IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/43ISM/2024/4323024/
Vol. 2024 (1), Article ID 4323024

Is the Chief Information Security Officer an Orchestra Conductor or a Concertmaster? Qualitative research from France*

Daniel LANG

Institut Mines-Telecom Business School
9, rue Charles Fourier, 91011, Evry Cedex, France

Correspondence should be addressed to: Daniel LANG, daniel.lang@imt-bs.eu

* Presented at the 43th IBIMA International Conference, 26-27 June 2024, Madrid, Spain.

Abstract

As companies become increasingly global and Internet based, information security has become a critical issue for organizations. To face these new threats, the position of Chief Information Security Officer (CISO) has emerged in many companies. We aim to study this new career and determine its current scope of actions and seek to investigate this new profession in terms of roles, tasks and competencies. This study relies on a qualitative questioning methodology, with structured face-to-face interviews in France. Despite many contributions on security risk management, there is limited research on the CISO profession. The CISO needs many skills, competencies, and carries out a range of tasks.

This research investigates the role, tasks, competencies, skills and levels of autonomy of CISOs in various organizational settings. It provides an understanding of the CISO profession and organizational involvement. The results could be useful for recruitment, training and career planning of CISOs.

Keywords Security practices, CISO, profile, cyber security

Introduction

This contribution elucidates the contemporary digital landscape that organizations navigate. It underscores the imperative integration of emerging technological trends within corporate strategies to bolster performance and operational efficiency. This digital evolution encompasses the adoption of social media, Web 2.0 tools, Internet of Things (IoT), Bring Your Own Device (BYOD) policies, and cloud computing solutions, aiming to sustain productivity and quality amidst increasing work mobility and flexibility.

This digital proliferation necessitates robust information system security to safeguard data integrity, confidentiality, and availability. The paper sets its sights on exploring the evolving role of the Chief Information Security Officer (CISO), probing into the profession's scope, responsibilities, and competencies amidst the digital transformation era.

Through a meticulous examination of existing literature on key executive roles such as the Chief Information Officer (CIO) and the Chief Executive Officer (CEO), and their interplay with information security practices, the study aims to fill a research void. It analyzes the predominant focus on technological solutions for security challenges, advocating for a balanced emphasis on organizational processes and user compliance to foster a secure IT environment. This approach underscores the pivotal role of CISOs in cultivating a security-conscious culture within organizations.

Employing a qualitative research methodology, the paper details the findings from 17 interviews conducted across French organizations, aimed at delineating the multifaceted role of CISOs. This inquiry sheds light on the

Cite this Article as: Daniel LANG, Vol. 2024 (1) "Is the Chief Information Security Officer an Orchestra Conductor or a Concertmaster? Qualitative research from France " Communications of International Proceedings, Vol. 2024 (1), Article ID 4323024, https://doi.org/10.5171/2024.4323024

professionals' duties, autonomy, competencies, and their integration within organizational hierarchies, offering insights into their contribution towards strategic information security management.

In essence, the study endeavors to enhance our comprehension of the CISO's position within the corporate echelon, their instrumental role in shaping security protocols, and the requisite skills and educational backgrounds pivotal for the role. By dissecting the missions, hierarchical dynamics, and qualifications of CISOs, particularly within the French corporate context, the research aspires to contribute significantly to the discourse on information security leadership, with implications for recruitment, training, and career progression in this critical field.

Literature Review

Information Security

Computing is omnipresent in our society, as the Internet and other networks have become essential. All objects, in our daily lives, are currently or will soon be equipped with microchips. These technologies can communicate amongst themselves digitally and are applied to a large range of fields: such as communications (cell phones), transportation (GPS), business, medicine (imagery, robotic assistance) and the environment (powering car motors).

Nevertheless, as soon as information can be stored and transmitted, its protection becomes necessary. Centuries ago, Julius Caesar transformed readable text into a coded document using cryptography. However, criminals have always tried to get around these means of protection. Today, the information space generated by information and communication technologies (ICT) is giving rise to a new form of delinquency: cybercrime. The many persistent attacks and ransomware suggest that threats to the security of information systems continue to evolve at a frantic pace (Li Yuchong and Liu Qinghui, 2021). The consequences can be particularly serious for companies, countries and citizens.

At the same time, the profile of attackers has evolved from that of a "highwayman", to the technology lover who wants to show off his or her exploits bypassing the authentication process, right up to the professional hacker seeking to steal confidential information for financial gain (Webb et al., 2017). Today the concept of a cyber-war is not only a potential subject, but also a reality (Ring, 2013). This includes highly organized groups or countries that intend to attack at the State level (Schiavone et al., 2014).

