EUROPEAN CYBER SECURITY ORGANISATION

SURVEY ANALYSIS REPORT

Chief Information Security Officers' (CISO) Challenges & Priorities

Users Committee

APRIL 2021

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use contact nina.hasratyan@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

This document will be continuously updated based on developments within the sector and ECSO members' input.

Copyright Notice

ABOUT THE USERS COMMITTEE

In September 2018, ECSO created its Users Committee (UC), a European transversal (cross-border and cross-sector) committee where Users and Operators of Essential Services (OES) can share sensitive information and strategic intelligence on cyber threats in a confidential and trusted way. In 2021, the UC is set to evolve into a pyramidal structure, representing at the top CISOs of Users/Operators, in the middle the European CISO community, and at the bottom, the Community of Verticals where Users/Operators can establish an ongoing dialogue with suppliers and providers.

The UC members are restricted to a network of European Chief Information Security Officers (CISOs) (or equivalent) who provide strategic suggestions from a private sector and strategic operational perspective in order to tackle current and future challenges and needs for the cybersecurity solutions providers (CSSP) and more widely the cybersecurity market.

Indeed, it is our understanding and approach that Users and OES are the drivers of all activity on the European cybersecurity and digital market, and while a dialogue with the public sector already exists, often at the national level, a complementary dialogue with the private sector is also necessary to create a direct impact at the European level. Users/OES are key actors in the field of cybersecurity, especially since CSSP (the offer) can only offer tailored products based on the needs expressed by the Users/OES themselves (the demand).

Based on these elements, the UC has a quadruple approach to its portfolio of activities:

- ✓ A network of European CISOs (or equivalent) across sectors and across borders
- ✓ An open forum of exchange and discussions for lessons learned and best practices
- ✓ A trusted and confidential environment for strategic intelligence sharing among peers
- ✓ Understanding of the needs, requirements, and challenges of a CISO and conveying these messages to the right actors

TABLE OF CONTENTS

Executive summary

This report summarises and analyses the results of an EU-wide survey run by the European Cyber Security Organisation (ECSO) from November 2020 to January 2021, targeting Chief Information Security Officers (CISOs) or equivalent, from all over Europe and from all sectors. The results are divided into 4 major sections.

The first section covers the different elements of the survey presented to the CISOs and the adopted methodology in reaching out to them. The survey questions were divided into 7 sections pertaining to the different aspects of the daily job and responsibilities of a CISO: General / The work of a CISO; Board investment / Business continuity; Information sharing – Threat intelligence – Crisis management; Certification; Authentication; Liability & Governance; European, Regulatory & Cross-sector aspects. The sections and questions aimed to show that the role of a CISO goes beyond the purely technical prerequisites that may primarily come to mind.

The second section provides some statistics relating to the representation of the respondents' professional certifications, job positions, and sectors. One of the key observations are that the CISOs' position is not a harmonised or universally implemented role in every sector, company, and organisation. In addition, professional certification is not a universally agreed upon topic either as the degree and number of certifications held by CISOs, as well as the importance given to certification, varies a lot from sector to sector.

The third section deep-dives into a sector-by-sector analysis of the different survey elements. For each sector, we have highlighted the major threats targeting them, cybersecurity challenges that they are encountering, but also in-company challenges that CISOs encounter on a daily basis, as well as the regulatory and international cooperation aspects. The covered sectors are energy, finance, food, health, industry/manufacturing, public sector/government, telecommunications, transportation (air – rail – sea – road – space), and utilities (water). There was also an "other" category that contained unique entries from "luxury", "retail" and "consultancy services covering different sectors".

Finally, the fourth section provides cross-sector recommendations stemming from the common messages identified in the vertical approach.

- *On CISOs Roles and Responsibilities*: CISOs must be given the weight to implement their decisions with the necessary resources, through involvement in their organisation's strategy and with a direct channel of communication to their Boards. One of the suggested ways to achieve this is to allow CISOs to directly sit at their Boards with defined legal responsibilities. In turn, CISOs need to learn to report to their Boards by quantifying security risks in terms of economic and financial losses, and link cybersecurity to business continuity. For these reasons, a mandatory Code of Conduct for CISOs is considered appropriate to implement by the majority of respondents, to ensure a cybersecurity posture and Corporate Social Responsibility (CSR) in organisations.
- *On budget and investments*: Boards think in financial and economic terms to ensure business continuity, but they do not see the link with cybersecurity because cybersecurity does not show a direct return on investment. As such, companies and organisations remain vulnerable because the CISOs do not get the necessary resources to ensure a holistic

protection. To remedy the situation, one of the most common suggestions is for Europe to implement a reporting framework for CISOs to their Boards based on concrete KPIs that would include a risk analysis on the main business assets.

- *On Strategic Information Sharing between CISOs*: CISOs are very aware of the gaps and limitations of information sharing as there is indeed a lack of cooperation across sectors and across borders. CISOs unanimously call for the creation of a network of CISOs under the umbrella of a neutral European entity that would ensure the coordination of the network and of the shared information across sectors and across borders. Several respondents mentioned ECSO as a potential organisation that carries this neutrality and could be at the source of the network as a coordinator. It is important to note that at the CISO level, there is an interest in sharing strategic information as opposed to operational or technical information.
- *On company culture*: Company culture and evolution of mentalities remain extremely slow and CISOs are often met with resistance when trying to implement a cybersecure culture in their companies for a more cyber-hygienic workplace environment. One of the main recommendations is for CISOs to actively collaborate with human resources departments to elaborate company-wide trainings and awareness programmes that would be made compulsory to all employees, including Boards.
- *On staffing*: There is a huge cybersecurity skills gap in the world, and especially in Europe. Europe is already on top of many initiatives and programmes for awareness and to attract more people to cybersecurity education and professions. But there is always more that can be done, and Europe needs to invest more in cybersecurity talents.

At the end of the report, based on the issued recommendations, **ECSO announces its intention to create the "CISO's European Community" in the second half of 2021 for the establishment of a network of cross-sector and cross-border CISOs and to facilitate the information/strategic intelligence sharing.** The CISOs European Community will be **supported by a dedicated platform**, initiated by a special collaboration between the Chairs of the UC, Intesa Sanpaolo (finance sector) and EDF (energy sector), for strategic information sharing on threats and on IOCs (Indicators of Compromise) in particular.

Introduction

Foreword by the UC Chairs

Intesa Sanpaolo – finance sector

***Giorgio CUSMÀ LORENZO**, Group Senior Director, Cybersecurity, Business Continuity Strategy and Group Governance*

Cyber-attacks are among the main risks for citizens and corporates: global attacks and their damages increase year by year, following the evolving complexity of attack techniques especially targeting data and information.

In the financial sector, cyber frauds against customers are worth mentioning, considering they increased significantly due to the COVID-19 emergency and the subsequent increase of «digital customers». This increase is especially linked to some factors like particularly relevant events such as merge and acquisition, or the widening of the digital financial landscape introduced by PSD2 and, last but not least, the COVID-19-induced emergency that further pushed the already ongoing digitalisation, making usually "physical" customers become digital. In most cases, these customers are not used to technology and therefore remain more vulnerable to social engineering and online frauds.

The above-mentioned landscape requires companies to have a holistic approach to protect data, systems, applications, processes and services and to enhance their overall resilience. Furthermore, great importance should be given to the concept of trust which should be the foundation of relationships between all actors potentially involved: from customers to other companies to third parties and the whole ecosystem at national and global level. These two concepts of holism and trust should be applied through cooperation and information sharing, cyber culture and awareness raising, and continuous improvement of cybersecurity solutions to guarantee a secure ecosystem considering that the time we are living in is based on interconnections.

EDF (Electricité de France) – energy sector

***Olivier LIGNEUL**, Group Chief Information Security Officer, Group Cybersecurity Office*

Cybersecurity has become a strategic activity for European critical operators, of which EDF is a part. We are all facing a great increase of threats (EDF's ecosystems attacks on the supply chain followed a 300% growth between 2019 and 2020).

Over the same period, we have noticed an inflation of 70% of manufacturer and service provider's critical vulnerability publications from our suppliers, and in reaction, we acted swiftly on the remediation of those vulnerabilities.

In this context, a trusted relationship as well as an efficient communication, information sharing and strong partnership between the organisations and their suppliers are essential not only on incidents but also on vulnerabilities management.

Introduction to the report

This report is in direct continuity of the "Green Paper on Challenges for CISO's & Threat Intelligence Sharing" [1] issued by the Users Committee in November 2020 that already offered some observations and avenues of consideration on several points related to the roles, responsibilities, and liabilities of CISOs, as well as the current limitations of threat intelligence sharing. Following the Green Paper, ECSO launched an EU-wide survey from November 2020 until January 2021 targeting CISOs (or equivalent) from all over Europe and from all sectors.

In this paper, we analyse the results of the survey and offer some conclusions and outcomes in line with the CISOs' answers and recommendations.

The methodology in drafting this report has been to apply as neutral and structured an approach as possible in order to provide valuable conclusions. This paper is therefore divided into four major sections:

- The **first section** covers the different elements of the survey presented to the CISOs and the adopted **methodology** in reaching out to them.
- The **second section** provides some **statistics** presented in different visuals relating to the representation of the respondents' professional certifications, job positions, sectors.
- The **third section** deep-dives into a **sector-by-sector analysis** of the different survey elements.
- Finally, the **fourth section** provides cross-**sector recommendations** stemming from the common messages identified in the vertical approach.

This paper is aimed at and will be distributed to all stakeholders from the EU Institutions, national public administrations, and European industry leaders, to help them get a better understanding of the cybersecurity threat landscape through the point of view of a CISO, and to work on joint solutions to address the gaps and limitations that CISOs currently encounter in order to achieve a more harmonised and resilient European cybersecurity ecosystem.

On the CISO Survey and the Methodology

Target of the Survey

The survey was specifically **designed for and targeting Chief Information Security Officers** (CISOs) working in different sectors considered as Users and/or Operators of Essential Services (OES). However, considering that not all companies/organisations/entities hold a CISO position, all communications regarding the survey explicitly mentioned "CISOs (or equivalent)" with the aim of also reaching out to people holding cybersecurity management positions in their companies without having the title of CISO.

The survey was carried out in an anonymous setting so that only the sectors and job titles were seen by ECSO upon receipt of the filled in form.

In order to ensure a widespread coverage of the survey, the ECSO Secretariat used the following means to circulate the link and invite CISOs to participate:

- ✓ Direct mailing to the Users Committee members
- ✓ Direct mailing to the ECSO Membership Database
- ✓ Social media posts on official ECSO Channels
- ✓ Bilateral contacts with all European national public administrations in charge of the NIS Directive implementation requesting them to circulate the Survey to their identified Operators of Essential Services (OES)
- ✓ Mapping of and targeted mailings to CISOs from all European (EU + EFTA/EEA + UK) countries working specifically in energy, finance, transportation, and health[1].

Scope of the survey

As mentioned in the previous section, geographically the survey aimed to cover the entire European continent by reaching out to Users and OES from EU Members-States, EFTA/EEA countries and the UK.

Content-wise, the survey contained a total of 24 questions covering a wide range of topics, encouraging CISOs to provide feedback on different aspects of their day-to-day work and encountered challenges. The questions were divided into 7 broad categories:

- ✓ General / The work of a CISO
- ✓ Board investment / Business continuity
- ✓ Information sharing – Threat intelligence – Crisis management

[1] While considering all sectors equally important, the ECSO UC has identified these four sectors among the most mature when it comes to cybersecurity. Following this rationale, the UC has decided that by focusing specifically on these sectors, other sectors would benefit from their maturity. Nevertheless, this did not preclude CISOs from other sectors to participate and all inputs were taken into account.

- ✓ Certification
- ✓ Authentication
- ✓ Liability & Governance
- ✓ European, Regulatory & Cross-sector aspects

For the full questionnaire and overview of the questions, please refer to Annex 1 of the current paper.

The sections and questions were formulated based on discussions and observations stemming from the UC and aimed to show that the role of a CISO goes beyond the purely technical prerequisites that may primarily come to mind. These observations were confirmed by the respondents of the survey who answered all questions comprehensively, illustrating that these different themes are indeed an integral part of their daily responsibilities.

The survey remained open from November 2020 until January 2021. In that timeframe, ECSO received a total of **101 responses** covering different sectors which will be further analysed in the report. We believe that this number constitutes a significant and representative sample of the European CISO landscape, providing legitimacy and weight to the results of the survey that sometimes could look as disruptive with respect to certain narratives.

