to see clearly when investing in cybersecurity solutions. Another possible issue might be the lack of technological knowledge that a CFO might have.

Reporting to the CDO (*Chief Data Officer*) is another option, considering that they see data as an asset, but at the same time, they might want to use it to increase revenues at the expense of security.

Reporting to the CEO makes the CIO independent and enables better communication concerning prioritization, budget, and risk. At the same time, if the CISO is still not part of the management team, then they probably won't be included in the discussion anyway. Reporting directly to the board can only be possible if the importance of cybersecurity is embedded into the organization.

One thing that must be considered is the fact that some of these C-suite roles might not be present in small and medium enterprises.

A survey by *Forrester Research Inc.*, cited by Stupp (2019), shows that in 35% of cases, the CISO reported to the CIO, and in 18% of cases, they reported to the CEO. These percentages, compared with the ones from the year before, shift towards the CISO to CEO option.
LaSalle, cited by Stupp, said that considering it is a hybrid role, it is difficult to find the right placement for a CISO. Their role changed from compliance enforcer to risk coach, which “brings a different set of disciplines and skills required to navigate that shift”.

Osborne (2006) reviewed where the security function should be positioned in his book about information security management, with observations made from his 10 years of experience in security consulting.
The most common position was already in 2006 right under the CIO. The advantages and disadvantages reported are exactly the same as the ones mentioned above from other sources. This is considered, again, the best option in case the main core of the organization is IT. Good partnering and communication with other departments and units may reduce the disadvantages of this position.
The other option mentioned is the one where the CISO is positioned below the CEO, CTO (*Chief Technology Officer*) or CFO, which the author defines as the best one because it ensures a more holistic approach to information security.

The point is, as Ellis (2022) remarks, that **CISOs are Chiefs**. It's in their title. Not every organization has information security embedded in its culture, so if the employers decide to start by hiring a CISO, but they bury them below many layers before being able to communicate with the board, maybe they may never be heard. For instance, as the author notices, if the CIO decides to cut costs, it will probably impact security as it is seen merely as an IT function. The reporting formula of CISO to CIO can only work in situations where a cultural change has already started. If the organization just started the change, they should put the CISO directly below the CEO.

An article from Wynn (2005), already evidenced the issue of forgetting about the "Chief" part in *Chief Information Security Officer*.
A 2004 survey evidenced that 34% of respondents placed the CISO below the CIO (perfectly in line with the current state of the art). Wynn describes this situation, saying it "hinders the CISO's effectiveness and limits his or her ability to implement change". Specifically, one of the reasons described for this is that "when threats may cause business disruption, **tactical issues take precedence over longer-term planning**. It is easier to buy and implement firewalls and intrusion detection systems than to develop security policies and implement a sound awareness program". Basically, when the CISO cannot easily reach the board of directors and must report to the CIO, "**security loses out to availability** (of information systems)".

The solution proposed is to separate information security management (intended as a long-term program) from the daily IT security operations, and the CISO should directly report to the board of directors or the CEO.
Another possible solution suggested (and applied by 34% of respondents at that time) is to combine information security and general security, elevating the CSO to report directly to the CEO or do the same with CRO in medium to small enterprises, considering information security risk to be part of general risk management in its totality.

Inskeep (2019) analyses the different factors influencing the reporting structure, highlighting the perspective on the security of the organization and the industry as the main ones. Confirming what I stated before, Inskeep noticed that CISOs typically report to the CIO in situations where companies highly value cybersecurity and see it as an enabler for the business and that when security is considered as a mere cost, "the CISO is perceived as a technical caretaker of security technologies", with the only goal of compliance towards requirements.

Another driver he considers is the type of industry. I will list below the different ones highlighted by the author:

- **Finance**: The CISO typically reports to the CIO and, in some cases, to the CRO.
- **Energy**: Same reporting structure as above, even if, in some cases, the information security function is split between other roles.
- **Retail, transportation, and manufacturing**: The CISO reports two layers or more below the CEO, typically to the CTO or CIO.

Inskeep then proceeds to assess the benefits and risks of the different reporting structures. Again, I will briefly list some of his findings below:

- **Reporting to CIO**: Useful for communication since the IT function thoroughly understands the information security needs, but might cause possible conflicts of interest, with the direct consequence of postponing security plans and limiting the budget to prioritize other goals.
- **Reporting to CRO**: It can provide an alternate funding channel for information security budgeting, and also moves information security away from the IT function, reinforcing the principle that cybersecurity risk is part of the general risk to take into account, but if the CISO lacks the proper soft skills, they might not be able to properly do their job.
- **Reporting to CEO**: Permits to ensure the right authority, priority, and recognition to information security, but may cause the CIO and CISO to compete for the same piece of the budget.
- **Reporting to the board**: The CISO must be an established leader with the right soft competencies for this solution to be right.

"It's very rare to find a CISO who reports to the CEO, yet that is **the most dramatic indicator that a company takes its security seriously**," says Ted Julian, cited by Hale (2014, p. 17). In his article, many executives report the issues with the implementation of this role, the right positioning, and the struggles to implement security in general inside organizations, with poor budgeting and resource shortages. They state that the type of reporting structure where the information security officer reports below the IT function works only if the CISO is reporting to an executive who understands how critical information security is and actually works towards it when needed.

When the CISO reports to the CIO conflicts of interest arise, in operational, goals, strategic planning and budgeting terms. A CIO's priority is to keep systems operational and a CISO's priority is to get the support of executive management to protect the organization and take fast decisions. In organizations where the CISO reports directly to the CEO and the board of directors, these roles are "sending a clear, unequivocal message to their organizations, investors, partners, and their customers that they are committed to addressing cyber risks with transparency, shared responsibility, and accountability. The stakes are too great for organizations to do otherwise" (Chanaga, 2017).