These offenses are not limited to intrusion and data theft (viruses, online fraud) but also relate to their content (insults, xenophobia and pedophilia) and it is necessary to take into consideration copyright and intellectual property (text, music, video, software). In addition, the risks are not limited to fraudulent intentions but also to accidents such as improper use or natural events (fire, earthquake). The dysfunctions can affect one or several of the three principal components of an information system:

- Infrastructures and technical skills (servers, networks, material …),
- Software-related (application software),
- User practices.

It is therefore the totality of potential threats, which must be taken into account. For example, a flood in the computer room can leave the server storing accounting software unusable. Considering the growing dependency of organizations on their IS, companies need to consider inferred risks (Kraemer et al., 2009) as a partial or total dysfunction can weaken an organization. Some data, whether it concerns employees, suppliers or clients, are confidential, and any loss or alteration would lead to very serious damage. Moreover, in a context of high competitiveness, information represents value that can lead to greed and incite theft.

As a result, companies are putting into place security strategies that are adapted to protect their information capital (Karanja & Rosso, 2017). In fact, information capital has become a raw material without which companies cannot do business. Initially the security process was often perceived as solutions emanating from technical tools, and so was delegated to technological staff. Nevertheless, this restrictive vision is evolving, since risks involved do not only concern material aspects, but also legal aspects, loss of confidence and financial repercussions (Mc Adams, 2004). It is now recognized that management's role is fundamental in putting into place a security culture and policy (Solms & Solms, 2004). Information protection depends on change management, especially persuading employees of the need

to behave in a secure manner (Ashenden & Sasse, 2013) and developing a security policy addressing the three following components: humans, processes, technology.

Some experts assert that the level of security sought, must be proportional to the value of the information and to the financial losses that would follow an information capital dysfunction. It is also necessary to nuance this assertion by taking into account the company's sector of activity. Thus, a hospital's charter specifies that its main objective is first to care for the ill in priority and second to manage its financial flows. However, in all cases, information security is a strategic issue, which must be managed by decision-makers who must define its mission, goals and objectives.

Solms and Solms (2004) highlight the fact that organizations must consider the protection of information as an organizational problem (Ashenden & Sasse, 2013) whose components are the following elements: corporate governance, organizational policy, ethics, law, humans, technology, auditing, maturity, conscience. A fundamental principle in the implementation of a security policy concerns the individual perception of risks by the actors involved and the way in which they consider what constitutes a barrier to security (Musekura, 2003). One way to improve this perception consists in investing in training and raising awareness among all employees in view of developing a security culture within the organization. Albrechtsen's research (2007) suggests that users want a "user-involving approach" to security awareness and that "mass media-based awareness" campaigns, have, according to the interviewed users, no significant long-term effects on users' behavior and awareness. In addition, we argue that the presence of IT security experts on a steering committee is a significant advantage, as they can inform the rest of the committee about cybersecurity risks. The CISO acts as liaison between the IT department and the board of directors on issues related to cybercrime. He or she must understand where the company information is at all times and avoid unauthorized access.

Professional Roles

The delineation between the terms "profession" and "occupation" emerges distinctly within the scholarly discourse, with "profession" acquiring a substantive value when it encapsulates a recognized status and symbolic designation (Friedson, 2001). The academic terrain is rich with analyses on professions, setting a foundational backdrop to explore the classification of Information Technology (IT) professions as proposed by Beynon-Davies (2016).

The term "occupation" embodies a conglomerate of activities and social roles within an organization, translating into specific tasks (Friedson, 2001). In contrast, a "profession" signifies an organized collective where members share an identity, consensus, and a regulatory framework for their practice (Larson, 1979). The transition from an occupation to a profession, or "professionalization," denotes a group's capacity to monopolize certain services, thereby excluding others from practice. This process is illustrated historically through the evolution of medicine into a recognized profession in the early 19th century, marked by the establishment of legal and ethical standards to delineate qualified practitioners (Kou & Gray, 2018).

The discourse extends to the requisite skills, knowledge, and competencies essential for IT professionals, underscoring the intricate relationship between competencies and practical skills (Gallagher et al., 2011; Sonteya & Seymour, 2012). The paper posits that addressing the scarcity of qualified Information Systems security personnel necessitates establishing a more defined and recognized professional community within IT security, characterized by clear job roles, career pathways, and a regulatory body.

Palmer et al. (2021) enumerate both technical and managerial skills vital for network security engineers, advocating for comprehensive training in IT, information security, and related fields. Furthermore, the Cybersecurity Workforce Skills Report (University of Phoenix & (ISC) Foundation, 2014) calls for the standardization of a professional skills set aligned with industry demands to bridge the gap between existing skills, practical experience, and the dynamic nature of security threats.