Survey respondents

Represented positions/job titles

When it comes to the exact job title of the respondents, while some indicated were as expected the title of CISO, CIO, CSO, etc., others were more surprising. In general, as shown in Table 1, the range of positions and titles filled by cybersecurity “managers” is more than heterogenous. As the survey targeted “CISOs and equivalent”, based on the responses, the “equivalent” part can be categorised as follows:

- ✓ C-level
- ✓ Director/Head-level
- ✓ Manager-level
- ✓ Officer-level
- ✓ Other/Unknown-level

This heterogeneity can be found in almost all the represented sectors among the respondents. However, it is interesting to note that 85% of the entries from the financial sector held a CISO position. The remaining 15% had Director/Manager positions dedicated to cybersecurity but not at C-level. None of the other sectors indicated such seniority level when it came to having a framework and specific CISO position inside their companies.

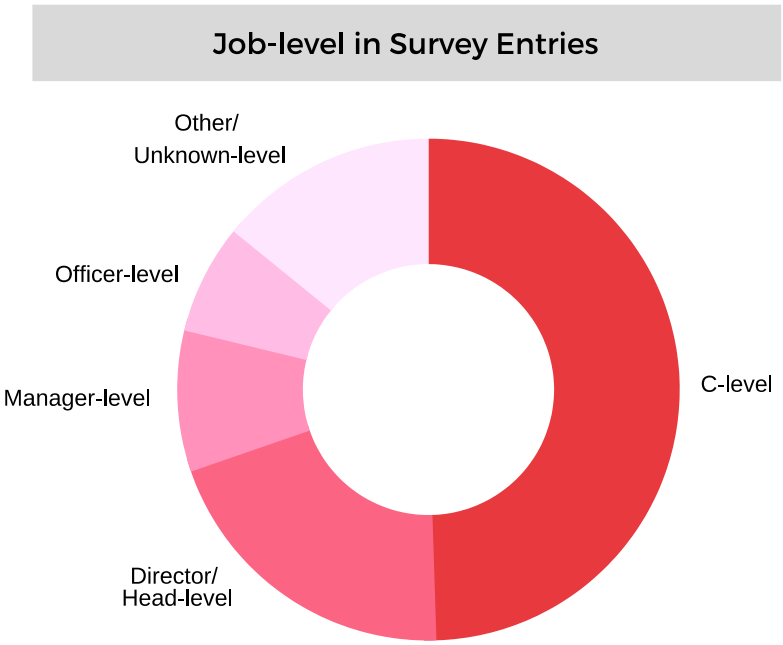
Finally, when considering all sectors together, it is interesting to note that only 50% (ref. Table 2) of all respondents held a title at C-level, showing there is still a long way to go to have cybersecurity considered as a Board-level topic.

Table 1

	Job Title variation
C-level	Chief Information Security Officer (CISO) Chief Security Officer (CSO) Chief Information Officer (CIO) Outsourced CISO Regional CISO Chief IT Security Officer
Director/ Head-level	Chief of Information Technologies Chief of Marketing and New Technologies Deputy Head of Information System Security Deputy IT Director Director of Digital Transformation and Informatics Director of Information Systems Department Director of Management Control and Corporate Development IT Security Director Head of Department Organization & Informatics Head of ICT Department Head of Informatics/IT Department Head of information and communication systems Head of Information Security Head of Network and Information Security Section Head of Security Head of Security and Surveillance (CSR) Responsible for ICT Security Unit

Manager-level	ICT/IT Manager Information security manager IT Infrastructure Manager IT/OT Manager Security & Compliance Senior Manager
Officer-level	Information Security & Data Protection Officer Information security officer IT Security Officer/Security Officer Senior Information security officer Senior Systems Engineer / Information Security Officer
Other/ Unknown level	IT Security Specialist / IT Architecture Coordinator of Information Security and Cybersecurity Counsellor Cyber Security Expert Information Systems Designer Network and Computer Administrator RSE

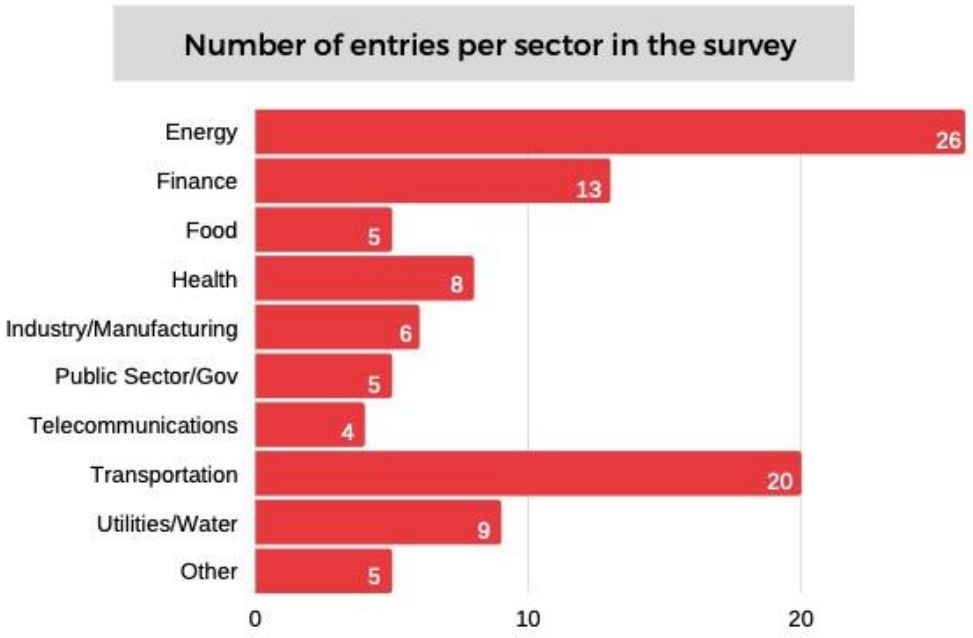
Table 2



Represented sectors

From the 101 received entries, several sectors were represented as depicted in Table 3, with most respondents coming from the energy, transportation and finance sectors.

Table 3



It is worth mentioning that for the transportation sector, we received responses from the air, rail, road, sea and space sub-sectors, thus providing us with a comprehensive coverage of the sector.

The “Other” category contains entries from “luxury”, “retail” and “consultancy services covering different sectors”.

Represented trainings and professional certifications

As part of the general questions, we asked respondents to indicate which professional certifications (if any) they hold (CISSP, CISM, CISA, etc.).

Table 4 shows the big heterogeneity of the answers received and indicates the number of respondents holding each of the different professional certifications.

We also calculated the number of certified respondents per sector as opposed to the respondents not holding any certification. Although for several sectors the number of respondents was limited

and maybe not sufficient to be a representative sample, it is interesting the showcase the following sectors:

- ✓ **Energy: 57.7%** of respondents held one or more certifications
- ✓ **Finance: 84.6%** of respondents held one or more certifications
- ✓ **Transportation (air – rail – road – sea – space): 70%** of respondents held one or more certifications.

Unsurprisingly, finance, transportation and energy came up as the most represented (and they are among the more cybersecurity mature applications) sectors in terms of identified CISO position and readiness against cyberattacks in their field. However, where financial CISOs carry several certifications (among the most common are CISA, CISM, CISSP, CRISC, ISO27001), the energy and transportation sector CISOs would not necessarily have certification. Other sectors showed more heterogenous results with regards to the CISO position and certification.

This is only a preliminary visual of the number of mentioned certifications, but we will have a more thorough approach to understand each sector's approach to certification in the next section tackling the vertical analysis.

Table 4

Name of professional certification	
No certification	38
ISO 27001	38
CISM	21
CISA	18
CISSP	10
CRISC	5
Other/Miscellaneous	50

Results of the survey: sector by sector analysis

This section covers an analysis of the challenges as seen sector by sector. For a better understanding of the results, within each sector we have tried to identify first the “in-company and governance challenges” and second the “cooperation aspects and challenges”.

Energy

Cybersecurity is one of the main drivers for revising business continuity plans and a critical pillar of the energy sector since any disruption can cause significant societal and environmental problems. However, despite being considered as crucial, **cybersecurity does not get enough financing** for correct implementation of measures because it is **approached as a separate issue and managed by different in-company groups** instead of leveraging on existing processes. Moreover, it seems that the nuclear sector, for which the core business remains in the analogic systems, is not quite as impacted by cybersecurity for the time being but could soon become a major challenge for its intrinsic sensitiveness.[2]

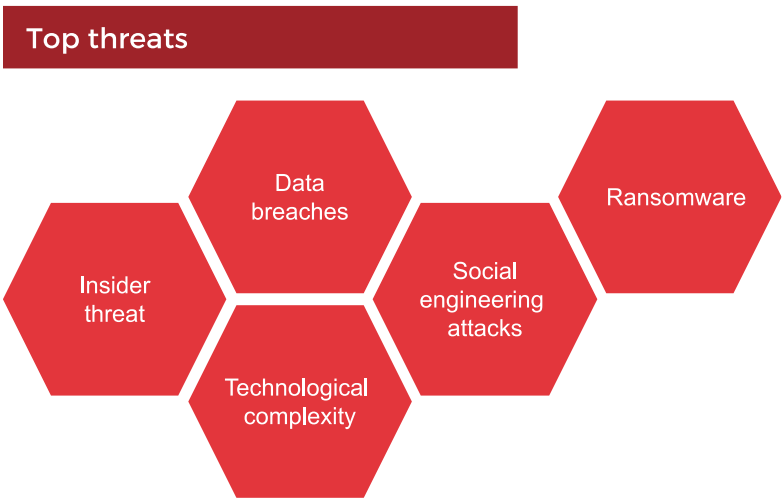
Yet, companies and systems remain vulnerable to cyberattacks of which the survey highlighted some very **disruptive aspects**. The energy sector is primarily affected by the following:

- ✓ *Service availability affecting the production line*: ransom extortion criminals or state actors will target OES with the goal of disrupting the service for as long as possible, therefore incident response planning with an OT disaster recovery plan including backups and system recovery for OT systems is crucial
- ✓ *Reputational damage*, especially in the case of loss of users’ data
- ✓ Loss of customer loyalty
- ✓ *Financial losses*: security breaches often result in substantial financial losses arising from theft of corporate information, spread of commercially sensitive data, of financial information and transactions data, and finally additional money and costs associated with repairing affected systems, networks and devices
- ✓ Human life endangerment
- ✓ *Social disruption* affecting local areas, villages, people, etc.
- ✓ Environmental costs and damages
- ✓ *Political impact:* possible chain reaction effects with other OES as the critical infrastructure (CI) interdependency makes them vulnerable and the lack of resiliency leads to national and social risks.

These disruptions are the direct consequence of cyberthreats which are numerous. The energy sector is plagued by many threats with cyberattacks becoming increasingly prevalent and

[2] ECSO’s observations lead us to believe that this statement is likely to change as OT increasingly converges with IT.

sophisticated due to the critical energy sector's attractiveness as a cyber target related to geopolitical risks. However, some threats are more prominent than others and the visual below illustrates the main ones, followed by the ensuing top challenges.



Legend

Some threats such as social engineering attacks and ransomware are quite straightforward to understand, others have **layers of implications** and consequences.

Data breaches would include **data leakage** coming from **cloud vulnerabilities** and ending in **identity and personal data management theft**.

Top Challenges – Energy Sector

- ✓ **Breaches from internal sources**, whether voluntary or non-voluntary, due to a **lack of cybersecurity culture** and awareness, and even a lack of cybersecurity skilled staff.
- ✓ Urgent need to establish a **company culture and shift mentalities to include cybersecurity in all business aspects**, thus impacting personnel behaviour including the resistance to change from OT business units
- ✓ **Boards need to allocate necessary budgets** for in-company **awareness and training** programmes.
- ✓ **Lack of cybersecurity skilled staff** due to skills shortage and talent retention in Europe
- ✓ The **network and technology complexities** raise challenges such as establishing an ICT security network framework and problems linked to zero-trust architecture and incident management. The technological complexity stems from the fact that energy infrastructures are complex (and more often old) systems, making the convergence of IT and OT networks and systems a difficult task. In general, obsolete operational equipment makes it very difficult to ensure the continuous operations of the CI.

In-Company and Governance Challenges

Certification

The protection of CI, of the networks and of the systems is not totally dependent on the number of certifications obtained by the companies/operators. The most commonly mentioned certification is IS27001 and in most cases, **companies/operators choose to get certified as a measure of compliance**. However, a **non-negligible minority of respondents mentioned that certification is not considered as a priority in their organisation**.

Compliancy to certification does not increase or guarantee the cybersecurity or risk posture of companies. Rather than a certification-based approach, respondents would choose a risk-based approach to prevent this "check-the-box"/compliancy mentality that provides a false sense of security. They would rather advocate internal audits, cybersecurity vulnerability assessments and pentestings for a continuous evaluation of the risk level.