A more recent survey from Heidrick & Struggles (Aiello et al, 2023), with 262 respondents from the U.S., U.K., Germany, France and Australia, evidenced a 5% of CISOs reporting to the CEO (with a decrease from the 11% of 2021 from the same survey), a slight degree from 36% to 38% in the ones reporting to the CIO and a slight increase in those who report to the CTO. Two-thirds of the CISOs surveyed report to a role that reports directly to the CEO, and complexly 64% report to someone other than the CIO.
The authors "believe that the number of CISOs reporting to CIOs will continue to decrease as the CISO role takes a broader enterprise risk oversight role with direct ties to the audit committee and board" (p. 14).

According to a research study conducted by Karanja and Rosso (2017), newly created CISO positions tend to report to the CEO (74% out of 35 respondents), while old CISO positions (so newly hired CISOs that replace a position) tend to report to the CIO (63% out of 19 respondents that fell in this category). In companies that want to elevate the position of the CISO with the aim of better reflecting a focus on information security, it makes sense that newly hired employees are easily placed higher in the hierarchy, since "creating a new position at a higher level is likely easier politically than changing who a current position reports to" (p. 37).
The two authors state that CISOs that report to the CIO "might be less inclined to disclose security flaws that might cast the CIO in a negative light" and that "a lack of direct CISO - CEO reporting structure might mask security vulnerabilities to the top management team" (p. 37). Still, for this last reporting structure to work, CISOs must possess the soft and leadership skills I already discussed.

Shayo and Lin (2019), in their research study, found five main drivers for the reporting structure, which are the maturity of the organization towards information security, the different perceptions of risk of the CISO and the CEO, the knowledge of the CISO about the business they are working in, their cybersecurity knowledge and the communication and collaboration between CISO and CEO.

Maloney, cited by the two authors (they wrongfully credit Curry as the author), states:

> “There is no silver bullet to bridge the culture gap that currently exists between CISOs and the board, and right or wrong, it’s not going to happen unless the CISO can prove that he or she is worthy of that respect and authority. The CISO must present themselves to C-level executives as a **businessperson first and a technologist second**. Leading with bits and bytes is a surefire way to lose the respect and interest of the C-suite. It’s about establishing a new dialogue with the business and exercising soft skills” (Maloney, 2016).

As shown from the findings, the current state of the art is **unclear**, and the statistics are too mixed up to fully understand if companies prefer the CISO to CIO approach or the CISO to board/CEO one.

The reality is that many highlight an issue: information security officers, in order to have visibility, might need to report higher up in the chart. Considering how critical cybersecurity is in every industry nowadays, maybe it would be time for companies to recognise that **there is a C in Chief Information Security Officer**, and behave accordingly to ensure not only that they are working appropriately, but that they also give information security (and the experts that work towards it) the right importance.

Chapter 4

Duties

The placement of the CISO in the organizational hierarchy, the exact reporting structure and whether they report directly to an executive on the board of directors or not, are directly related to the duties and responsibilities of this role.

I will explore different bibliographic sources to understand what this role should manage, even if, depending on the exact organizational reporting structure, some of the duties and responsibilities could be of another executive.

Starting from my interviews, I will list the various tasks and security strategies reported by the various CISOs:

- **Advisory**: The CISO checks periodic reports from various technologies that monitor warnings, anomalies, and traffic detection, as well as reports coming from the IT function, such as disaster recovery tests and recovery time tests. They perform vulnerability assessments and risk assessments and instruct penetration tests. They develop and maintain the ISMS, the procedures, and operational instructions for the company, as well as the cybersecurity awareness strategies for the employees. They are involved in meetings to discuss vulnerabilities. They use AI technologies to control security. The role of the CISO is defined in a specific policy.

- **Wholesale**: The CISO checks periodic reports and works in close collaboration with internal auditors to monitor compliance. They take care of the awareness programs for the employees, on a technical side but also a social engineering side. They implement a “toolbox” of information security practices given by third parties. The security strategy implemented follows a risk approach and a cost evaluation approach. They implement AI technologies for anomaly detection.

- **Services**: The CISO takes part in security committees where quarterly initiatives, advancement and policies are discussed. They periodically review reports and establish KPIs for incident sustainability. They monthly participate in committees on performance management and review the asset inventory. They perform risk assessments for critical points and overview change management. They follow processes and procedures from an ISMS given by thirds. They perform vulnerability assessments every month and penetration tests twice a year. The role of the CISO is defined in a specific procedure. They overview the work of two SOCs (*Security Operations Centers*) with weekly reports. They instruct the disaster recovery plan and the phishing tests for awareness training. They implement AI solutions.

- **Retail**: The CISO periodically reviews information security projects and reports from automatic asset mapping. They instruct continuous, automatic, low-impact vulnerability assessments and request patching. They instruct internal audits to monitor security. They operate risk assessments and take care of the information security awareness platform. They rely on an external SOC and perform deep web research for vulnerabilities.

- **Healthcare**: The CISO overviews change management. They perform risk assessments and plan disaster recovery. They develop awareness training plans for the employees.

Before diving into what the literature shows about a CISO's duties and specific responsibilities, I want to introduce the concept of **GRC**, which stands for *Governance*, *Risk* and *Compliance*. The term was coined by Scott Mitchell and appeared for the first time in his paper for the International Journal of Disclosure and Governance titled "*GRC360: A framework to help organizations drive principled performance*" (Mitchell, 2007). Like other concepts inside this thesis, I won't dive too deep into a description of what led to the GRC definition or all the possible applications, but since it is a reference for an integrated approach that a business can use to achieve its goals (and a CISO's job is, again, to take care of a big portion of the business objectives using a set of interrelated practices), it is necessary for me to give the reader a background on why the CISO should take care of certain aspects.