As the landscape of information security risks expands, the role of the Chief Information Security Officer (CISO) has evolved in response to these challenges, necessitating adherence to emerging standards such as Basel II or ISO 2700x. Unlike professions with statutory protection, such as medicine or law, the field of IT security, and specifically the role of the CISO, often lacks formal regulatory defense, underscoring the necessity for professional recognition and regulation within this domain. This exploration into the professionalization of IT security roles highlights the imperative for a structured approach to skill development, certification, and regulatory oversight to meet the escalating demands of information security in the digital age.

The CISO: full-time or part time position?

Some authors (Shayo C. & Lin F., 2019) have opted for the term "CISO functions". Others lean more specifically towards a separate profession. Information security can sometimes be assigned to an employee who is also responsible for other very different tasks, depending on the type and the size of the company. In this case, information security becomes a function amongst others rather than a professional role.

The CISO's mission

Globally, the CISO's mission (Kovacich G. L., 2016) is:

- Define the general security policy of the company
- Risk management
- Advise on the security of IS projects
- Check regulatory compliance
- Business continuity/disaster recovery
- Test solutions

His or her mission is to ensure the information system security of the company by taking into account fundamental criteria: integrity, confidentiality, continuity. His or her most important task is to define the company's level/need of security. However, the task that takes up the most time is that of following-up IS projects in the company.

According to the company's sector of activity, the CISO must put standards into place, be an advisory force, formalize standards/guides/recommendations, drive security, and watch over the protection of intellectual property. The CISO intervenes all throughout an IS project, at the level of analysis, when deciding the means to implement IS and finally verifying that the security solution is in place.

To achieve their mission, CISOs carry out both operational and managerial tasks (Ahmad A. et al., 2014).

The CISO's autonomy

The hierarchical position of the CISO and his or her budgetary autonomy are indicators that can illustrate some independence with regards to IS management (Colette R & Gentile M., 2006). Experts in the IS security field have expressed their opinion on this subject as follows:

"The CISO contributes in a transversal manner to all information systems in the company, from an organizational and technical point of view, in synergy with different heads. It is generally accepted that the CISO, for reasons of independence and efficiency, must be placed at a high level of hierarchy (ex. associated to head office) and dispose of a specific budget".

The ideal skills and capacities of the CISO

The CISO must be able to explain IS security constraints in simple terms to individuals who are far removed from technical aspects (functional management). Moreover, he or she must be technically well informed in order to implement adapted solutions and to be able to interact with operational IS employees. The CISO also has to have legal notions since he will have to comply with international norms and certifications.

Wunderlich & al. (2017), proposed a non-exhaustive list of the skills that a CISO must possess

- Good communicator
- Good sense of policy/strategy
- Ability to synthesize and make abstractions
- Capacity to integrate technical skills into professional actions
- Sense of organization
- Capacity to adapt
- Pedagogical skills and ability to make information easily comprehensible

- Good listener
- Knowledge of key technical and functional concepts

Since the 1970s, the traditional model of professions based on qualifications has been challenged and a model based on skills has grown in importance (Paradeise & Lichtenberger, 2001). The traditional model sees jobs as corresponding to a type of qualification. However, there has been a growing demand for more flexibility, which no longer depends upon a regime of certifications. Skill is considered a combination of knowledge, expertise, experience and behaviors.

Research Methodology

The study aims to dissect the professional landscape of CISOs, probing into their positional dynamics, roles, managerial and technical obligations, autonomy, functions, communicative responsibilities, and educational backgrounds. Employing a phenomenological approach as proposed by Moustakas (1994), the research leverages Interpretative Phenomenological Analysis (IPA) to delve into the lived experiences of Information Systems security professionals. This qualitative methodological choice is predicated on the necessity to explore the nuanced contours of this relatively nascent profession, particularly within the French context.

Methodology used

The research invokes the principles of phenomenology, an approach that seeks to capture phenomena as directly experienced by individuals, to scrutinize the professional experiences of Information Systems security professionals. Through semi-structured interviews, the study aims to elicit rich, detailed narratives that illuminate the professional challenges and technological threats these professionals navigate. The methodological rigour is maintained through a meticulous adherence to the four procedural steps of phenomenological research as outlined by Moustakas (1994), with a particular emphasis on maintaining an open, non-judgmental stance by the researcher—a process termed 'epochal'. The researcher does not interpret what he or she is studying from his or her own benchmarks and norms, but allows the phenomenon to reveal itself, to come to him or her (Tompkins L., Eatough V., 2010). This bracketed approach is the condition of rigor of the method. By forbidding any judgment of values, meaning or nonsense, the epoch is a conversion of the gaze into a spectator gaze. Thus, the epochal makes phenomenology a method that is essentially based on listening to the narrative of the other, who, by speaking, reveals his lived phenomenon. In this perspective, the lived experience of the actors in charge of IS security can be seen as revealing the profile and qualities necessary for these actors.