Even for the companies following certification schemes, they often recommend **choosing minimal certification** scope, while always having the top management's approval and support. This would facilitate the risk-based approach by applying certification only to the core critical infrastructure zones instead of getting too deep into the technical controls, i.e., **companies would prefer a certified process that can more easily be adapted to new threats rather than certified components** which can have a limited certification lifetime. It would also help Boards to provide their approval and support, and implementors understand the organisation's business process. The balance between certification and agility lies in the company/operator's cybersecurity resiliency. One crucial detail to be considered is that most respondents replied that **the CISO is not necessarily involved in the certification processes of their company**, raising a number of issues with regards to the participation of CISOs in key activities/decisions inside their own company/organisation. Such activities include the use and running of cyber ranges or technical exercises, and the management of authentication inside the company. It seems that at least in the energy sector, **CISOs tend to be fully involved in the planning and implementation of cyber ranges**.

Special focus on authentication

Authentication remains a tricky topic although all agree that a holistic approach is mandatory. MFA (multi factor authentication) is key in the application, but the methods vary slightly from company to company, although they all agree that the methods are stricter when applied to critical systems. A holistic access management remains a challenge unless all the infrastructure is centralised which is not the case in industrial companies (IT and OT environments are and shall be completely separated).

Code of Conduct for CISOs

These different aspects raise the question as to whether a mandatory **Code of Conduct for CISOs** should be implemented and directly **linked to Corporate Social Responsibility** (CSR). Respondents agreed that **a Code should exist because mandatory minimums are necessary for compliance rules**, although it would be advisable to keep in mind that small companies usually lack resources and for them a Code would be an additional burden in terms of work and expenses. The Code should at least be mandatory in the relation with and from the point of view of the customers and civilians. As for the enforcement of the Code, reactions were mixed, mainly stating that although penalties should exist – as they are the most persuasive way to promote changes and quantify risks – they should only be used as a last resort.

CISOs need to start implementing security strategies by categorising the criticality of projects but the key is to have a proper and clear allocation of cybersecurity roles and responsibilities (the CISO is not only an IT advisor). In this sense, perhaps a **centralised corporate risk (IT & OT) management** could be suggested where all corporate risks are evaluated jointly, and then a risk owner is designated to track and manage designated critical risks (as opposed to company acceptable risks). An important missing link is the management across the senior leadership in all business and corporate areas. All these areas should take ownership of risks with a **clear allocation of cybersecurity roles and responsibilities under the CISO leadership.** This would help for a strong governance model and harmonise the entire company's cybersecurity strategy with strong coordination mechanisms.

It is understandable that **business continuity is one of the core concerns** and it should be **underlined by a solid governance** which comes with awareness and a good dialogue where Boards are aware that there is no such thing as 100% security.

CISOs working lifecycle: *identify, protect, detect, respond, recover* (according to NIST Framework [2]):

For energy sector respondents, the order of importance depends on the maturity of the organisation in cybersecurity and the IT/OT environment. In general, 'protect' (sometimes coupled with 'recover') is the most important aspect to be tackled, while 'detect' should come last as the priority seems to be business continuity. In other cases, for respondents working for companies with seemingly a lack of cyber-maturity, it seems that 'detect' and 'respond' are the most important. It all depends on the company's cybersecurity strategy, whether to have an active (respond) or resilient (protect and recover) approach to cyberattacks.

Boards of Directors

In general, respondents mentioned receiving an adequate level of support from their Boards, although there could be room for improvement, especially when it comes to **Boards investing (in-)sufficiently in cybersecurity**. For the energy sector, there are **three major reasons** for this:

- ✓ *Non-awareness of the seriousness of the consequences of possible cyberattacks/cyberwarfare*: Boards do not believe their business is going to be affected by cybersecurity threats and do not see the return of investment in the short term, so instead they invest money in more fast-returning projects; and even if they do invest, it remains impossible to reduce the risk to zero.
- ✓ It is *not made clear in business terms why cybersecurity can be a business enabler* and not a detractor: it is made difficult because it is hard to quantify the cybersecurity benefits.
- ✓ *CISOs do not communicate about cybersecurity to their Boards in a business-related language*: they tend to use technical jargon which leads to misunderstandings and confusion from Boards. It is also a good opportunity to encourage Boards themselves to become literate in cyber-risks which does not necessarily mean becoming a technical expert.

Some suggestions of recommendations were provided to improve the situation:

- It is very important that ***CISOs reach out to their Boards and get their support*** and commitment for all in-company implemented actions.
- There is a general agreement about the necessity to create a dialogue and ***engage both the leadership and employees*** across the company. Even if it is hard to achieve, whether they start with the recommended top-down approach or bottom-up one, it would lead for more consideration and weight for the CISO position.
- The most important thing is to ***secure the Boards' understanding*** before working on spreading the information to the other levels in the organisation.

In order to do so, **CISOs must learn to talk in financial terms**, mentioning the context and the concrete implications of cyberattacks, providing their Boards with a reference framework for understanding, such as a **cyber-risk management framework that must identify and align threats/vulnerabilities/risks/remediation actions, all identified with relevant metrics**. The key is to report in a business-like language, avoiding technical discussions and ensuring that risks are quantified, and investments justified. Another suggestion would be that **Boards should have mandatory cyber-training and at least one Board member should be specifically accountable for cyber reporting** to the rest of the Board on the matter. This Board member could be the CISO him/herself or a Board member trained on purpose for such a task to whom the CISO reports.[3]

Cooperation Aspects and Challenges

Information sharing

Information or intelligence sharing is at the core of cooperation when it comes to cybersecurity and the challenge remains on how to improve it, which channels to use, how to proceed and most importantly whom to trust. In order to address this challenge, respondents from the **energy sector recommended creating a European forum and CISO information channel which would be based on a closed circle based on trust and competency with integration across all OES sectors and across EU countries**.

CISOs need to start working together and exchange expertise, and there is a need for a CISO hub where they can share threats and solutions on how to protect their companies against attacks in a confidential manner. Existing information sharing mechanisms, such as **ISACs, could be seen as too limited** for this purpose **as they often include a wide array of stakeholders** (users, suppliers, consultancies, etc.) collaborating in an open format **which could deter CISOs from sharing confidential information**. Since many CISOs are business competitors, **the hub should ideally be operated by a non-for-profit organism that would coordinate the activities, information sharing and help businesses against real cybersecurity threats and how to face them**. Other respondents mentioned that such a structure could possibly be led by a government

[3] Indeed, the ECSO UC deepened this topic observing that cyber reporting should always lie with the CISO (or equivalent). Yet, organisations could ensure that at least one Board member (other than the CISO) holds the entire Board accountable to ensure that cybersecurity is monitored, and appropriate measures are taken when needed to maintain a certain level of cybersecurity posture within the organisation.

agency or a CSIRT, although in order to avoid geopolitical conflicts, a neutral entity should be favoured, and a private sector independent body could be more operational.

Some respondents suggested that the European Cyber Security Organisation as an intermediary could play a critical role for good information sharing and cooperation between CISOs.

Respondents also recommended using a secure portal through strong authentication architecture. This **specialised platform** would allow **in-depth exchange of information** without the fear of being stigmatised and to which CISOs would have direct access.

With information sharing comes the **aspect of the quality of information** shared which has brought up the possibility of collaboration between CISOs and Law Enforcement Agencies (LEA).

A majority of respondents mentioned that they are **open to collaboration with LEA** as it would be important and useful in dealing with criminal attacks faced by companies that manage critical infrastructure. However, it does not seem that any such type of cooperation is concretely happening which is obviously a big gap. Despite the fact that there is already a collaboration between CSIRTs, LEA and the judiciary (though CSIRSTs are rarely called to testify in court cases), **challenges remain in this type of cooperation, such as diversity of legal frameworks, data retention, sharing of personal data (including Internet protocol addresses) and the confidentiality around criminal investigations, as well as the admissibility of digital evidence in court cases.** But a good practice of collaboration between CISOs and LEA could still take place within that framework. If helpful, national authorities and Interpol were also suggested as intermediaries for communication between CISOs and LEA, as long as information is not shared one-way.

The possibility of cooperation between CISOs and LEA raises many issues, in particular cross-border and cross-sector fragmentation. When asked how to overcome such fragmentation, CISOs proposed the **creation of a single joint entity to act as a point of communication to help develop policies and share best practices/methodologies/tools especially from more mature sectors**. A **CISO community should be created to share knowledge, tactics and new technology**. This in turn would optimise information flow between European CISOs and LEA, create cross-border interest groups for essential services providers. Whether such a community would be lead at the national level or European institutional level, **CISOs recommended establishing a common standard framework and a single harmonised European regulation, providing formal information sharing and exchange mechanisms**.

In the meantime, energy sector respondents are monitoring and relying heavily on the NIS Directive [3]. Most consider the NIS as a good beginning although they mention that regulation needs to be simplified and bureaucracy reduced.[4]

Among the suggested improvements, **CISOs recommended an increase in the communication frequency between the OES, the national authorities and the EU** by organising meetings/events for CISOs to meet with each other and exchange technical experience/expertise,

[4] It is interesting to note that the proposed NIS 2 Directive (published in December 2020) is a welcome development in this regard as it directly addresses some of the more controversial and difficult-to-implement measures of the initial Directive.

to share knowledge/information/best practices especially in securing OT infrastructure. This brings the topic back to the need for a central entity coordinating such activities.

Procurement

A final point important to CISOs in the energy sector is the procurement aspects and the use of cybersecurity solutions.

Energy CISOs primarily value the following criteria: **costs/cost-benefit**, **performance** (which includes efficiency, flexibility, adaptability/complexity of implementation and installation, ease of use/low administration effort), **trusted source of origin/made in Europe**, **necessity**, and finally the **guarantee of quality from other organisations using the solution**.

CISOs find it **very important to use EU certified solutions for the trusted management of sensitive data**. At the very least, EU certified solutions are a bonus in the decision-making and in preventing any compliance issues. European solutions and services are **preferred for reasons such as sovereignty, autonomy, availability of customer support, and necessity for regular updates**. Energy sector CISOs find EU solutions provide a level of protection thanks to the EU legislation and regulation that is not found outside of EU borders.

Finance

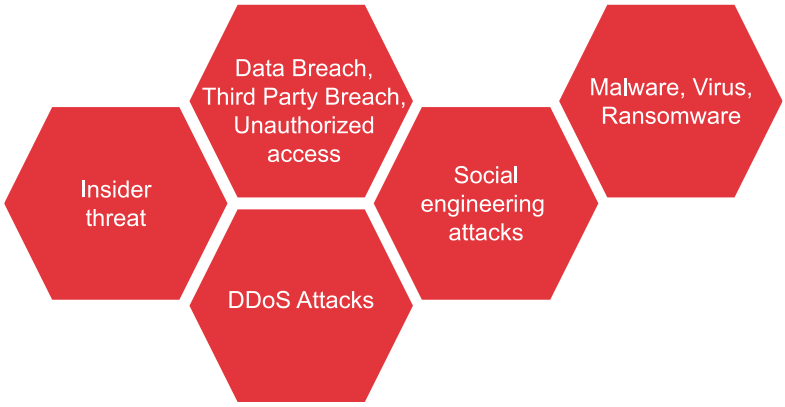
In the financial sector, cybersecurity is considered among the main issues to be tackled, if not the driving force for business continuity in order to have aligned technology investments, better incident preparedness and response and recovery processes. This is unsurprising as the **financial sector can face significant disruptions in case of cyberattacks**. Disruptions can include:

- ✓ Financial impact
- ✓ Cost of insurance

- ✓ Effect on customer behaviour
- ✓ Fines imposed by authorities
- ✓ Impact on reputation/reliability
- ✓ Impact on technology infrastructure/loss of service capability
- ✓ Personnel data and secret data leakage

The below visuals highlight the most frequent and common threats in the financial sector and the most commonly faced challenges:

Top threats



Legend

Social engineering attacks here refer in particular to phishing, SIM swapping and fraud.

The implications of **insider threat** include data leakage, unpatched vulnerabilities, lack of staff training and lack of awareness.

Top Challenges – Finance Sector

- ✓ Need to **continuously invest in cybersecurity infrastructure**
- ✓ Constantly battling with **vulnerabilities stemming from legacy systems** (e.g. incidents caused by security patches and updates, thus undermining trust)
- ✓ **Evolving cybersecurity threat landscape** with increasing complexity of technology and increasing sophistication and resources of cybercriminals.
- ✓ **Difficulties in promoting a holistic IT security framework** throughout the organisation because of the lack of maturity of the staff and of the processes.
- ✓ **Ever evolving and demanding regulatory framework**, constantly increasing the burden of compliance.