GRC collects all the processes (and people and technology inside the organization) that help an organization drive toward objectives while staying within the boundaries of both uncertainty and the need for integrity. These 10 main processes are not isolated silos but are interrelated and overseen by multiple actors inside the organization. I will now briefly list and discuss them. To do so, I will directly reference Mitchell's paper:

- **Governance**: Processes executed by the top management which aim at governing the decisions inside an organization by checking the strategy in place, cultivating relations with stakeholders, evaluating current performance with aimed performance, and overseeing risks.
- **Strategy**: Processes executed by the C-Suite that include setting the steps to reach the organizational goals and managing the performance.
- **Risk management**: Processes typically executed by the CRO that include the identification, assessment, and management of all types of risk for the organization.
- **Audit**: Processes typically executed by auditing bodies (or certain executives inside the organization itself) that cover the execution of audits and the consequent reporting, and the proper investigations in case of non-compliance.
- **Legal**: Processes executed by the legal staff that include the definition of the legal strategy, litigation and ensuring compliance with regulatory requirements.
- **Compliance**: Processes that include the identification of the regulatory requirements of various types and the steps to be compliant with them.
- **Information Technology**: Processes covering automatic controls, ensuring privacy and security, managing electronic assets and digital information and reporting.
- **Ethics and corporate social responsibility**: Processes that cover the promotion of principles and common values, the management of the code of conduct and understanding the socio-political-economic context of the organization.
- **Quality management**: Processes aimed at ensuring the delivery of the organizational objectives with the desired quality, which include the analysis of root causes and the implementation of projects for process improvement.
- **Human capital and culture**: Processes executed by human resources staff which aim at the construction of the organizational culture and the management of the human assets of the organization.

Communication, evaluation and responding capabilities, proactivity, training, policy enforcement, standards implementation, information quality and reporting improvement, boundaries identification, cost evaluation and reduction of costs, and continuous improvement are all meta-processes that are common to the 10 main processes just discussed.

All these processes perfectly align with cybersecurity aspects.
Considering what I learnt during my internship, the uniqueness and distinctiveness of the CISO role stand in this: **they cover the entire GRC**.

Literature review on duties

Worstell (2014) identifies the following four key factors that define the focus areas for the role of the CISO:

- Standard of care strategy
- Governance and accountability
- Clear roles and responsibilities
- Metrics, reporting, and executive visibility

The author states that the CISO has a specific driver for their strategy, and that is to "put in place the mechanisms (controls, oversight, monitoring, metrics, and reporting) that will enable the business to demonstrate due diligence to that standard of care" (p. 4).
By "*standard of care*" we mean the set of policies and procedures which must be reviewed, monitored, and of course applied, to mitigate documented information security business risks, assessed in order to identify areas that could be exploited for a breach and therefore cause a certain impact that could be measured in various ways. The defined standard of care must be implemented and monitored through a series of controls.

The author states that it is not a CISO's job to "get involved in monitoring firewall rules or router configurations". What the CISO should take care of is making sure that the rules are applied by monitoring established periodic reports, and correctly identifying specialised technical staff that can correctly implement the standards. The role of the CISO is "blending into business functions" in order to address risks "throughout the life cycle of business strategy, plans, and execution".

Mather, stated by the author, thinks that CISOs should take care of the promotion of information security objectives **without forgetting about people and policies** and that they should unify those objectives with business objectives and risk evaluation, but also human acceptance. CISOs should aim to translate information security objectives “in terms of business risk that business unit personnel can understand and appreciate”. The protection of business in all its domains is essential and “must be coordinated to avoid weak links in the protection strategy that could prove disappointing if not devastating to a business, or to individuals” (p. 9).

Considering this interdisciplinary approach, the tendency is to centralise all the functions under a CISO to ensure that information security is controlled and managed by a single manager in a consistent way in all of its aspects. However, the author states that placing all the functions under a single manager should be resisted and that they should be distributed across all executives from all business units, to ensure accountability and due diligence by every business executive, to avoid conflicts of interest, to integrate information security in the entire business process, in order to install it in the organizational culture, and to make sure top management understands that this is a business matter, not an IT issue. The approach to security must be policy-driven.

Worstell then proceeds to list a set of principles for accountability and reporting where the CISO participates at different degrees, from leader to observer. These 10 principles must be evaluated considering the specific organizational context.
I will proceed to list some of them that apply to the scope of this thesis and summarize them briefly because they provide a guideline to understand what could be a CISO’s responsibility, at least in the opinion of the author and considering they also match my personal experience of what I observed during my internship:

- The CISO manages the IT assets of the business and governance processes are in place for proper asset management.
- A third party reviews the implementation and effectiveness of information security measures (perfectly in line with the Three Lines of Defense model).
- The CISO and the business units establish together the cybersecurity budget.
- Cybersecurity is actively monitored by an IT governance board (it is not specified how this is composed, but I am personally assuming it includes the CISO since the author believes they belong to top management).
- Information security is tied to business rules “in ways that are traceable, understandable, and agreed to by the business” (p. 12).

- Changes in IT security must be authorized by designated IT change boards (again, it is not specified if the CISO is involved or not).
- Cybersecurity processes are "standardized, documented, and reviewed regularly for consistency" by IT management (again, I assume this includes the CISO for the reason above).