Data Collection

The participant pool comprised Information Systems security professionals across various sectors in France, including 13 CISOs from large enterprises (banking, insurance, food processing, aeronautics, automotive...), and 4 from small to medium-sized businesses(consulting, education…). A total of 17 interviews were conducted, drawing participants from a targeted sampling strategy utilizing the university's alumni directory among other resources. These interviews spanned diverse sectors such as aeronautics, automotive, banking, insurance, media, and government, with an anonymity clause to protect the identities and sensitive information related to their organizations.

Data was meticulously collected through phenomenological interviews and transcribed verbatim, with the NVivo tool employed for data organization and analysis. This process, spread over nine months, culminated in an extensive analysis phase where emerging themes were identified and linked across interviews, revealing the unique and collective experiences of CISOs in their professional milieu.

The study's questionnaire can be found in Appendix A and contains twenty-five questions (14 general questions about the company and 11 specific questions about CISO's business). Semi-structured interviews were used because they are the most commonly used method for qualitative research on information systems (Myers, 2013) and allow the researcher to explore and clarify sensitive issues. This questionnaire served as a guideline for the exchange with the interviewee, knowing that in the framework of an IPA research method, the main objective is to get the interviewee to speak and to listen and analyze the person's feelings. From August to December 2023, we conducted 17 face-to-face interviews in France, focused on roles and competencies of CISOs. Crouch and McKenzie (2006) agree with this approach and cite other authors who argue that in real life inductive research, a small number of interviews can improve the quality of the research results. Their value comes from the analysis and explanations provided rather than from generalization.

This method of collecting data to analyze the role of the CISO may be suitable for qualitative research, as the in-depth data collected often reveals a wide range of topics from a small number of interviews. The average length of interviews was 38 minutes. These interviews analyzed the different tasks of the CISOs, and in particular, security awareness programs, to explore this important communication channel between CISOs and end-users.

Discussions and Analysis of Findings

Descriptive Questionnaire Results

The position, title, hierarchical link and the type of job of a CISO

Our sample included 13 large companies (76.47%) among the 17 actors interviewed.
The CISO position is a full-time job for 11 (64.7%) of our all questionnaire respondents. (See question 16 in Appendix 1). Questionnaire results to questions 16-17 (see Appendix A) in Table 1 show, that the largest companies have more full-time CISO positions (84.61%) compared to smaller companies.

Table 1: Answers about full-time or part time position and hierarchical relationship

Respondents	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**	**R9**	**R10**	**R11**	**R12**	**R13**	**R14**	**R15**	**R16**	**R17**
Type Business	Large Company	Large Company	Large Company	Large Company	Large Company	Large Company	SME	SME	Large Company	Large Company	Large Company	SME	Large Company	Large Company	Large Company	Large Company	SME
Full-time job?	No	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
If not, what % of your business?	30% to 60%	up to 30%					30% to 60%	30% to 60%	up to 30%			30% to 60%					30% to 60%
Hierarchical link (N+1)?	CEO+ CFO	CIO	CEO	CEO	CIO	CIO	CEO	CIO	CEO	CIO	CEO	CIO	CEO	CEO	CEO	CIO	CIO

Based on the data in Table 1, it would appear that full-time CISO positions in large companies correspond to a more professional role, compared to part-time CISO positions in small companies and could arguably be seen as a job.

The literature on business skills (Palmer & al, 2021) categorizes them into “core business” skills such as communication skills, leadership, creativity, delegation…, skills related to a business process; e.g. marketing, finance, or logistics and organizational skills such as administrative and planning skills.

In terms of skills oriented towards risk management (Omran et al., 2018), they include management, communication, legal aspects, identification and forecasting of risk exposure.
However, they vary according to the type of business; for instance, financial acumen to assess market or credit risk in a financial company; or managing patient safety in healthcare.

In terms of skills for ICT professionals, the literature (Picatoste et al., 2018) have classified job types according to their ICT and business skills.

ICT skills consist of traditional professional computing skills such as Data management and queries, computer programming. In terms of IS security, this means specific technical skills on network applications and hardware.

We can distinguish 3 types of jobs:

Job type 1 emphasizes basic ICT skills, supplemented at the periphery by business skills.
Job type 2 is characteristic of new ICT jobs related to technological developments.
Job type 3 includes jobs where ICT skills are secondary, for example business processes that are managed on a daily basis within the company and with which the CISO interacts regularly; business skills are therefore more important in this category.