In-Company and Governance Challenges

Certification

Certification is also considered as less important and less valued than regulation (or, rather, over-regulation) **and standards**. However, all respondents stressed that the CISOs are normally fully involved in all cybersecurity related activities of the company. Their objective is to find ways to cover the organisation's weaknesses without spoiling the climate of cooperation between colleagues and assessors by leveraging on employees' skills and putting operational procedures in place.

Special focus on authentication

Strong authentication is considered as an information security requirement. Usually, the process is managed by developing relevant policies and procedures inside the infrastructure and the applications, beyond the technical controls.

They would rather use a more operational risk-based approach instead of high-level and bureaucratic. The financial sector CISOs surveyed all use cyber ranges in their companies and are fully involved in the implementation process.

These aspects show that the **financial sector is quite mature when it comes to the basics to be covered by CISOs**.

Code of Conduct for CISOs

Although they would welcome a **Code of Conduct for CISOs in which organisations should act proactively**, take appropriate measures and apply necessary remedies, respondents highlighted the fact that the banking sector is already heavily overloaded with strict regulations and penalties. For the Code, penalties, though largely unpopular, could be used as a very last resort.

Beyond the Code, financial sector CISOs are very much aware of their roles and responsibilities. In order to ensure a good governance accompanied with risk optimisation, the **CISOs recommended making mandatory annual security risk analysis and cybersecurity activity reports to the Boards, establishing and promoting a holistic IT security framework throughout the organisation, and applying accountability throughout the organisation**.

CISOs working lifecycle: *identify, protect, detect, respond, recover* (according to NIST Framework [2]):

CISOs working lifecycle: identify, protect, detect, respond, recover (according to NIST Framework (ref. [2]):

Financial sector respondents mentioned that all aspects were equally important to implement in finance. However, 'protect' should be considered as the necessary first step, while 'respond' & 'recover' should be given a particular attention to get the control systems back running as fast as possible in case of an attack. For all these reasons, respondents also recommended that CISOs should sit at the Board of Directors.

Boards of Directors

Despite certain mature aspects of the financial sector when it comes to cybersecurity, **CISOs still do not receive a full support from their Boards or are not always part of the Board**. In certain cases, the **CISO position is not even at C-level**. Big steps should be made quickly to improve the communication between the CISOs and their Boards. On the one hand, **Boards are aware of cybersecurity but not its consequences, so they prefer to focus on financial and organisational issues** instead of recognising the advantages of a small risk operation. On the other hand, **CISOs do not communicate risks well enough by explaining their business value**. CISOs should report and communicate their decisions to the Boards in a simple and non-technical way and be able to do so independently. They should deliver good quality reports and **regular presentations to their Boards on the security posture of the company** and **organise awareness training programmes both for the Boards and for the employees**.

In order to improve on these issues, the respondents suggested the following solutions:

- Setting up *reporting committees* on operational, cybersecurity and data privacy aspects
- Setting up cybersecurity, cyber-threats and cyber-response KPIs
- Setting up regulations that will make of *cybersecurity a Board-level topic* so that CISOs can sit at the Boards
- Setting up *regulations making Boards legally liable* should they not take proper control or give proper attention to cybersecurity matters.

Cooperation Aspects and Challenges

Information sharing

Financial sector CISOs are mostly interested in creating official procedures for information sharing that would run periodically (e.g., regular bulletins or specific information sharing meetings) and that are approved by the EU financial institutions. They **recommended the creation of a Threat Intelligence Platform (TIP)** which could be a useful solution to improve cyberthreat sharing (e.g., on IOCs – indicators of compromise) among sectors and countries. TIPs can be **used by major private sector leaders and European and national (intelligence) agencies and associations to periodically share information that is strategic, geopolitical**, on new hacking techniques, cyberattacks trendscan, etc. The TIP could also be used as a direct communication channel between CISOs and law enforcement agencies (LEA), as it is crucial for the financial sector to share information and address crime-relevant issues.

Additional suggestions included the **creation of a regulation for network of information sharing implementation across sectors and OES** and the organisation of conferences organised by EU/CERTs/regulators to **share experience and trends with the private sector, which would allow a facilitated flow of information from the public sector towards the private sector at the European level**.

By applying these private-sector inclusive recommendations, it would be possible to **enhance and consolidate cross-border and cross-sector information sharing in Europe**, with a priority on the cross-sector aspects as cybersecurity is a horizontal topic. On the long-term, the created **network of CISOs would establish common practices in common areas for all sectors (governance, operational and cybersecurity risk management, business continuity management, third party risk management, response plans analysis and reporting) and provide recommendations to harmonise EU regulation and standards across Member States**.

On the topic of regulation, the financial sector relies mostly on the NIS Directive and regulations stemming from the European Banking Authority (EBA), although the sector is submitted to stricter regulation than other sectors, and the implementation is not at the EU level but at country level. This is the reason why enhancing cross-sector and cross-country collaboration is crucial for the financial sector as it will enable harmonised regulation thus **lessening the administrative burdens and controversies that come from over-regulation**. By taking into account the evolution of the cyber threat landscape, it will also be possible to **clearly define the role, responsibility and liability of CISOs.**

Procurement

It seems that regulation is not the only aspect in which the European Union could step up when it comes to the financial sector. Indeed, while CISOs consider it **very important to use EU certified products**, they do **not necessarily apply this criterium to procurement**. They agree that certified products provide additional levels of assurance and confidence to the organisation's customers, shareholders, and partners, and give a competitive advantage to the organisation within the sector, while also providing common rules and practices.

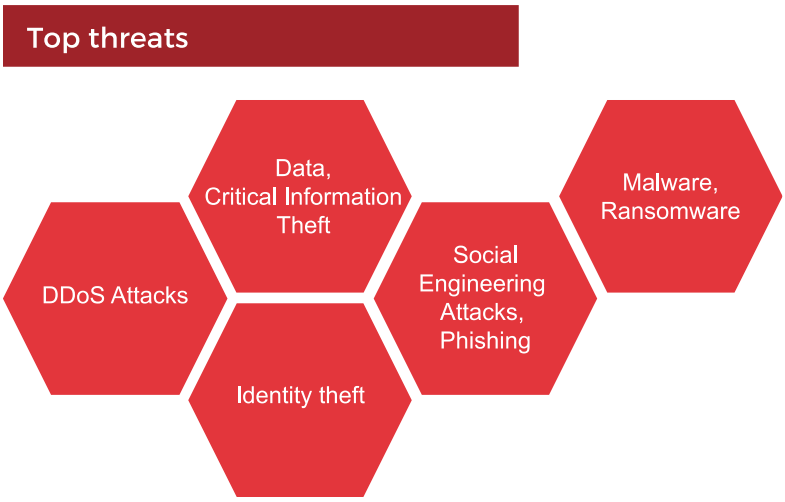
On the other hand, the financial sector considers that **protectionism (such as "made in EU") as seen around the globe will not bring any benefit**. CISOs, using their own words from the survey, "do not need European products, [we] need good products [we] can trust". **Performance, quality, and reliability** are the top criteria. The origin of the products does not matter as long as these criteria are met because of the constant evolution of threats making systems more and more vulnerable. Other important goals of financial sector CISOs are **customer satisfaction and secure payments transactions.**

Food

Cybersecurity along with maintaining an updated technological infrastructure is quite a priority for the food sector. Should the food sector be under cyberattack, the disruptions would be significant and impactful:

- ✓ Economic impact
- ✓ Reputational impact
- ✓ Loss of critical and strategic data
- ✓ Societal impact due to *food shortages* and/or suspension or interruption of service
- ✓ *Loss of trust* of internal and external users.

As shown in the visuals below, the food sector deals with typical attacks and challenges in terms of cybersecurity.



Top Challenges – Food Sector

- ✓ **Continuous updates following the cyber threat environment** are required but remain hindered by legacy systems.
- ✓ **Human resistance** to change is ever-present: regular awareness and trainings should be implemented to properly train and qualify organisations' staff.
- ✓ There should be a **constant sharing and training of good practices** to sensitise about the importance of maintaining secure protocols.
- ✓ Need to **create a habit of "business as usual"** in the combination of processes and procedures that must be applied regularly at the operational and administrative levels.

In-Company and Governance Challenges

Certification

For the food sector, **if the above-mentioned procedures are properly applied, the respondents indicated that they do not necessarily see the need for certification** and some stated that they do not currently apply any in their company. When certification is used, it seems that CISOs are fully involved in the process.

Special focus on authentication

While authentication management is considered as very important and usually managed through a centralised authentication platform, it is not always clear who oversees it.

Food sector companies are also starting to increasingly carry out simulations and technical exercises, although the **participation of the CISO is considered as irrelevant** since **in many cases the organisation does not even have a dedicated CISO position**. This means that many of these **issues that should be handled by CISOs are scattered across the company** and **put under the responsibility of other existing positions that are not necessarily at a senior level**.

Code of Conduct for CISOs

The food sector respondents agreed that having a Code of Conduct for CISOs **would guarantee some minimum compliance rules and sanctions would play an important part in the compliance**.

Boards of Directors

While respondents unanimously confirmed having the support of their Boards, they still **estimated that Boards are not aware of the real threats** and how complex they can be. **Boards do not see cybersecurity as an investment** or a first level expense necessary to the running of the organisation, but rather as a second/third level expense.

CISOs working lifecycle:
identify, protect, detect, respond, recover
(according to NIST Framework [2]):

Overall agreement on the order of actions although the prioritisation between Identify/Protect/Detect seemed to vary a lot from company to company, with 'protect' coming first most of the time. Food sector respondents also noted that zero risk does not exist, and that Boards should be trained in and made aware of information security skills.

An interesting suggestion from the respondents on how to improve the situation was to bring awareness to the Boards and all company employees through the **implementation of a cybersecurity by design across all business processes** and through **tailored trainings**. While training Boards to be more knowledgeable in cybersecurity, CISOs should also learn to report in simple non-technical and commercial terms that would align cybersecurity risks with business process risks. It would also help to **make the CISO's legal responsibility mandatory so that Boards cannot contradict measures** that could put the integrity of the infrastructure and of the CISO at risk.

Cooperation Aspects and Challenges

Information sharing

The lack of or vague responses on the topic of information sharing indicates **the lower maturity level of the food sector when it comes to cybersecurity**. However, some suggestions are worth mentioning such as the **proposal to establish a procedure for collecting, storing, and distributing information on cyber threats** so that CISOs improve their ability to act preventively and can act quickly and consistently against cyberattacks, generating a common and shared knowledge.

Respondents also **suggested publishing a European Web Portal with open data about attacks and risk level and establishing a training curriculum that a CISO must follow in order to face the daily challenges that comes with the role**.

In general, food sector CISOs agreed that **sectorial associations should promote good practices**. To avoid cross-sector fragmentation, clusters of CISOs should be supported and actions that strengthen incident response and threat intelligence capabilities across sectors should be promoted so the sector can learn from the more mature sectors. This also means that there should be a faster implementation time of the NIS Directive at country level. European regulation should also enable more fluid communication between operators with quick answers and interaction in case of incidents.

Procurement

Regulatory compliance is also one of the criteria applied to procurement by the companies in the food sector, along with performance/type of protection, origin, and product design. However, cost seems to be the most important criterium.

Overall, respondents found it would be quite important to rely on EU certified solutions, but according to them the **EU level should have a reliable and uniform management of sensitive data**. What counts is that data must be stored in a secure way. So, while it is preferable to use EU solutions, it is also **not impossible for them to look for solutions outside of European borders**.

Health

Cybersecurity, far from being a priority for the health sector, is rather considered as a luxury or a subset of the entire security of the organisation. Patient safety is the priority, but the respondents indicated that **they are aware of the criticality of cybersecurity** and the need for more cybersecurity investments. Their awareness stems from the understanding that cyberattacks would and can disrupt the operations of medical equipment and bring increased costs. Plus, beyond the reputational aspects, they would also need to consider the loss of revenue and required investments for remediation.

On average, the healthcare sector is particularly affected by the following threats and challenges:

Top threats

Top Challenges – Health Sector

- ✓ **Low funding priority**: there is not enough budget to outsource security services or to get the appropriate tools to monitor and control cybersecurity operations.
- ✓ **Lack of qualified staff**: there is not enough trained IT personnel.
- ✓ **Big dimensions of the organisations** and the **big geographic distribution** of the infrastructure: hospitals are in some cases gigantic infrastructures widespread and sometimes geographically sectioned, making it very difficult to cybersecure correctly.
- ✓ **No knowledge from Boards** about the importance of cyberthreats.

These challenges make the work and tasks of CISOs very difficult. The **CISO position in the health sector is almost non-existent, and where it does exist, there is not a clear list of their duties and responsibilities.**

In-Company and Governance Challenges

Certification

One of the responsibilities – beyond the creation of a CISO position – is for CISOs to **make a long-term plan, adapting good practices and methodologies of management of risks** and of security of information to the particularities of their organisation.