The major obstacle of a CISO is a business that does not understand the value of IT. In the words of the author:

> "IT is the business. That is to say, IT today governs the systems that process the information that is **the lifeblood of the business**. Without the information, the business will stop. [...] once the business realizes its own accountability for the confidentiality, availability, integrity, ownership, and possession of business information, as well as for information-security practices and improvements, it will enjoy a whole new level of interest in, and responsibility for, the enterprise" (p. 12).

Worstell basically states that, independently of the specific duties of the CISO that are directly influenced by the context of the organization and its scope, the governance of information security must be in the hands of the business at every level, especially top management. The critical thing the CISO should care about is how the governance structure is established, and making sure it is enforced effectively and measurably, by establishing clear accountability through proper reporting practices and metrics, that must be KPIs to provide to the business to demonstrate the work done (and the fact that cybersecurity could provide an actual return on investment if implemented correctly).

In order to ensure compliance with the latest regulations, such as the GDPR (*General Data Protection Regulation*) and the NIS2 (*Security of Network and Information Systems*) Directive, the CISO must apply a comprehensive approach that is "a single comprehensive response to all queries".

Hale (2017), to identify the responsibilities of the CISO, refers to the periodic job task assessments conducted by ISACA, which identified four knowledge domains that are essential for an information security executive:

- Information Security Governance
- Information Risk Management and Compliance
- Information Security Program Development and Management

- Information Security Incident Management

Hale then proceeds to expand on each of them, and I will again summarize his thoughts to identify the key activities of the CISO.

The CISO defines the information security goals and objectives, aligning them with organizational goals. They develop the policies and procedures that must be followed, identify the key factors in the organizational context that might influence information security risk, and establish the metrics that must be reported to management to properly measure risk and how effective the information security strategy is. To do so, the CISO has a series of knowledge requirements that Hale lists, and that perfectly aligns with what I already discussed in the chapter about the CISO competencies.

The CISO is accountable for information risk management, by promoting and maintaining proper processes and ordering periodic risk and vulnerability assessments. They evaluate the controls and report whether there is a need for a change in the level of risk considered and assist in developing the needed changes.

A CISO must also ensure compliance by identifying legal and regulatory requirements. The author also specifies that some accountability may be shared with other executives depending on the organizational structure.

The CISO is also responsible for the development of awareness programs inside the organization, which permit the information security strategy to be fully implemented in the organizational culture. They take care of the integration of the cybersecurity requirements into organizational processes and also into contracts with third parties. The CISO must also provide frequent reports to higher executives and board members about the efficiency of the security program.

The CISO is also the security incident manager. They are responsible for defining the severity of incidents and developing and maintaining an incident response process. They are responsible for testing periodically the incident response plan and for training the teams for efficient response, as well as conducting post-incident analysis and investigation to develop the appropriate corrective actions.

The level of direct application of the activities mentioned above depends on the context of the application and the industry in which the CISO is operating.

The specific duties just discussed can be summarized into three main categories:

- **Govern**: the strategic direction for the implementation of the information security objectives of the organization, based on business-specific needs. It includes processes such as risk assessment, strategy definition, ISMS creation, implementation and maintenance, establishment of reporting plans and identification of key stakeholders.

- **Make**: the operational management of the information security strategy established. It includes the definition and implementation of policies, procedures and operational instructions for the organization, as well as crisis response procedures and the creation of awareness projects.
- **Control**: the monitoring processes of the information security strategy. It includes audit activities and alarm monitoring.

The NIST Cybersecurity Framework already described in the previous chapter offers a clear representation of the areas of interest just discussed.

Legal compliance

Delving more into the legal and compliance area of interest, the necessity of the CISO is even more relevant if we consider that companies (and their managers) could incur into civil liability in case proper protection measures are not in place, with consequent financial penalties, both in terms of loss but also legal sanctions from regulatory bodies and data protection authorities, like the French CNIL (*Commission Nationale de l'Informatique et des Libertés*), the Italian GPDP (*Garante per la Protezione dei Dati Personali – Italian Data Protection Authority*) or the EDPS (*European Data Protection Supervisor*) and ENISA (*European Union Agency for Cybersecurity*), especially after the application of the GDPR, or the NIS2 Directive. Companies might incur **severe sanctions** in case of non-compliance, depending on the gravity of the violation and the level of damage and degree of responsibility (De Éminville, 2020).

The GDPR guarantees European citizens their rights to the ownership of their personal data and regulates the permission and conditions for their usage with substantial fines in case of unintended use.

The *Data Controller* (which is a legal person detaining the personal data of users that determines the purposes and means by which these are processed) is responsible for ensuring appropriate security measures (that are measured depending on the risk posed to the data) during the processing of data, taking into account factors such as the state of the art of technology, the context and purpose of processing and the severity of risks in the rights and freedoms of data subjects. These measures are a continuous duty and include common cybersecurity practices (Sharma, 2019).

Article 5, paragraph 1.f of GDPR states that personal data shall be "processed in a manner that **ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures", and that "the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1".
Article 32, "*Security of processing*", specifies the specific duties of ensuring CIA to processing systems and services and regular testing, and Article 33, "*Notification of a personal data breach to the supervisory authority*", makes it a duty for the Controller to properly notify the DPO in case of a breach, by assessing the type of breach and their degree, therefore making it essential for a CISO to collaborate with the DPO.