Our questionnaire respondents also pointed out that the CISO can also be in contact with other staff such as the Risk Manager, the Control Officer, the Head of Security of Persons and Property, the Business Continuity Manager or even the Security Manager.

There interactions require CISO to combine ICT skills with business skills on a regular basis, indicating that the CISO position corresponds to job type 2. The questionnaire answers to question 15 listed "Chief Information Security Officer" as their job title, as well as "Global Information Security Officer", "Security and Disaster Recovery Manager" and "Information Security & Risk Management Lead", thereby emphasizing the global aspects, the business continuity and the risk management characteristics of information security.

Interviews Findings

Findings about mission and tasks of a CISO

Questionnaire results (questions 20 "What is the role (responsibilities) of the CISO in your company?" see Appendix 1) show the following common tasks per number of respondents. Each respondent offered several answers in order of importance. We selected the top four responses from each interviewee:

Figure 1: Role and responsibilities of the CISO (17 respondents-multiple answers)

The answers to question 20 illustrate the range of tasks some operational (audit and control, training and raising users awareness, implementing security actions, ensuring data security); whilst other tasks are more concerned with the study and analysis of security risk (risk analysis, technological watch, compliance with laws and regulations, recovery action plan). The CISO role also includes strategical level responsibility in defining security policy (14 answers).

It is also interesting to note that 14 (82.35%) respondents are in phase 4 of a risk analysis, the last phase that formulates an action plan to respond to potential threats. However, it is highly probable that this situation is due to many of our respondents working in large organizations, with budgets that can be dedicated to this type of work. As a result, the nature of work performed by the CISO is inevitably linked to the size of the company.

4.2.2 Findings about Skills

Beyond tasks carried out daily, it is interesting to be able to determine the required skills for this position. The questionnaire answers provided to question 22 were classified a skills evaluation analysis grid, as shown in Table 2.

Table 2: Questionnaire respondents' opinions about required skills for a CISO position

(4 answers by respondent)

Skills	Description of skills	Number of answers
Social abilities Total answers: 31	Communication skills (in team, oral and written) Ability to cooperate and work in a team (negotiate and defend idea) Customer orientation (having a sense of service)	16 13 2
Personal skills Total answers: 18	Basic personal skills (analytical and synthesis skills) Responsible behavior (perseverance, being honest) Targeted commitment (respect of specifications, autonomy)	7 9 2
Organizational skills Total answers: 10	Staff management and promotion (managing e team, to be a diplomat) Business Management (developing a vision for the future)	2 8
Professional skills Total answers: 9	General professional skills (mastery of the IT Tools required for the job) Skills specific to the job	8 1

The ability to communicate (16 answers) and to negotiate (13 answers) which are social abilities, illustrates the links with business departments. The CISO must defend his or her ideas before different services that are not necessarily preoccupied with security as a primary objective.

Findings about hierarchical position

Questionnaire results show that 43% of respondents do not have a specific budget for information security (Question 17), thereby contradicting what some practitioners wish for. Table 3 shows the hierarchical position of the CISO in our questionnaire survey:

Table 3: Questionnaire responses about the hierarchical position of the CISO

CEO	CIO
9	**8**

8 CISOs out of a total of 17 respondents (47%) are dependent on the CIO, head of the IS management division. This shows a mixed picture about CISO autonomy, since 9 (53%) depend directly on executive management.

The analysis of our interviews shows two possible organizational charts.

In the first organizational chart, the CISO is directly attached to top management (CEO). (9 interviewees stated this). This allowed interviewees (9) to intervene as IS security advisors in IS management projects.

This organizational chart is especially used by large companies or in sectors of activity where information security is a major stake such as banks or insurance). The CISO intervenes in a portfolio of projects for which s/he supervises the security aspect but is not an integral member of the project team. Based on the analysis of these interviews, we suggest what such an organizational chart looks like in Figure 2.

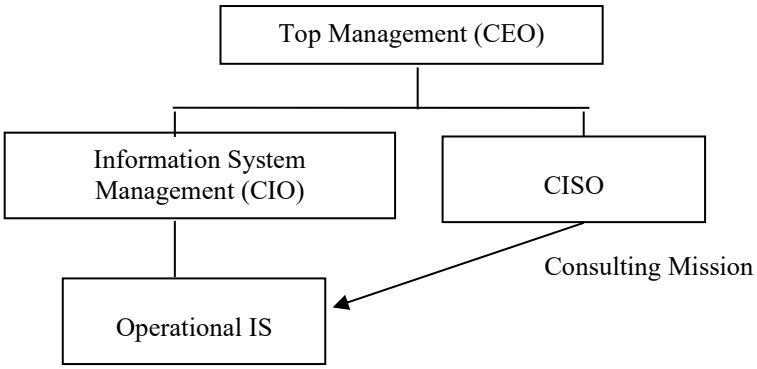

Figure 2: Analysis of interview data: possible organizational chart in large companies

According to other interviewees (8), particularly in all SMEs, the CISO is generally integrated into the IS management division and works with IS project teams.