Special focus on authentication

Authentication aspects are tackled through Identity Management, most likely using a multi-level security approach, although it is not clear who is in charge of this from the top either.

By doing so, they will find the balance between managing security to minimise risks and reaching the objectives of the organisation.

For the healthcare sector, **certification is not considered as a priority or a good representation of the organisation's cybersecurity state**. In general, when organisations have certification, it is

not related to information security. In the same vein**, cyber ranges or technical exercises are not widely used in the sector at all.**

Code of Conduct for CISOs

The **primary objective to implement a good governance in the sector is therefore to start by ensuring that a CISO position exists in all users, operators, and critical infrastructures**.

CISOs should then implement guidelines and provide advice to be followed by the entire company, and continuously monitor and handle all the network activity of the hospital. CISOs **need to align cybersecurity with the objectives and priorities of the organisation and create and design security policies and norms to be followed across the entire organisation**. In this way, clear and measurable cybersecurity objectives should be assigned to all employees. Some respondents also suggested the creation of a Chief Risk & Governance Officer position that would closely work with the CISO.

Boards of Directors

On top of these considerations, as previously mentioned, **Boards do not have enough knowledge because IT is considered as so complicated** that people prefer to ignore its importance, mostly since **cybersecurity is considered as a luxury**. Additionally, their lack of awareness of cyberthreats and consequences brings **Boards** to **prioritise budgets targeting the health of patients and associated needs, with no room left to invest in cybersecurity**.

To overcome this issue, it is recommended for **Boards to have mandatory** annual cybersecurity and IT-related **training** to understand healthcare information, data management and the accompanying risks. Boards need to receive factual information about attack losses and **create actual cybersecurity departments under the CISO management**.

Cooperation Aspects and Challenges

Procurement

As per the words of one of the respondents:

"*Hospitals rely on a very low degree of regulations and actions for the protection of critical infrastructure, and there is a lot to be done. First, critical from non-critical assets should be defined and security controls and solutions must be implemented. In many cases medical devices could cause security alerts on the IT infrastructure due to hidden vulnerabilities, and sometimes oncoming connections are allowed from the providers posing great threats to patient data*."

This brings up the question of procurement and use of cybersecurity solutions. The healthcare sector prioritises **performance, costs, and maintenance criteria**, with a special thought for **system integration and source/provider.**

They believe it is **quite important to rely on validated European solutions**, not only on standards related to the acquisition and management of health information systems, but also on **standards related to the communication between healthcare devices and the sharing of medical information**.

Information sharing

On information sharing, respondents advocated a step-by-step approach. First, there is the need to create healthcare security teams which would make the information sharing come more easily. It would facilitate the convergence of MISPs and various other networks and allow the **creation of a portal or tool where information could be accessible**.

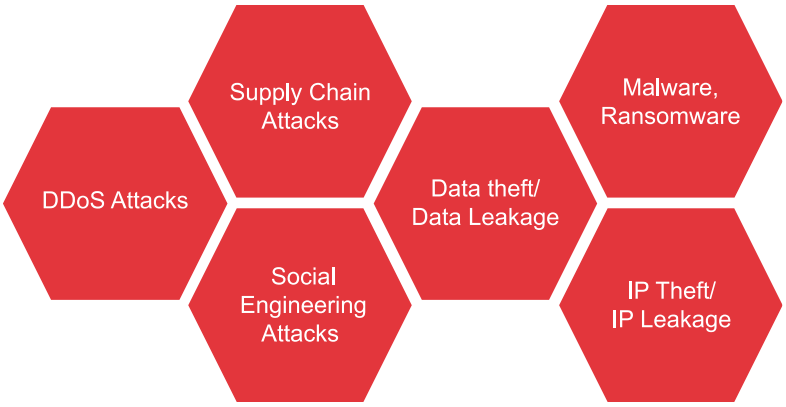
Among the suggestions was also the **possibility to implement an ISAC with the establishment of a single point of contact and bottom-up information sharing**. In any case, any chosen means should begin with the building of trust and ensure that **information sharing goes from public to private sectors and vice versa**. Of course, private-private cross-sector cooperation should also be defined by setting up a list of companies being in “good shape” and getting them to work together and help the other companies.

Industry/Manufacturing

Cybersecurity is crucial for the industry/manufacturing sector for **business continuity in order to ensure continuous production**. The **challenge is in finding the right balance in terms of investment versus outcome**. Disrupting operations would cause an extreme cost burden and potentially lead to economic death. According to the respondents, **cyber insurance does not fix the problem at all**. Other more common disruptive aspects of cybersecurity to the sector touch on the leakage of sensitive information, implying reputational issues, as well as the **obsolescence in the business systems and processes**.

The following are the most common threats and challenges facing the industry/manufacturing sector:

Top threats



Legend

It is interesting to note that **social engineering attacks** cover various sub-types: the usual phishing, but also CEO fraud and blackmailing as well.

Top Challenges – Industry/Manufacturing Sector

- ✓ **Thin budget**: low investments and lack of Board approval on cyberthreats
- ✓ **Weak staffing** and **missing skills**
- ✓ **Poor security culture and lack of security incident response** because of the large scale and the complexity of the industry organisations

In-Company and Governance Challenges

Certification

A majority of respondents mentioned that their **companies hold certifications** and that the **CISOs are fully involved in the processes**. Certification should be considered early on, even if it is not a necessity. **Certification is seen as just a means; it does not run the security of the company**.

Special focus on authentication

In the industry sector, they use a holistic approach by monitoring the authentication of individuals and of systems using a Global Multi Factor Authentication and Identity Management Service.

On the other hand, there were **mitigated responses to the use of cyber ranges in the industry sector**, as it seems it is not a popular concept yet.

Although there is an agreement that cyber ranges should be monitored and implemented by the CISOs, in the same way as it is done for authentication.

Code of Conduct for CISOs

CISOs need to set up a right **framework so that risks are made transparent to the right levels**, including their Boards. The sector needs **strong investment in risk analysis and training managers** will help reduce the risks and improve successful projects. On the topic of reaching out to the Boards, responding CISOs agreed on the need for a Code of Conduct or ethical behaviour, though they favoured awareness to penalties in case of breach of the Code.

CISOs working lifecycle:
identify, protect, detect, respond, recover
(according to NIST Framework [2]):

Industry sector respondents overall agreed with the working cycle although for the sector this breakdown is considered as too basic. It represents just one dimension and should be complemented with other factors such as business processes, technology dependencies, risks and threats, appropriate investments, etc.

Board of Directors

As for the other sectors, in industry/manufacturing, the lack of investment stems from the fact that **Boards lack understanding on cybersecurity issues**. There is potentially a **gap of appropriate KPIs to demonstrate to them the return of investment**. Although it seems that there is already quite a good communication between CISOs and their Boards in the sector, it can always be improved with **CISOs learning to better communicate to their Boards in a non-technical manner**, reporting in a simple and clear way. There were also **suggestions to set up a cybersecurity committee or making one Board member accountable to understand the cybersecurity issues**.

CISOs also need to **develop awareness campaigns for all employees** creating a good cybersecurity dashboard to help communicate to the Board level, including reporting risk analysis of the main business assets.

Cooperation Aspects and Challenges

For the industry/manufacturing sector, current regulations are not sufficient as they rely more on existing governance structures within their organisations. Although when it comes to used solutions, CISOs responded it being **quite important to use EU certified solutions as a go-to option**, but **only if the European solutions offer the same quality, set of features, etc. than non-European solutions**. Their go-to criteria for procurement are certified products, costs and system integration.

Like in other sectors, the industry sector is also open to cross-sector cooperation. CISOs **suggested setting up a European association** that would organise webinars, exchange of experiences, mailing lists, etc. to **create a network of CISOs with the right level of trust** to participate in exchange

groups. Unlike the **CERTs that lack transparency**, industry **CISOs would like a direct communication channel whether within an ISAC, through mailing lists or a common platform** (to keep the CISOs informed and allow information sharing).

Public sector/Government

Cybersecurity has become **increasingly important for the public sector with the implementation of technological infrastructure and the use of the cloud**. When it comes to disruptions, even governments or governmental agencies are impacted by damage to their reputation, in addition to the disruption of activities that bring up the costs of requalification to restart the activities.

The public sector also suffers from the threats common to the other sectors, although there is one **new element particular to the public sector which is cyberterrorism**. This is of the utmost priority for each Nation State and national public administrations need to also face attacks considered as cyberterrorism from state-actors, non-state actors, or hybrid actors.

Top threats

Legend

Here cyber hygiene in addition to awareness also includes human errors due to lack of resources and improvisation.

Top Challenges – Public Sector/Government

- ✓ **Continuous updating** and disruptive technologies
- ✓ **Lack of awareness** across the entire organisation
- ✓ **Lack of CISO empowerment**
- ✓ **Lack of resources** according to business expectations because of lack of budget.

In-Company and Governance Challenges

Certification

The **lack of budget also impacts the certification aspects**, not allowing personnel to be certified. Instead, administrations prioritise upgrading security skills before any certification. This approach allows to **consider information security by design where administrations implement security**

education in general so that the adoption of new security measures is not seen as an obstacle in the development of the business activities. It is a matter of company culture and maturity.

CISOs responding to the survey almost unanimously mentioned **not yet using cyber ranges** inside their organisations, while **authentication is considered as very important**.

Code of Conduct for CISOs

The proposal to create a Code of Conduct for CISOs linking it to corporate social responsibility (CSR) raised mitigated responses from the CISOs. **Half of them were pro-Code and pro-penalties as enforcement**. The other half showed more scepticism mentioning that it would still be better than nothing at all.

Board of Directors

In general, it seems that the **position of the CISO is not consolidated within the public organisations**, with them also **lacking support from their management**. As for the other sectors, there is the dire need to educate management about risks. The public sector CISOs **suggested setting up a new modern, simple and understandable risk methodology, which could be a good start and improve the risk management process**. Boards remain ignorant to dangers, mostly because **CISOs do not present enough information to the Boards, with governmental restrictions adding to the issue**. CISOs need to explain that cybersecurity is not just a technical issue and they should be **given the weight to implement their decisions with the necessary resources – economic, human, autonomy of decision and of work, involvement in the organisation's strategy**. **CISOs need to sit at the Board** and be able to explain problems in a simple and clear manner. They should also **ensure the education, training, awareness, and sensitisation about cybersecurity of all Boards members.**

CISOs working lifecycle:
identify, protect, detect, respond, recover
(according to NIST Framework [2]):

Only half of the public sector respondents agreed with the proposed order saying that all aspects are equally important. The other half mentioned prioritising Detect/Respond/Recover before Identify and Protect, explaining that one cannot be prepared to unknown situations. We do not have further data to explore the reasons, although we suspect that this difference in approach might be dependent on the country and the maturity of the public administration.

Cooperation Aspects and Challenges

When it comes to regulation, the public sector does not get enough recommendations. There is a **common wish for harmonisation and application of regulation to all structures** (even the smallest), and for a clarification of the roles and responsibilities of CISOs. **EU regulations should be more complete and more detailed** to avoid cross-border and cross-sector fragmentation, **so that Member States do not have to publish additional regulations to complete the European ones**. This is where the heterogeneity appears. The public sector is also willing to learn from the more mature sectors, although there are still differences between sectors as some of them do not even have cross-border activities.

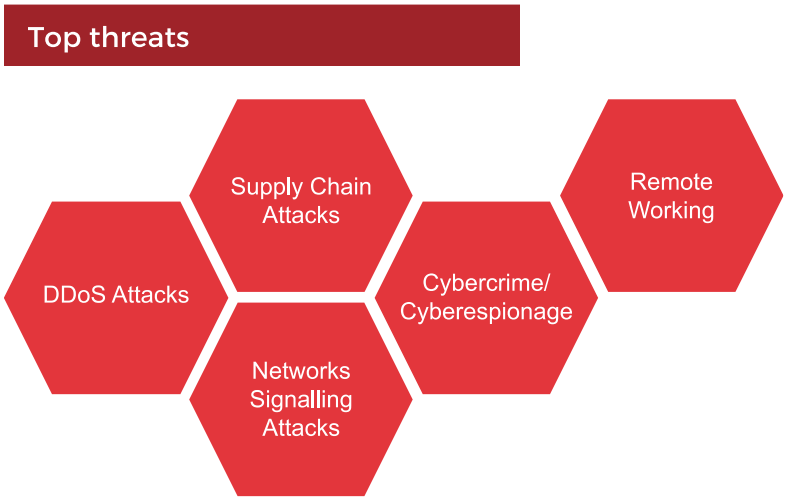
To better learn each sector's specificities and cross-sector similarities, public sector CISOs **recommended developing a CISO network managed by a national/EU authority**. This channel would empower CISOs within companies, allowing them to share information with national authorities. It would also open the possibility of establishing essential collaboration with law enforcement agencies.