Since the GDPR makes it possible for a DPO to be hired outside of the company or inside of it, we could think of the possibility of merging the two roles. After all, both should aim at the protection of data. The point is, however, that the DPO protects data for the interests of users, and the CISO protects data for the interests of the company, so the two roles shouldn't match, even if the *Litigation Chamber of the Belgian Data Protection Authority* approved the combination of the two roles in a decision in 2021, but only if the CISO is just an advisor and security measures are not within the scope of the CISO, which, considering what we have seen until now, does not make sense (Michielsen, 2023 & Atallah, 2023). Another thing to consider is that DPOs and CISOs usually have two completely different backgrounds so it is inherently difficult to find someone with the right competencies to fulfil both roles at once. However, as stated before, the two roles should definitely collaborate, especially in case of a data breach. The Controller, as I said before, must report a breach within a certain amount of time. The DPO can immediately intervene and work with the C-Suite to do a first assessment of everyone's responsibility and accountability and to also check who was impacted directly (Swinhoe, 2020).

The NIS2, which is the second version of the Network and Information Security Directive of the EU, considers new factors to better reflect the increased digitalisation across different industries by providing a policy with legal measures to increase the overall level of cybersecurity across the Union. The Directive also identified the essential sectors that should pay particular attention to cybersecurity, such as transport, healthcare, and energy, since they provide essential services, socially and economically.

NIS2 poses greater responsibility to the management bodies of the entities (which include the CISO). It is stated that they must approve and oversee the implementation of measures, they can have liability for infringements on the framework, must assess the due diligence of suppliers and get proper training on cybersecurity approaches and techniques, as well as have reporting obligations in case of a breach (Article 23). Essential entities may be subject to fines of up to 2% of their total turnover in case of non-compliance (Article 34) (Vandezande, 2024).

The entities fall under the jurisdiction of the Member States in which they operate. For instance, in Italy, companies must ensure compliance with the *Legislative Decree n. 231/2001* and with the *Legislative Decree n. 82/2021.*

The *Cyber Resilience Act* is another measure taken by the EU which complements the NIS2 Framework, expected to be applied in early 2024. The Proposal aims to guarantee rules for upcoming products in the market and a framework of cybersecurity requirements and relative obligations, by requiring transparency from manufacturers to consumers, covering the entire lifecycle of the product. The imposition of administrative fines is up to the market surveillance authority of the Member States (up to 2,5% of the total turnover, considering the circumstances and specific situation), but we can again see how it is essential for companies to be compliant and to have a role like the CISO overseeing these aspects (along, of course, with the legal team of the company).

The EU Law is developing day by day for both digitalization and cybersecurity. Along with the regulations mentioned, the proposal for the regulation on Artificial Intelligence (*AI Act*) and the most recent *Data Act* are signs of the most recent changes in our society (and the need to regulate these changes as fast as possible).

The Data Act is an EU Regulation on the usage of data, in action since the 11th of January 2024, which complements the already in place *Data Governance Act*, which already called for data spaces that ensure high levels of cybersecurity, and whose scope is to regulate processes for data sharing. The two regulations together help establish fair rules for the access and usage of data. This will certainly help continue the digitalisation process of European companies, therefore opening to possible future threats.

However, in the Data Act itself, it is stated that:

> “This Regulation should be without prejudice to rules addressing needs specific to individual sectors or areas of public interest. [. . .] Such rules may also include limits on the rights of data holders to access or use user data, or other aspects beyond data access and use, such as governance aspects or security requirements, including cybersecurity requirements” (Data Act, 2023, p. 31).

A CISO must acknowledge even these Regulations, by communicating properly with the legal team in the company and be a step ahead of possible open doors for breaches.

Conclusions

The increasing legal landscape leads to an increased possibility of facing **litigation** after a breach. Being able to properly document the information security actions pursued inside the organization and choosing transparency with customers is an insurance for the CISO. Two examples are Uber's CSO, convicted of obstruction of proceedings and misprision of felony for his attempted covering of an attack suffered in 2016 (USAO Northern California, 2022), and the most recent charges against SolarWinds' CISO, for fraud and internal control failures against allegedly known cybersecurity risks and vulnerabilities (U.S. Securities and Exchange Commission, 2023).

Moraetes, interviewed by CSO Online (2008), believes that security professionals should be covered with legal protection or **insurance**, and start preparing for legal depositions and collection of evidence. This of course applies to the U.S. legal landscape, and I personally do not know how applicable it might be to the European one.

Garrie (2015) states that the most important factors that a CISO must document in order to prove that they have been compliant with their job requirements and state regulations are the number of resources and priority cybersecurity has been given, how the most valuable company's information has been identified and protected, whether or not the same rules have been applied to the third-party partners, whether or not the procedures have been continuously evaluated, if a crisis management plan is in place and if the company and its executives are insured in case of a breach.

Another clear challenge the CISO faces is **the rise of AI**, the most popular IT topic nowadays. The Rise of AI can be both an obstacle and an aid for CISOs. On one hand, AI permits new tools which create new vulnerabilities. It can help malicious hackers build new malware easily and use AI-generated voice to bypass controls and it can be used for social engineering attacks. On the other hand, it can help to identify vulnerabilities. Three out of the five CISOs interviewed stated they are already implementing AI solutions for anomaly detection. Referring to the AI Act can certainly help CISOs better navigate this digital and social transformation.

In conclusion, the role of the Chief Information Security Officer is surely a complex one. The CISO is not only the supervisor of IT security in an organization but also a change agent, and their position should be supported by top management because they are business enablers and protectors and therefore, they are subject to high levels of stress. Doing even a small online research with the words "*CISO*" and "*burnout*" will clearly show how these professionals are struggling and will continue to struggle even more with the digitalisation times we're going through.

A standardised role could be beneficial to reduce this stress, and here we go back to the question we introduced at the start and the main point of this thesis:
"*Can the role be standardised?*"
Considering what we have learnt in the past chapters, after evaluating academic literature and articles and surveys, the answer is: "*Well, yes and no*".
Even if a generalisation can be made on a CISO's best practices, the truth is that their duties and organizational position **change depending on the context**, and to be fair the literature is too scarce to give a clear answer. However, the CISO should be **standardised at least inside the organization**. By this, I mean that every CISO, before accepting their job, should make sure that the company has already a policy in place that clearly defines the duties and responsibilities of the role and how they will interact with top management.