In other cases, there is no real CISO position: an operational IS employee who is specialized in security acts as a CISO on different projects, but this is not his or her only job. In smaller structures (2) the CISO is associated with the head of quality management or the head of production (in the smaller structures IS security is seen essentially as a technical component). We suggest what the organizational chart of these types of firms, looks like in Figure 3.

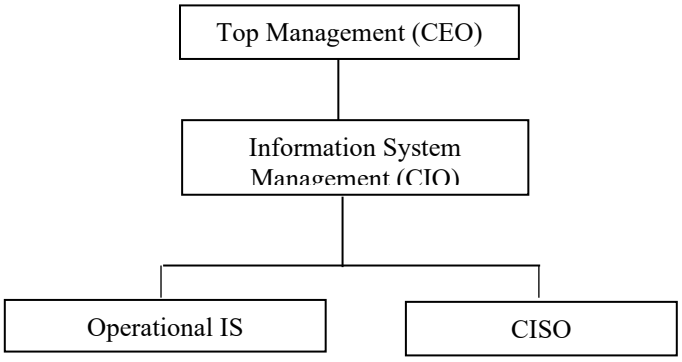

Figure 3: Analysis of interview data: possible organizational chart in SMEs

When the CISO is directly associated with top management, he is more of a manager than a technician. The inverse is true when he or she is integrated into IS management, since he or she is closer to the technical implementation of security in IS projects. In general, the larger the structure or the more the sector of activity is sensitive to security risk, the more often the CISO is associated with the top of the hierarchy, and the less s/he is close to operational aspects. This can be the case of either a position that is mostly operational or a position without any operational component.

Findings about Training and Education

According to a large majority of interviewees (14 respondents), the best training remains learning in the field and practical experience. The majority (82%) of the CISOs we questioned face-to- face hold degrees from engineering schools with a specialization in IS. If they are then specialized in IS security (5 respondents) and have the necessary

experience (9 respondents) they become CISOs. Sometimes the CISO (3 respondents) comes from other departments in the company (e.g. quality control): this allows them to have a good overview of needs.

Focusing on the CISO educational background, the results of the study in France show that:

- 11 (65%) respondents (among 17) have studied in universities or engineering schools
- 3 (18%) respondents (among 17) enrolled in professional courses for technical and methodological training on topics such as standards, ISO 27001, Lead Auditor ITIL v3 Foundations; attended conferences, trade fairs, exchanges with other CISOs; consulted specialized books and magazines; completed certificates such as CISSP (Certified Information Systems Security Professional), attended or took internships/training courses with agencies specialized in IS security

Among 17 respondents, 10 respondents (59%) benefited from professional practical experiences (as security integrator, head of security projects, security developer, security consultant …)

Very few (2 respondents), i.e. 12% our questionnaire respondents had initial training in IS security; their security careers developed from positions as project managers, administrators or consultants. We can probably state that starting from a professional activity involving information production/exploitation, even though it is generally held in low consideration, is an advantage for learning the realities of the IS field.

We formulated several questions to determine what type of training CISOs preferred. However, the results are mixed and do not distinguish clear preferences between general training and more specific short-term specializations. It is not possible to identify the most suitable training and additionally management in different companies does not formally specify their requirements in terms of training. Figure 4 presents the questionnaire answers on this topic.

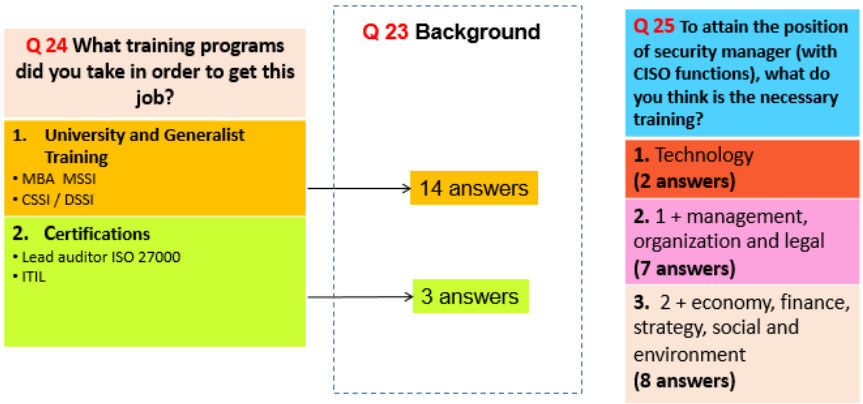

Figure 4: Questionnaire responses on the reputation and content of various training courses