Finally, it is evident that national public administrations find it of the **utmost importance to use EU certified products**. And if there are not EU solutions, then they can at least **refer to nationally certified solutions until EU certified solutions a created**. Public CISOs also value performance and costs as main criteria, although they admit that for the moment, **European products and solutions may not cover all needs**.

Telecommunications

Along with privacy risks, **cybersecurity is a high priority** in the telecommunications sector. Disruptive aspects of cyberattacks are numerous:

- ✓ *Reputational*: loss of sales and loss of customers
- ✓ Disruption of business operations
- ✓ Heavy *financial losses*: contract losses, money losses, theft of financial information
- ✓ *Costs* for repairing damaged systems, networks and devices.



Among the common cyberthreats and challenges faced, it is intriguing to find cybercrime and cyberespionage as one of the focal points of the telecoms sector.

Legend

While "Remote working" may not sound cyber-threatening at first glance, for the telecoms sector, the implications are significant: employees' vulnerability to social engineering, employees' remote access to production data, insider threat, etc.

Top Challenges – Telecoms Sector

- ✓ **Budget restrictions**
- ✓ **Culture reluctance to invest time/effort** in embedding security and privacy by design and by default
- ✓ **Legacy technologies**
- ✓ Dramatic **increase in the amount of data being processed**.

In-Company and Governance Challenges

Certification

Special focus on authentication

Authentication is of the utmost importance. Some of the methods used are IAM, PAM, 2FA, MFA, etc. The sector CISOs are working towards a holistic approach but it is a work in progress.

To face these threats and challenges, the **telecoms sector relies heavily on certification** and its CISOs seem to be fully involved in the process. Their goal is to **merge certification requirements with business needs** and avoid plain repetition of audit-like questions.

Moreover, **cyber ranges are widespread** in the sector and fully overseen by CISOs.

Code of Conduct and Board of Directors

CISOs working lifecycle:
identify, protect, detect, respond, recover
(according to NIST Framework [2]):

Telecoms CISOs fully agreed on the order and mentioned that all aspects are equally important. However, they also added another equally important aspect for them in telecoms: Anticipate/proactivity.

With all the heavy lifting that CISOs do, respondents considered the implementation of a Code of Conduct a **great idea to ensure a good cybersecurity posture**. However, respondents deemed that penalties are already sufficiently in place with regulations such as the General Data Protection Regulation (GDPR) [4].

In any case, minimum requirements in the Code should cover a **continuous assessment by CISOs of risks with effective solutions and the incorporation of KPIs to measure the risk optimisation on a regular basis**. This brings up the topic of the relations between CISOs and their Boards. Respondents mentioned having an acceptable support but there is definitely a lot of room for improvement. As for the other sectors, **telecoms' Boards impose general restrictions and prefer to follow other business priorities and the market pressure**.

CISOs should manage the protection of information assets and technologies but also adequately communicate about risks to Boards and employees and provide possible solutions from a security perspective and about functionality. For this, there is the **need to build a common KPI framework to allow CISOs to report in a "business" language but also to involve other departments**, especially financial and legal, in addition to the digital one, to make a holistic risk assessment.

Cooperation Aspects and Challenges

The telecoms sector considers as **critical factors for regulation the need for clear requirements, regular audit cycles, knowledge transfer, continuous improvement and study of the latest market trends and solutions**. Especially knowledge and threat solutions transfer through a transparent EU entity (such as ECSO and ENISA – both were mentioned by the respondents) would be more than helpful, in particular when tackling cross-border and cross-sector aspects. The **transparent and independent authority should ensure the confidentiality of the collected and shared information between registered CISO members in order to generate trust**. The entity would also allow a useful and important collaboration with law enforcement agencies where CISOs could assist in the creation of case studies and better enhance cybersecurity in practice.

On the **procurement** aspects, telecoms CISOs value performance and costs. They also consider the origin but **made in Europe cybersecurity solutions are limited**. However, they deem it is of **major importance to rely on EU certified solutions for the management of sensitive data and for effectively addressing the supply-chain security threats**.

Transportation (air – rail – sea – road – space)

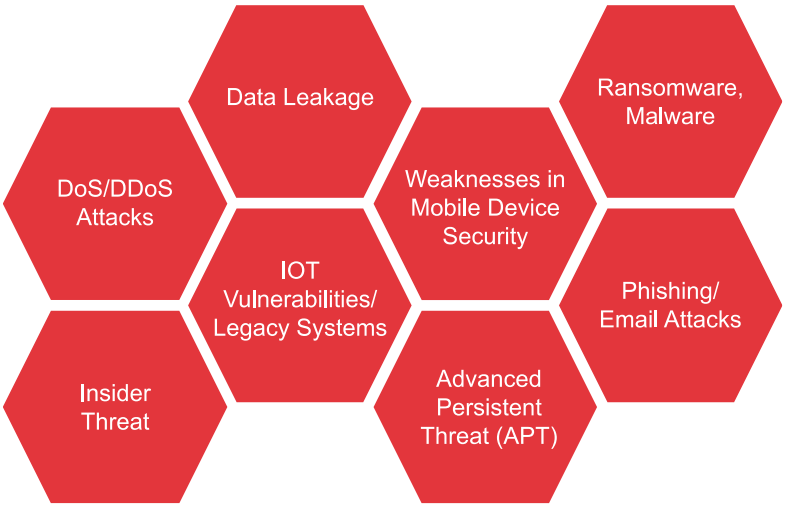
The transportation environments are **highly dependent on IT and OT infrastructure**, so the protection of critical infrastructure (CI) assets is paramount for business continuity. However, although in many cases the concept of **cybersecurity** is considered as important and recognised as a major element to prevent cyber threat and allow business continuity, it **still lacks the proper funding to fight against the many disruptive aspects** in the sector:

- ✓ Break of commercial operations and *service unavailability*
- ✓ Competitiveness
- ✓ *Safety and security* issues (including human life)
- ✓ Environmental issues
- ✓ *Financial losses*: economic impact and costs stemming from the recovery for replacement of essential assets
- ✓ *Reputational* damage: user perception after an attack, lack of trust
- ✓ Data and information theft
- ✓ *Legal consequences* and regulatory compliance.

As much as the **disruptive aspects are numerous**, so is the **variety of threats and challenges facing the transportation sector**. It is worth mentioning that when tackling the transportation sector, one does not approach a unique sector but rather a set of **5 sub-sectors: air, rail, road,**

sea, space. As mentioned in the beginning of this report, we received responses from all 5 sub-sectors.

Top threats



Top Challenges – Transportation Sector

- ✓ **Lack of time** to implement controls and systems and to implement a comprehensive cybersecurity strategy
- ✓ **Lack of awareness** from both the management and the staff; need for employee trainings
- ✓ **Lack of budget** due to restrictions
- ✓ **Lack of qualified and/or trained personnel**
- ✓ **Complexity and legacy of the systems**.

In-Company and Governance Challenges

Certification

With all these threats and challenges, transportation sector CISOs have a vast array of responsibilities to secure their companies. Overall, a big **majority** of respondents mentioned that their **companies are certified** and that the **CISO is heavily involved in the process.**

However, they still **strike a balance between certification and agility of processes and operations**:

Special focus on authentication

Authentication is considered of the utmost importance and transportation CISOs aim for a holistic and centralised approach. The most used authentication appliances are LDAP/AD, 2FA, MFA, SSO, Active Directory, MS Intune, F5 Big-IP. A small detail worth mentioning is that despite the centralisation aims, ATMs (Air Traffic Management) are standalone and isolated from the LAN and the Internet.

- *By classifying assets and priorities* (knowledge of technology, IT processes and business processes; also, good communication from CISOs to the rest of employees)
- By simplifying the process related to the compliance of the certification goals and controls
- By having a practical view and less paperwork to focus on the main and weak issues and design an action plan to cover the minimum needs to get the certification.

In addition, an overwhelming majority of CISOs responded carrying out **frequent cyber range exercises.**

Code of Conduct for CISOs

A large majority of CISOs mentioned being favourable to a CISO Code of Conduct, saying that it **would provide a minimum acceptable level of cybersecurity posture for each organisation and especially the OES**. They are also in favour of penalties in case of non-compliance as a necessary evil (**carrot/stick perspective**), although there was also a minority opinion rather valuing motivation and awareness as better incentive than penalties which could lead to bad practices.

Moreover, by **integrating Corporate Risk Management with Cyber Risk Management** (e.g., including cyber risks into the Corporate Risk Governance Model), it is also important for a good governance to **educate senior management about IT security issues** also in terms of trade-off between costs of security measures and of potential damages. CISOs need to continuously monitor and evaluate by performing information security audits and risk assessments. In turn, CISOs should expect a full support from their Boards. Currently, **transportation CISOs seems to receive adequate support but there is always room for improvement.**

Board of Directors

Despite the maturity of the transportation sector on cybersecurity topics, even transportation sector Boards do **not invest sufficiently in cybersecurity**. This fact is **due to a lack of cybersecurity risk assessment with quantitative economic impact and the fact that not all investments are related to a legal requirement**. Cybersecurity is a relatively new field, so **it is difficult for the management to understand and they do not see a direct return of investment because cybersecurity does not directly generate profit**. On top of that, **Boards also do not understand the risks of cyberattacks**.

CISOs working lifecycle:
identify, protect, detect, respond, recover
(according to NIST Framework [2]):

Transportation sector respondents agreed with working lifecycle mentioning that all aspects were of equal importance. However, there were some discrepancies on Identify which in some cases was completely overlooked or considered as the least important, and in other cases, as the most important among all the aspects.

For all these reasons, **CISOs need:**

- ✓ To bring a **direct channel of communication to the Boards** and create awareness programmes for the employees.
- ✓ To **align with human resources departments** for spreading the cyberthreat awareness across the company.
- ✓ To be taught to **better communicate (in terms of business and economic impact)** and involve Boards in cybersecurity processes (e.g., exercises and simulations of cybersecurity incidents).
- ✓ To help set up a specific committee for communication between Board and CISOs or **making reporting to one Board member responsible for the security across the company**.

Cooperation Aspects and Challenges

At the European level, transportation CISOs mentioned that guidelines should be laid down on how critical infrastructure should be managed. The NIS Directive, which so far has been operational for the last three years, does not tackle in-depth aspects on OES in terms of best practices and common concerns and does not define the cybersecurity controls, methodology or processes to apply to OES (the implementation instructions are missing).

Procurement

The respondents also consider **using EU certified cybersecurity solutions as highly important**, mainly because there is **trust among EU countries** which provides a higher confidence level. There is a legal normative that provides organisations with sufficient guarantees regarding the protection of sensitive information and privacy. Among the criteria privileged in their procurement choice of cybersecurity products and solutions are **system integration and maintenance, offered functionality and performance, costs, and certification of the product/reliability**.

Information sharing

Finally, on the topic of cross-border and cross-sector cooperation, CISOs advocate **collaboration between EU-wide and nation-wide authorities and OES**, aiming for a homogenisation of standards and controls and the creation of a trusted environment to share information and experiences between countries and sectors.

To this effect, it would be useful to **define a common framework with the same compulsory cybersecurity controls in every EU country and learn the efficiency in the control and measurement mechanisms from more mature sectors**. To trigger such a cooperation, the CISOs came up with different recommendations:

- *Create a European CISO body* or a modern security information sharing framework involving CISOs such as a European CISO Portal
- *Create a dedicated information sharing platform* with subgroups for each OES sector (to share on threats, strategies, tools, countermeasures, etc.)
- Improve collaboration with CERTs as there is currently a clear lack of transparency from them
- Create information sharing mailing lists, etc.

The possibilities are numerous, the only thing is not to be afraid to share information. The coordinating Europe-level entity could periodically check the exposure of each OES and alert CISOs for possible threats in their environment in **all anonymity without needing to share the origin of threat**.

As for the other sectors, such a setting would also enable a collaboration with law enforcement agencies that would be quite useful, although **transportation CISOs need to see a full collaboration from A to Z for it to be meaningful and worth their time investment**.