In the uncertainty of my answer, one thing is undeniable: in an era of digitalisation, where data is the new gold and vulnerabilities will only arise in the future, a CISO is a **necessity**, and organizations and governments should recognise it and properly act for it.

Bibliography

Aiello, M., Thompson, S., Reventlow, C., Shaul, G., Randria, M., Vaughan, A. (2023). *Global Chief Information Security Officer (CISO) Survey.* Heidrick & Struggles. heidrick.com/-/media/heidrickcom/publications-and-reports/2023-global-chief-information-security-officer-survey.pdf

Anderson, K. A. (2014). The Hybrid (Frugal) CISO. In *The Frugal CISO: Using Innovation and Smart Approaches to Maximize your Security Posture* (pp. 311-322). Auerbach Publishers, Inc. doi.org/10.1201/b16888

Atallah, M. (2023). *Data Protection Officer And Conflicts Of Interests.* Mondaq. mondaq.com/data-protection/1279234/data-protection-officer-and-conflicts-of-interests

Bittianda, K. (2018). *What's The Best Reporting Structure for the CISO?* EgonZehnder. egonzehnder.com/industries/technology-communications/cybersecurity/insights/whats-the-best-reporting-structure-for-the-ciso

Brody, B. (2021). *Should the CISO Report to the CIO?* CISCO. blogs.cisco.com/security/should-the-ciso-report-to-the-cio

C—CISO. EC-Council. eccouncil.org/train-certify/certified-chief-information-security-officer-cciso/

Certification in Outsourcing Management for IT (COMIT). Singapore Computer Society. scs.org.sg/certifications/comit

Chanaga, J. (2017). Three security actions CEOs must take. In *SC Magazine* (vol. 27, fasc. 12, p. 50). proquest.com/trade-journals/three-security-actions-ceos-must-take/docview/1863563438/se-2

Chief Information Security Officers' (CISO) Challenges & Priorities. (2021). European Cyber Security organization (ECSO). ecs-org.eu/ecso-uploads/2022/10/6087e6f2d1357.pdf

CISA. ISACA. isaca.org/credentialing/cisa

CISM. ISACA. isaca.org/credentialing/cism

CISSP - Certified Information Systems Security Professional. ISC2. isc2.org/certifications/cissp

CISSP Exam Outline. (2021). ISC2. isc2.org/certifications/cissp/cissp-certification-exam-outline

CISSP Experience Requirements. ISC2. isc2.org/certifications/cissp/cissp-experience-requirements

COBIT. ISACA. isaca.org/resources/cobit

Cotton, S. (2022). *Experience and Qualifications Required for a Chief Information Security Officer: An e-Delphi Study.* University of Phoenix. proquest.com/dissertations-theses/experience-qualifications-required-chief/docview/2725631467/se-2

CRISC. ISACA. isaca.org/credentialing/crisc

CSO Online. (2008). *Data Breach Fallout: Do CISOs Need Legal Protection?* CSO. csoonline.com/article/522120/metrics-budgets-data-breach-fallout-do-cisos-need-legal-protection.html

De Éminville, M. (2020). *Cybersecurity and decision makers: Data security and digital trust.* John Wiley & Sons, Inc. doi.org/10.1002/9781119720362

Death, D. (2019). *Must-Have Skills for CISOs: A CISOs Connect Report.* Security Current. securitycurrent.com/wp-content/uploads/2019/02/Must-have-skills-for-CISOs-CISOs-Connect-2.pdf

Decreto Legislativo 8 giugno 2001, n. 231 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre

2000, n. 300. (2001). In *Gazzetta Ufficiale della Repubblica Italiana* (year 142, n. 140). gazzettaufficiale.it/eli/gu/2001/06/19/140/sg/pdf

Decreto-Legge 14 giugno 2021, n. 82 - Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. (2021). In *Gazzetta Ufficiale della Repubblica Italiana* (year 162, n. 140). gazzettaufficiale.it/eli/gu/2021/06/14/140/sg/pdf

Directive (EU) 2022/2555 of the European Parliament and of the Council [Of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)]. (2022). In *Official Journal of the European Union.* eur-lex.europa.eu/eli/dir/2022/2555/oj

Ellis, A. (2022). *CISOs are still chiefs in name only.* CSO. proquest.com/trade-journals/cisos-are-still-chiefs-name-only/docview/2637032524/se-2

Espinosa, C. *A CISO Isn't a Technical Role.* The Secure Blog. christianespinosa.com/blog/a-ciso-isnt-a-technical-role/

European Commission. (2021). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.* eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

European Commission. (2022). *Proposal for a Regulation of the European Parliament and of The Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.* eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

Evdokimov, A. (2018). *What it takes to be a CISO: Success and leadership in corporate IT security.* Kaspersky daily. kaspersky.com/blog/ciso-report/24288/

Foundry. (2023). *Security Priorities Study 2023. The security leader's ongoing battle for cyber resilience.* IDG, Inc. resources.foundryco.com/download/security-priorities-executive-summary

Fox, J. (2023). *Top Cybersecurity Statistics for 2024.* Cobalt. cobalt.io/blog/cybersecurity-statistics-2024

Fruhlinger, J. (2018). *What is network security? Definition, methods, jobs & salaries.* CSO. proquest.com/trade-journals/what-is-network-security-definition-methods-jobs/docview/2063502064/se-2