Responses to question 23 show that generalist profiles (14 responses) are widely preferred to highly specialized profiles (3 responses). With respect to "necessary training" (question 25), the trends confirm our analysis in Part 2. Indeed, the CISO must be in a position where he or she can understand the constraints of the various services and departments, which requires knowledge in various fields such as management, organization, legal, economics, finance, etc.

Findings on the human qualities necessary for a CISO

According to a large majority of the CISOs interviewed, 3 qualities are expressed very regularly: listening, conviction and communication. This job requires a great deal of listening to the various actors in the company and a great deal of communication in order to convince them to adopt the actions linked to the proposed Information Systems Security strategy. It is a question of being diplomatic, to implement decisions to increase the level of security at all levels of the company.

To describe the various human qualities needed to become an effective and responsible CISO, we chose to retrieve the responses to question 18 ("What human qualities a CISO should have?") and represent a word cloud allowing us

to see the occurrences of the most frequently suggested qualities. In order to do this, we naturally eliminated manually the words that were not characteristic of the qualities of the CISO's answers.

Figure 5: Word cloud representative of the qualities of a CISO

Conclusion

The escalating cybersecurity risks confronting organizations necessitate the development of nuanced information security strategies that address the dynamic and intricate landscape of information systems (IS) security threats. In response, there is a discernible trend towards the increased recruitment of Chief Information Security Officers (CISOs). These pivotal figures are progressively cementing their roles within executive boardrooms, paralleling the stature of other high-ranking executives, and are playing an increasingly vital role in shaping strategic organizational directions (Alexander & Cummings, 2016).

The primary objective of our study was to shed light on the evolving roles, responsibilities, and competencies of IS security professionals amidst growing technical threats that pose significant security risks. Our findings indicate an urgent need for CISOs to foster robust connections and dialogue with the business sector and other organizational entities to address these escalating risks effectively.

The CISO role is undergoing profound transformation. Beyond possessing comprehensive technical expertise, CISOs are required to excel in communication and negotiate security measures across various departments without the formal authority typically vested in top executive positions. To persuade and align their colleagues with security initiatives, a deep understanding of the business is crucial. Hence, CISOs may not exactly be the conductors of the organizational orchestra but could be likened to 'concertmasters', who, while leading, also play alongside their peers. This analogy encapsulates the multifaceted nature of the CISO's role, which encompasses being a manager, expert, strategist, project leader, guardian, educator, occasionally an administrator, and a researcher, as articulated by Refalo (2003).

For future research, it would be beneficial to undertake a more extensive study, possibly encompassing the entirety of Europe, utilizing questionnaires and conducting in-depth interviews. Such an expanded approach would enhance our comprehension of how the CISO profession is evolving and adapting to emerging technological challenges, such as information privacy and data theft, thereby contributing valuable insights into the progression and adaptation of IS security practices within the contemporary digital milieu.

Annex: questionnaire

	General information	
1.	Name	
2.	First Name	
3.	Job	
4.	Company's Name	
5.	Sector of activity of your company	
6.	Size of your company	
	Company address	
7.	Street	
8.	Postal code	
9.	Town	
10.	Country	
11.	Phone	
12.	Fax	
13.	e-mail	
14.	Website	
	CISO jobs	
15.	Does there exist within your company a CISO job and which is his/her designation?	
16.	Is it a full time job? If not, what is the percentage of activity for this job?	
17.	Who is the CISO's hierarchical superior?	
18.	What human qualities a CISO should have?	
19.	What other functions does the CISO in your company interact with?	
20.	What is the role (responsibilities) of the CISO in your company?	
21.	What are the 5 most important tasks in decreasing order that you look after daily as the CISO?	
22.	What are the required skills for the CISO?	
23.	What background does the CISO in your company come from?	