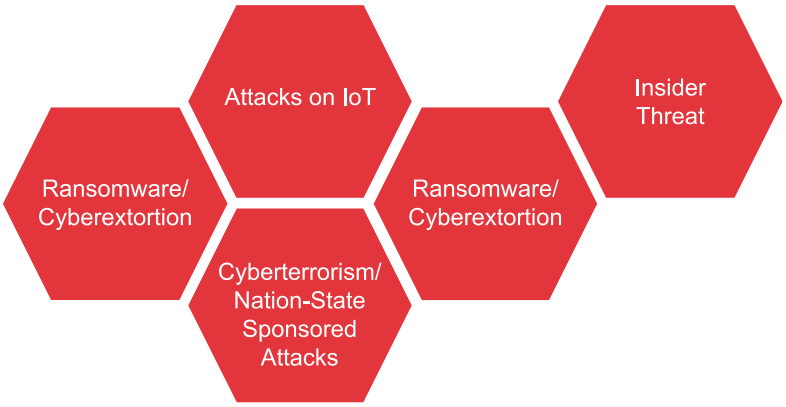
Utilities (water)

The lack of maturity of the utilities sector when it comes to cybersecurity is showcased in the mitigated responses when enquiring about the importance of cybersecurity for their sector. **Half of the respondents mentioned that cybersecurity is very crucial, while the other half answered that it is not crucial at all**. And yet, it does not prevent cyberattacks from bringing disruption to the sector:

- ✓ Reputation
- ✓ Break of business continuity
- ✓ Critical assets destruction
- ✓ Noncompliance *fines*
- ✓ *Environmental* impact (because of the disruption of services) that could lead to *public health issues*.

In the same vein as for the public sector, it is interesting to note that the **utilities sector is also a major target for cyberterrorism**, raising the fact that any issues falling on the sector directly apply under the national sovereignty prerogatives.

Top threats



Top Challenges – Utilities Sector

- ✓ **Protection of the industrial devices/data/network segregation**
- ✓ **Lack of cybersecurity awareness** and understanding from Boards
- ✓ **Lack of user education**
- ✓ Involving the **conflicting interests between IT and OT** staff
- ✓ Increase in the **sophistication of cyberattacks and the continuous evolution of technologies**, while aligning the cybersecurity strategy with the business objectives that are required.

In-Company and Governance Challenges

Certification

The Utilities sector's priority is to ensure the continuity of activity, so the same priority should be given to those certification security controls that imply a better and effective level of organisation and protection of the systems, discarding other controls that provide little value at the security level and that pose an obstacle and generate less agility. In terms of certification, **half of the respondents mentioned that certification is less important than knowledge, while the other half considers certification as very important and needing more visibility**. In all cases, the **CISO is completely involved in the processes**, including in the **widespread use of cyber range exercises** in the sector.

Code of Conduct for CISOs

The Utilities CISOs surveyed indicated that they did not have any concrete opinion about the implementation of a Code of Conduct for CISOs. However, they provided several recommendations on how to implement or to improve the company governance. There is a **need to create a security governance framework that could be an auditable reference framework** (also for comparison purposes between companies) **and raise C-level security awareness**. The framework would cover a transversal across-the-company security policy that would include the requirements and procedures for cybersecurity and business continuity.

CISOs working lifecycle:
identify, protect, detect, respond, recover
(according to NIST Framework [2]):

There was an overall agreement on the order and equal importance of each aspect from Utilities sector respondents, although, in some cases, 'detect' and 'respond' seemed to be considered as the most important aspects to achieve before 'identify' and 'protect'.

Overall, in the Utilities sector, the **CISO position needs to be consolidated and CISOs need more authority**. Plus, there is always the need to make cybersecurity a priority in the organisation and get the needed support from the Boards as a result. The level of support from Boards seems to be mitigated given the answers from the respondents and they generally **advocate improving the communication between CISOs and Boards for a greater sensitivity and harmony** on the company's problems at the security level.

There is a **general lack of knowledge, understanding and investment by Boards on cybersecurity issues because they do not see a direct return on investment and consider it as a waste of money**. That is, until an incident happens. But security is a common effort, and it can only be reached by raising awareness and providing more information/education. Although that would also require the CISOs to get the necessary authority within the organisation.

It was also **recommended that CISOs participate in all management meetings and committees, make frequent reports to show alternative costs and the risks, establish an annual awareness plan for the staff and Boards** where the importance of cybersecurity is highlighted in the threats and risks that the company faces. It could also be useful if companies that have been targeted by cyberattacks share their experiences (from CEO to CEO, not publicly).

Cooperation Aspects and Challenges

The utilities sector especially relies on the NIS Directive at the European level, but there is the need to bridge the gap between the public sector and corporate best practices. Moreover, the NIS needs to homogenise criteria to define strategic sectors and appoint OES.

The utilities sector is open to cross-sector and cross-border cooperation via the promotion and facilitation of a **European forum and collaborations between CISOs from different EU countries**. To this effect, a **platform and regular contacts between CISOs** (meetings, secured messaging services among themselves, etc.). would be a start. Forums and associations would also be good enablers for the interpersonal aspects. Another possibility to enhance cooperation would be through legislation and CERTs/CSIRTs.

Finally, on the procurement of cybersecurity solutions topic, Utilities' CISOs privilege cost and performance to be the most important criteria. They also **prefer EU certified solutions which would offer sufficient regulatory and legal guarantees, but it is overruled by the performance criterium.**

Other (retail – consultancy)

A few responses were also received from the "luxury" and "retail" sectors, and "consultancy services covering different sectors".

Overall, responses provided by the CISOs of these sectors were **aligned with the analysis of the other sectors**. There were no different or disruptive opinions on any of the topics and the recommendations on the CISOs conduct/roles/responsibilities, their relations with Boards, and on cooperation and information sharing were the same as what was shared by respondents from the other sectors.

Post-analysis remarks

Based on the analysis in the previous sections, some key observations from the survey results are worth noting:

- ✓ Depending on sectors, some **respondents carefully filled in all the sections** of the survey with complete answers to all questions, while **others considered some questions irrelevant, or skipped them altogether**. This led us to speculate that the **maturity** and involvement of the sector in cybersecurity could be at the cause of it, and especially the sector's level of contribution and preparedness in cybersecurity.
- ✓ Some received **answers** to the survey questions were particularly **generic** in nature. This statement is valid when only **compared to more detailed and comprehensive answers** from other respondents and could equally imply that on many aspects these sectors – all sectors except energy, finance and transportation for which we have received a larger number of entries, as referenced in Table 3 of this report – are far from being **mature** on the topic of cybersecurity.
- ✓ As seen in the tables in the previous section, for some of the sectors (all sectors except energy, finance and transportation), we did not receive a large number of answers and we could ask ourselves if they can be considered as a sufficiently representative sample of the sector itself, though their responses are showing relevant issues. In any case, we tried to find a **common narrative** and sum up in the best way possible the received responses.
- ✓ One **limitation of our survey** was that we failed to ask **which country the CISO** is operating in. Many variations of answers within the same sector on the same topic could potentially be dependent on the country of implementation, and thereby dependent on its existing regulations and rules. It would have been interesting to provide this additional layer of analysis and understanding.

- ✓ Finally, for each of the covered sectors, we have highlighted their Top Threats and Top Challenges. Although not exhaustive as we know that these sectors are impacted by other cyberthreats and challenges, it is interesting as it showcases the prioritisation for each of the sectors. We therefore regrouped all the covered threats in a dedicated table (ref. Table 5) in a way that shows the level of prioritisation of these threats for the different sectors, which could serve as food for thought concerning the normalisation of some of the threats.

Table 5

SECTORS / THREATS	ENERGY	FINANCE	FOOD	HEALTH	MANUFACT. / INDUSTRY 4.0	PUBLIC SECTOR	TELECOMS	TRANSPORT	UTILITIES
Ransomware	X	X	X	X	X	X		X	X
DDoS attacks		X	X	X	X		X	X	
Social engineering attacks	X	X	X		X	X			
Malware / virus		X	X	X	X			X	
Phishing			X	X		X		X	X
Insider threat	X	X				X		X	X
Data leakage / data loss				X	X	X		X	
Data breaches	X	X							
Supply Chain Attacks					X		X		
Cyberterrorism						X			X
Third Party Breaches		X							
Unauthorised access		X							
Data/Critical info theft			X						
Identity Theft			X						
Technological complexity	X								
Obsolescence/Vulnerability Management				X					
IP theft / IP leakage					X				
Cyber Hygiene						X			
Advanced Persistent Threat								X	
IOT Vulnerabilities/ Legacy Systems								X	
Weaknesses in Mobile Device Security								X	
Cybercrime / Cyberespionage							X		
Networks signalling attacks							X		
Remote working							X		
Attacks on IoT									X

Cross-sector approach: horizontal recommendations

It is quite evident that many topics, challenges and recommendations in the survey overlap across the different sectors. We chose to compile these overlapping topics in a cross-sector analysis to come up with general horizontal recommendations applicable to all sectors. We identified **5 general topics common to all sectors represented in the survey analysis**.

1. On CISOs Roles and Responsibilities
2. On budget and investments
3. On information sharing
4. On company culture
5. On staffing

1. On CISOs Roles and Responsibilities

In the survey, we asked CISOs whether they think it would be useful to have a **mandatory Code of Conduct** in place to ensure a cybersecurity posture and Corporate Social Responsibility (CSR) in organisations, and the suggestion was met very favourably by all respondents.

The Code should be both like a **reference framework** to which CISOs could refer to **legitimise their decisions and actions in front of their Boards**, and a **training curriculum** to help CISOs face the challenges they face on a daily basis. In turn, this would allow CISO to get legitimacy in their decisions and security strategies for companies, but above all facilitate their daily work and consolidate their position.

- ✓ Allowing CISOs to directly sit at the Board with defined legal responsibilities
- ✓ Allowing CISOs to directly report to a Board member specifically designated to be in charge of cybersecurity topics, although the perimeter of action and the responsibilities for which the CISOs respond to their Boards, to the shareholders and to the competent authorities as a "legal person" must still be defined
- ✓ Allowing CISOs to set up specifically designated reporting committees directly under Board orders.

Of course, in this case, the Code alone would not be enough. To add to that, **CISOs must be given the weight to implement their decisions with the necessary resources – economic, human, autonomy of decision and of work, involvement in the organisation's strategy and a direct channel of communication with their Boards**. The latter could be implemented by:

CISOs must also learn to **report to their Boards by quantifying security risks in terms of economic and financial losses, and link cybersecurity to business continuity**. For the moment, **CISOs have a tendency to report in too technical terms, and cybersecurity still being a relatively new topic, there is a lack of understanding from the Boards**. With the evolving cybersecurity threat landscape, the growing sophistication of cyberattacks and the new disruptive technologies, CISOs need to be on top of their game to effectively protect their companies and organisations, which includes protection of critical infrastructure, of network information, of data, and in some cases of the human lives working for the companies. In order to have a holistic approach to these challenges, CISOs cannot tackle them all by themselves, they need to be backed by their Boards.

“Identify, protect, detect, respond, recover” is the working lifecycle of a CISO as presented in the NIST Framework. As we can see, these aspects do not solely cover the technical aspects, so it would be **wrong to assume that CISOs are only technical people. There is a full range of skills, both hard and soft, that CISOs need in their position**. There is an overall agreement from CISOs on the order and equal importance of these 5 aspects, although sometimes we have noticed slight changes in the order of the priorities. It depends on some sector specificities but most of the time on the maturity of the company and of the sector itself. While the most mature ones seem to agree with this presented order, sometimes there is swapping of the priority between Identify and Protect with less mature sectors seeming to prioritise proactiveness with Detect first, and then dealing with the rest afterwards. For the most critical sectors, Respond and Recover remain at the core of their preoccupations in ensuring avoiding life-endangering, societal and environmental damages and allowing smooth business continuity.

It is **widely agreed that a Code of Conduct would be a good start in helping CISOs and raising awareness about the wide range of their responsibilities, especially in front of their Boards**.

It is important to note that while the idea of the Code was welcomed favourably, the idea of penalties attached to it in case of non-compliance bringing up the liability of the CISOs was advised against by the respondents and approached with caution. Most CISOs mentioned that **awareness would be a more favourable course of action than penalties** that could become the source of bad practices and/or directly breach the CSR terms. Others accepted the idea of penalties as a necessary evil for compliance and liability (both on CISOs and on Boards).

Penalties strongly depend on the fear from CISOs of having the correct tools to act, without which they would only have responsibilities with no real possibility of reducing risks. The most important issue remains in the allowed budget granted by their Boards. **If CISOs do not receive adequate budgets to reduce the risks, then CISOs fear to become personally accountable for incidents because of reasons not attributable to them and independent of their will**. For this reason, CISOs who do not have sufficient budgets or sources often refer to certifications and “consulting firm reports” to lighten the burden and weight of their responsibilities.

2. On budget and investments

The **lack of investment and low budget attribution by Boards** to cybersecurity was without doubt a unanimous and ominous commonality across all sectors. The general agreement to explain this fact is that Boards lack knowledge and understanding on cybersecurity matters. They usually

do not care about cybersecurity or fail to understand the true risks attached to it. This is because **Boards think in financial and economic terms, ensuring business continuity, and they do not see the link with cybersecurity because cybersecurity does not show a direct return on investment**.