Fruhlinger, J. (2021a). *CRISC certification: Your ticket to the C-suite?* CSO. proquest.com/trade-journals/crisc-certification-your-ticket-c-suite/docview/2574930565/se-2

Fruhlinger, J. (2021b). *Does it matter who the CISO reports to?* CSO. csoonline.com/article/565560/does-it-matter-who-the-ciso-reports-to.html

Garrie, D. (2015). *Do CIOs and CISOs Get Covered in Cybersecurity Litigation?* Bloomberg Law. news.bloomberglaw.com/business-and-practice/do-cios-and-cisos-get-covered-in-cybersecurity-litigation

Hale, J. (2014). Affecting the C-Suite. In *SC Magazine* (vol. 25, fasc. 6, pp. 16-19). proquest.com/trade-journals/affecting-c-suite/docview/1545532914/se-2?accountid=9652

Hale, R. (2017). Cyber Competencies and the Cybersecurity Officer. In *The Cyber Risk Handbook* (pp. 359–368). John Wiley & Sons, Inc. doi.org/10.1002/9781119309741

Hill, M. (2023). *Cybersecurity workforce shortage reaches 4 million despite significant recruitment drive.* CSO. csoonline.com/article/657598/cybersecurity-workforce-shortage-reaches-4-million-despite-significant-recruitment-drive.html

Hitch Partners. (2023). *CISO Security Leadership Survey Results.* Hitch Partners. hitchpartners.com/ciso-security-leadership-survey-results-23

IANS Research. (2023). *Trends in Executive Development & Certifications for CISOs.* IANS. iansresearch.com/resources/all-blogs/post/security-blog/2023/03/02/trends-in-executive-development-certifications-for-cisos

Inskeep, T. (2019). How to Properly Position the CISO for Success. In *SecurityMagazine* (vol. 56, fasc. 5, pp. 36-37). proquest.com/trade-journals/how-properly-position-ciso-success/docview/2229574304/se-2

ISO 22301:2019. ISO. iso.org/standard/75106.html

ISO 9001:2015. ISO. iso.org/standard/62085.html

ISO/IEC 27001:2022. ISO. iso.org/standard/27001

ITIL. Axelos. axelos.com/certifications/itil-service-management

Karanja, E., Rosso, M. A. (2017). The Chief Information Security Officer: An Exploratory Study. In *Journal of International Technology and Information Management* (vol. 26, no. 2, pp. 23-47). proquest.com/scholarly-journals/chief-information-security-officer-exploratory/docview/1981610373/se-2

Kayworth, T., Whitten, D. (2012). *Effective Information Security Requires a Balance of Social and Technology Factors.* Mays Business School Texas A&M University. ssrn.com/abstract=2058035

Kosutic, D. (2022). *What is ISO 27001? A quick and easy explanation.* Advisera. advisera.com/27001academy/what-is-iso-27001/

Maloney, S. (2016). *Bridging the Communications Gap between the CISO and the Board.* Cybereason. cybereason.com/blog/blog-bridging-the-communications-gap-between-the-ciso-and-the-board-2

Michielsen, C. (2023). *ECJ further shapes independent position of DPOs.* Stibbe. stibbe.com/publications-and-insights/ecj-further-shapes-independent-position-of-dpos

Mitchell, S. (2007). GRC360: A framework to help organizations drive principled performance. In *International Journal of Disclosure and Governance* (vol. 4, pp. 279-296). doi.org/10.1057/palgrave.jdg.2050066

Mohan, V. (2023). *ISO 27001 Certification: Complete Guide.* Sprinto. sprinto.com/blog/iso-27001-certification/

Muller, R. (2008). *Looming IT talent shortage.* MYBROADBAND. mybroadband.co.za/news/technology/2816-looming-it-talent-shortage.html

NIST. *NIST Cybersecurity Framework.* U.S. Department of Commerce. nist.gov/cyberframework/getting-started

Office of the Federal Register, National Archives and Records Administration. (2017). *82 FR 22391 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* Office of the Federal Register, National Archives and Records Administration. govinfo.gov/app/details/FR-2017-05-16/2017-10004

Oltsik, J. (2016). *The truth about cybersecurity certifications.* Network World. proquest.com/trade-journals/truth-about-cybersecurity-certifications/docview/1828013224/se-2

Oltsik, J. (2023). *The Life and Times of Cybersecurity Professionals, Volume VI.* Enterprise Strategy Group. techtarget.com/esg-global/wp-content/uploads/2024/01/Complete-Survey-Results-Cybersecurity-Professionals.pdf

Osborne, M. (2006). The Security Organization. In *How to Cheat at Managing Information Security* (pp. 2-6). Elsevier, Inc. doi.org/10.1016/B978-159749110-5/50008-7

OWASP Cybersecurity Certification. OWASP. owasp.org/www-project-cybersecurity-certification-course/

Puetz, N., Abdelkader, F. (2022). *C-Suite Shuffle: The CISO's Evolving Role and Reporting Structure.* CSO. csoonline.com/article/572253/c-suite-shuffle-the-ciso-s-evolving-role-and-reporting-structure.html

Regulation (EU) 2016/679 of the European Parliament and of the Council [Of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)]. (2016). In *Official Journal of the European Union.* eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2022/868 of the European Parliament and of the Council [Of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)]. (2022). In *Official Journal of the European Union.* eur-lex.europa.eu/eli/reg/2022/868/oj

Regulation (EU) 2023/2854 of the European Parliament and of the Council [Of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)]. (2023). In *Official Journal of the European Union.* eur-lex.europa.eu/eli/reg/2023/2854/oj