24.	What training programs did you take in order to get this job?	
25.	In order to attain the position of security manager (with CISO functions), what do you think is the	

Bibliography

- Ahmad A., Maynard S.B. & Park S. (2014). "Information security strategies: Towards an organizational multi-strategy perspective". Journal of Intelligent Manufacturing, 25(2), 357-370.
- Albrechtsen E. (2007) "A qualitative study of users' view on information security", *Computers & Security* 2007, 26:276-289
- Alexander, A., and Cummings, J. (2016) "The Rise of the Chief Information Security Officer" *People & Strategy* (39:1), Winter2016, pp 10-13
- Ashenden, D. & Saase, A. (2013), "CISOs and organisational culture: Their own worst enemy?" *Computers and Security*, volume 39, Part B, nov 2013, p396-405
- Beynon-Davies, P. (2016). "Information Systems Development: an introduction to information systems engineering". Macmillan International Higher Education.
- Crouch, M. & McKenzie, H. (2006) "The logic of small samples in interview-based qualitative research", *Social Science Information*, Sage 45(4), pp. 483-499
- Friedson, E. (2001). Professionalism, the third logic: On the practice of knowledge. University of Chicago press.
- Gallagher, K. P., Goles, T., Hawk, S., Simon, J. C., Kaiser, K. M., Beath, C. M. and Martz Jr, W. B. 2011. A Typology of Requisite Skills for Information Technology Professionals, In HICSS 2011, Hawaii International Conference on System Sciences, 1--10
- Karanja, E. and Rosso, M.A. (2017) "The Chief Information Security Officer: An Exploratory Study," *Journal of International Technology and Information Management*: Vol. 26:Iss. 2, Article 2.
- Kraemer S, Caryon P, Clem J, (2009) "Human and organizational factors in computer and information security: pathways to vulnerabilities," *Computers and Security* 2009
- Kou Y., Gray C.M. (2018). "Towards professionalization in an online community of emerging occupation: Discourses among UX practitioners". In Proceedings of the 2018 ACM Conference on Supporting Groupwork (pp. 322-334).
- Kovacich G. L., (2016). The Information Systems Security Officer's Guide: Establishing and Managing a Cyber Security Program, Butterworth-Heinemann, 12 janv. 2016
- Larson, M. S., & Larson, M. S. (1979). The rise of professionalism: A sociological analysis (Vol. 233). Univ of California Press.
- Li Yuchong, Liu Qinghui, (2021), « A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 2021,
- Moustakas, C. (1994). "Phenomenological research methods". Thousand Oaks, CA: Sage
- Musekura JB., Ekh R (2003) "Information security issues – difference between perception and practice in organizations", Orebro University, Sweden

- Myers, M.D. (2013) *Qualitative Research in Business & Management*. 2nd Edition, Sage Publications, London.
- Omran A., Abu-Bakara A., Abdul Manab N., & NizamAhmada, S. (2018). Developing a competency model for chief risk officers in Malaysia. Proceedings of NHRMC 2018.
- Palmer, A., Rothschild, M., & Ang, B. (2021). Successful cyber-risk management of operational technology and industrial control systems-technical and policy recommendations.
- Paradeise C., Lichtenberger Y. (2001). "Compétence, compétences". Sociologie du travail, 43(1), 33-48.
- Picatoste J., Pérez-Ortiz L., Ruesga-Benito S.M. (2018). A new educational pattern in response to new technologies and sustainable development. Enlightening ICT skills for youth employability in the European Union. *Telematics and Informatics, 35(4), 1031-1038*
- Refalo, P-L. (2003), « La fin du RSSI », *L'informatique Professionnelle*, 215 – juin-juillet 2003, p41
- Ring T. (2013), « IT Megatrends: the security impact", *Network Security*, volume 2013, Issue 7, July 2013, p5-8
- Schiavone, S., Garg, L., and Summers, K. 2014. "Ontology of Information Security in Enterprises," *Electronic Journal Information Systems Evaluation* Volume (17:1)
- Shayo C. and Lin F. (2019) "An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function" Journal of Computer Science and Information Technology June *2019, Vol. 7, No. 1, pp. 1-20*
- Solms B, Solms R, (2004) "The 10 deadly sins of information security" *Computers and Security Volume 23, Issue 5, July 2004, Pages 371-376*
- Sonteya, T. and Seymour, L. 2012. Towards an Understanding of the Business Process Analyst: An Analysis of Competencies. Journal of Information Technology Education: Research, 11(1), 43--63
- University of Phoenix, & (ISC)2 Foundation. (2014). Cybersecurity Workforce Competencies: Preparing tomorrow's risk-ready professionals (p. 16)
- Webb, J., Ahmad, A., Maynard, S.B., Baskerville, R., and Shanks, G. 2017. "Organizational Security Learning from Incident Response," in: *International Conference On Information Systems (ICIS)*. Seoul, South Korea: p. 11.
- Wunderlich N. and Beck R. (2017), "25 Years of CIO and IT Leadership - Revisiting Managerial Roles in Information System Research". PACIS 2017 Proceedings. 236.