Richardson, M. A. (2022). *CCISO vs. CISSP: Which Certification Is Best For Aspiring CISOs?* Spiceworks. spiceworks.com/tech/it-careers-skills/articles/cciso-vs-cissp/

Saltzer, J. H., Schroeder, M. D. (1975). The Protection of Information in Computer Systems. In *Proceedings of the IEEE* (vol. 63, no. 9, pp. 1278-1308). ieeexplore.ieee.org/document/1451869

Sharma, S. (2019). *Data Privacy and GDPR Handbook.* Wiley. doi.org/10.1002/9781119594307

Shayo, C., Lin, F. (2019). An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function. In *Journal of Computer Science and Information Technology* (vol. 7, no. 1, pp. 1-20). doi.org/10.15640/jcsit.v6n2a1

Siponen M. T., Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions. In *The DATA BASE for Advances in Information Systems* (pp. 60-80). doi.org/10.1145/1216218.1216224

Siponen, M. T. (2005). An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. In *European Journal of Information Systems* (pp. 303-315). doi.org/10.1057/palgrave.ejis.3000537

Smit, R., Hagedoorn, J. M.J. v. Y., Versteeg, P., Ravesteijn, P. (2021). The Soft Skills Business Demands of the Chief Information Security Officer. In *Journal of International Technology and Information Management, Suppl.Special Edition - Conference Proceedings 2021* (vol. 30, fasc. 4, pp. 41-61). International Information Management Association. proquest.com/scholarly-journals/soft-skills-business-demands-chief-information/docview/2619484533/se-2

SSAE 18. AICPA. us.aicpa.org/content/dam/aicpa/research/standards /auditattest/downloadabledocuments/ssae-no-18.pdf

StationX Team. (2024). *How Much Do Cyber Security Certifications Cost?* StationX. stationx.net/cyber-security-certifications-cost/

Stone, M., Irrechukwu, C., Perper, H., Wynne, D., Kauffman, L. (2018). *IT Asset Management. NIST Special Publication 1800-5.* National Institute of Standards and Technology. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf

Stupp, C. (2019). *CISOs Emerge From CIOs' Shadow.* WSJ Pro. proquest.com/trade-journals/cisos-emerge-cios-shadow-more-companies-are/docview/2330043348/se-2

Swinhoe, D. (2020). *How CISOs and data privacy officers should work together.* CSO Online. csoonline.com/article/569103/how-cisos-and-data-privacy-officers-should-work-together.html

The Institute of Internal Auditors. (2020). *The IIA's Three Lines Model.* IIA. theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

U.S. Attorney's Office, Northern District of California. (2022). *Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records.* U.S. Department of Justice. justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach

U.S. Securities and Exchange Commission. (2023). *SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures.* U.S. Securities and Exchange Commission. sec.gov/news/press-release/2023-227

US state CISOs lacking in security certificates. (2006). In *Computer Fraud & Security.* doi.org/10.1016/S1361-3723(06)70426-2

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. In *Computer Law & Security Review* (vol. 52). doi.org/10.1016/j.clsr.2023.105890

Warsinkse, J. (2019). Security Architecture and Engineering. In *CISSP: Certified Information Systems Security Professional* (pp. 213-362). John Wiley & Sons, Inc. doi.org/10.1002/9781119423300

Watkins, S. (2022). *ISO/IEC 27001:2022 : An Introduction to Information Security and the ISMS Standard.* ITGP. doi.org/10.2307/j.ctt5hh3wf

Weishäupl, E., Yasasin, E., Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. In *Computers & Security* (vol. 77, pp. 807-823). doi.org/10.1016/j.cose.2018.02.001

Worstell, K.F. (2014). The Role of the CISO. In *Computer Security Handbook* (pp. 65.1-20). John Wiley & Sons, Inc. doi.org/10.1002/9781118851678

Wynn, B. (2005). Repositioning the CISO. In *Security Technology & Design* (vol. 15, fasc. 7, pp. 62-63). proquest.com/magazines/repositioning-ciso/docview/232154977/se-2

Yvon, T. (2020). *Exploring Factors Limiting Implementation of the National Institute of Standards and Technology Cybersecurity Framework.* Colorado Technical University. proquest.com/docview/2435199859?sourcetype=Dissertations%20&%20Theses

Acknowledgements

Prima di tutto, voglio ringraziare il Prof. Gabriele D'Angelo e il Dott. Alessandro Leone, insieme al team GT Digital, per i loro insegnamenti e il loro supporto durante il tirocinio e la stesura di questa tesi.

Voglio fare un ringraziamento speciale alle persone del mio cuore, a cui spero arrivi pienamente tutto l'amore che ho.
Ai miei amici più cari, specialmente a coloro che hanno contribuito a trasformare Cesena nella mia seconda casa; ai miei zii e alle mie splendide cugine; ai miei nonni: siete i perenni cheerleader della mia vita, il mio pilastro. Mi amate esattamente per quella che sono e con le vostre coccole mi fate sentire amata e so che continuerete a farlo per sempre.
A mia mamma, mio papà, mio fratello e mia sorella, che con i loro sacrifici mi hanno supportato e sorretto in questo percorso: che famiglia meravigliosa che siamo. Siete e sarete sempre la mia ricchezza più grande.

Infine, voglio fare un piccolo ringraziamento anche a me. Qualche anno fa, guardando una foto di me piccolina, mi sono promessa che sarei tornata ad essere quella bambina allegra e sorridente. Oggi, con la grazia di Dio, sono così felice che se ci penso mi vengono le lacrime agli occhi.
A chi, per caso, si sta ritrovando a spulciare questi ringraziamenti e non sta passando un momento facile, voglio dire: abbiate fede perché, ve lo giuro, ritornerà la primavera.