With such an approach, companies and organisations remain vulnerable because the CISOs (or whomever is in charge of cybersecurity inside the company) do not get the necessary resources to ensure a holistic protection. This of course increases the risks of incidents and cyberattacks, and Boards tend to realise this only after an incident has happened.

This difference of perspective happens because companies aim for profit while Information Security aims towards reducing risks that are often intangible and constantly changing. Companies can and must **invest in Information Security by setting objective minimum goals** (defined by sector) that are **tangible, stable, and measurable**. Moreover, collective interest cannot depend only on companies' profit and market investments; it also needs to be **facilitated by the public sector because corporate cybersecurity has an impact on the security of countries**. For example, **for critical infrastructures with impact on national security and society, the national administrations could provide facilitations for the procurement of needed resources**.

There were **several suggestions to remedy to the situation and bring Boards to be more cybersecurity-savvy**. The most common suggestion was for Europe to **implement a reporting framework for CISOs to their Boards based on concrete KPIs that would include a risk analysis on the main business assets**. There could even be a modern, simple, and understandable risk methodology which could be a good start to improve the risk management process. The KPIs would not only help CISOs to report in non-technical terms, but also allow Boards to concretely see their return on investment.

One thing that Boards need to keep in mind is that in cybersecurity, **zero risk does not exist**. Cybersecurity is an ever-evolving field and buying just one solution and complying with certification guidelines by the book is not enough. It requires constant follow-up and investment, constant auditing and management of the risks, and a **constant assessment of the company's vulnerabilities**.

3. On Strategic Information Sharing between CISOs

Before proceeding to the recommendations in this section, it is important to highlight the **distinction between operational information sharing** and **strategic information sharing**. In the first case, **technical/operational information** can be handled through ISACs, CERTs, CSIRTs or a network of SOCs – the European Commission is currently working on establishing it at the EU level – so that the information **is shared in real time in an anonymised and centralised way through computerisation** (e.g., MISP). For this level of information, reaction times are fundamental. On the other hand, **strategic information/intelligence sharing** that is necessary **to take place at the CISO-level (or equivalent) covers information about market priorities, threat assessment, threat landscape evolution, geopolitical issues, cybersecurity trendscans**, etc.

For this type of information, the strategic implications of the landscape for the companies are fundamental.

CISOs are extremely aware of the gaps and limitations of information sharing and their responses confirmed the observations of the ECSO UC in their "Green Paper on CISO's Challenges and Threat Intelligence Sharing" (ref. [1]). To summarise, there is indeed a **lack of cooperation across sectors and across borders**. Private-private cooperation remains within the confines of one sector and public-private cooperation remains either within the sector (e.g., through sectoral associations) or within the borders of the country. Only public-public cooperation raises to the European level. But even in this case, **CISOs complain about a lack of return of information from the public to the private, and CERTs and CSIRTs overall lack transparency.**

Given these elements, it is clear that **CISOs unanimously call for the creation of a network of CISOs under the umbrella of a neutral European entity that would ensure the coordination of the network and of the shared information across sectors and across borders.** The information sharing within the entity could also be supported by a specifically designed platform.

The CISO network would **establish common practices in areas that concern all sectors** (governance, operational and cybersecurity risk management, business continuity management, third party risk management, response plans analysis and reporting) and provide recommendations to harmonise EU regulation and standards across Member States.

Several respondents mentioned ECSO as a potential organisation that carries this neutrality and could be at the source of the network as a coordinator. There is a clear gap to be tackled here that ECSO has already started working on with the creation of its Users Committee. But there are improvements to be made and to come (**see Conclusion**).

4. On company culture

It is commonly agreed on that in order to align cybersecurity with business priorities **CISOs not only need to manage up to their Boards, but also manage across to the employees/rest of the company or organisation.**

Company culture and evolution of mentalities remain extremely slow, and it is still a long road. CISOs are often met with resistance when trying to implement a cybersecure culture in their companies and push employees to have a more cyber-hygienic workplace environment.

It is still important to contextualise and keep in mind that every industry has widely different needs. Companies that have a great culture with IT tools within their core business will find it easier to adopt training programmes or risk mitigation tools. B2C (business to customer) companies or companies that use IT tools only in some company departments have much more difficulty in increasing the level of awareness.

To help with this, it is **recommended for CISOs to actively collaborate with human resources departments to elaborate company-wide trainings and awareness programmes**. With the backing from HR, these trainings should be made compulsory for all employees and regular updates on these trainings should be followed-up on depending on the cybersecurity strategies decided by CISOs on an annual basis.

One final point that was also mentioned several times is the **seemingly existing antagonism between IT and OT staff because of conflicting interests**. The responses provided in the survey did not allow us to detail this issue, but it is something that needs to be further analysed. One possible explanation based on previous ECSO observations is that the issue stems from the difficulties of merging physical security with digital security. Traditionally, physical security would prevail. However, with the evolution of technologies, digital security has been taking more and more space, to the point of co-dependency between physical and digital security. The difficulties in merging both remain in the human factor resistance, the discrepancies in the life-cycle between hardware and software, as well as the frequency difference between software/hardware systems update management.

5. On staffing

Finally, this last topic is less of a sectorial or cross-sectorial issue, and more of a general gap in cybersecurity. Several reports have been published on the topic by ENISA, ISACA and other organisations.

There is a **huge cybersecurity skills gap in the world, and especially in Europe**. This gap is even more noticeable in the sectorial applications of cybersecurity where sectors also complain about the skills shortage and talent retention.

This issue depends on the Information Security sector. **Academic training in this sector does not necessarily work for technical personnel because evolution times are faster than didactic standardisation**.

The various types of existing information security professional skills are not defined, and they are usually summarised under the generic name of "Cybersecurity Professional". These professional skills should be identified in different profiles and different training programmes to avoid having hundreds of information security professionals all gathered under the generic name of "Cybersecurity Consultants". It would be important to make a professional registry that collects all of them and formalises the perimeters of the job profiles. The ongoing work by ENISA's Ad Hoc Working Group on Skills Framework could be important in this regard.

Europe is already on top of many initiatives and programmes for awareness and to attract more people to cybersecurity education and professions. But there is always more that can be done, and **Europe needs to invest more in cybersecurity talents**.

ECSO has been working and continues to work on this issue in its WG5 on 'Education, Training, Awareness, and Cyber Ranges'. A dedicated Task Force "European Human Resources for Cyber" (EHR4CYBER) has also been established. Through WG5 and EHR4CYBER, ECSO is contributing to addressing the cybersecurity skills gap by:

- Gathering cyber ranges across Europe and highlighting the different purposes that a cyber range can be used for, i.e., by academia (educators) to improve teaching and learning (apply hands-on training) and by HR/recruiters to assess competences through simulations. ECSO has also published a paper on "Understanding Cyber Ranges: From Hype to Reality" [5] which aims to provide a better understanding of cyber ranges and with

a set of criteria that can be used to better identify and select suitable cyber ranges to meet specific needs and requirements.

- Bridging the gap between academia and industry in delivering education & training solutions to better meet market needs. In addition to releasing a Gap Analysis paper [6], ECSO is working on developing practitioner guidelines for cybersecurity course structures, descriptions, topics, and learning outcomes. This document will provide minimum level model curricula for cybersecurity courses and will help address industry needs when it comes to the skills and competence development of the cybersecurity workforce.
- Developing and advocating skills and abilities verification approaches to satisfy the increasing needs of the cybersecurity job market. Having mapped the cybersecurity professional certification landscape in an Analysis Paper [7], ECSO WG5 realised the need to develop agile and practical solutions to competence assessment that can complement existing certification framework approaches. This includes skills verification through the use of cyber ranges, an initiative to develop an assessment of the top 10 abilities needed for specific job roles and suggesting practical scenarios/simulations to test them (CISO could be one of the roles to be assessed), as well as tasks dedicated to better understanding HR needs and practices. ECSO is collaborating with the European Competence Centre Pilot projects and ENISA on surveying HR and recruitment specialists in order to get a better understanding of experiences and practices when it comes to hiring cybersecurity experts and collecting some initial cybersecurity recruitment data for Europe (which does not currently exist). This would allow all relevant stakeholders in this area to better adapt activities, support HR departments/hiring managers, and co-create solutions to meet market demands.
- ECSO is also contributing to the ENISA Ad Hoc WG on Skills Framework where work is being done on defining job roles (including C-level) and mapping these against needed competencies (using the eCF framework as reference) to arrive at a skills framework specifically adapted to the cybersecurity market in Europe.

Conclusion

Many of the topics tackled in this report were already part of ongoing discussions and in the general public awareness in the cybersecurity field. The ECSO UC members themselves have already tackled some topics in previous observations and publications. However, ideas have been scattered, remaining unconfirmed or just mentioned in passing.

With the survey, the UC's aim was to confirm or disprove these topics, and especially bring awareness to the implications of being a CISO and the challenges they experience. With this analysis report, there is now a solid foundation to concretely start working on tackling many of these challenges.

This is the reason why **ECSO has made the decision to take action** and to actively contribute to facilitating the cybersecurity field for Users and OES and consolidating the positions of CISOs.

With the already existing UC, ECSO will announce the creation and launch of the CISO European Community (the European network of CISOs across sectors and European countries) in the second half of 2021 to help gather all European CISOs in one setting. The network's purpose will be to build trust among CISOs, allowing frequent exchanges between them and helping in the cross-sector and cross-border information and intelligence sharing. To this effect, the **UC Chairs**, Intesa Sanpaolo – an Italian bank, financial sector – and Electricité de France (EDF) – a French energy provider, energy sector – **are already partnering to also create a platform designed specifically for CISOs that will become part of the network created by ECSO**.

The ECSO UC is also in regular contact with the European Commission and the European Parliament advising them on political, regulatory, and legislative matters, as ECSO is a privileged partner of the European Commission. We are currently closely following the evolution of the discussions on NIS Directive 2 for which the UC has published a position paper [8] in the past and provided its recommendations directly to the Commission.

Finally, we would like to note that we are aware of an **important topic missing** in this document which is about the SOCs and the ongoing discussions currently happening at the EU level on the creation of a **European Network of SOCs powered by Artificial Intelligence** (AI). This is due to the fact that our Survey (i.e., pre-defined questions) was already launched in November 2020, while the updated European Union Cybersecurity Strategy, that included the new focus on the SOCs, was published in December 2020.

The final word on this paper is for the Chairs of the UC

Growth in the frequency and complexity of cyber-attacks requires companies to increase their resilience and enhance measures for combating the phenomenon. The **burden, however, should not only be on the private sector side, but European institutions should address operational aspects of enforcement too**, also to put in place the Cybersecurity Act and the Commission's blueprint for rapid emergency response. For example, more supportive measures for the private sector should be envisaged, ensuring a **more effective operational support in particular for managing and responding to cyber-attacks** through law enforcement agencies such as Europol and by **strengthening the public-private cooperation and information sharing**.

The **proposed implementation** under ECSO's CISO activity **of a Pan European information sharing platform on IOCs** (Indicators of compromise) to enhance our global proactivity in terms of early detection of future attacks attempts should really contribute to the above.

In a spirit of collaborative work, an **agreed upon common set of Contractual Terms and Conditions** (T&Cs) between the clients and their partners would also improve our global visibility in case of compromise, with the overall objective to act swiftly.

As UC Chairs, we therefore fully support the ambition of ECSO, by proposing new initiatives and ways of working, with the aim to bring our contribution towards an enhanced EU cyber-resilience.

For ECSO, UC Chairs, April 2021

References

[1] ECSO Users Committee, November 2020, “Green Paper on Challenges for CISO’s & Threat Intelligence Sharing”, link

[2] National Institute of Standards and Technology (NIST), Cybersecurity Framework, link

[3] European Commission, December 2020, Directive on Security of Network and Information Systems (NIS 2 Directive), link

[4] European Parliament and Council, April 2016, General Data Protection Regulation (GDPR), link

[5] ECSO WG5, March 2020, “Understanding Cyber Ranges: From Hype to Reality”, link

[6] ECSO WG5, November 2017, “Position Paper: Gaps in European Cyber Education and Professional Training”, link

[7] ECSO WG5 & EHR4CYBER, November 2017 (updated December 2020), “Analysis: Information and Cyber Security Professional Certification”, link

[8] ECSO Users Committee, November 2020, “Position Paper: The NIS Directive Review”, link

Annexes

Annex 1: CISO Survey

The Survey was available online on the European Commission's Survey platform from November 2020 to January 2021.

For more information on the UC, visit ECSO's website.

General / The work of a CISO

*1 What is your job title?

*2 Which sector do you represent (energy, finance, transport, healthcare, manufacturing, etc.)?

3 Do you have any cybersecurity certifications (i.e. CISSP, CISM, Security+, ISO 27001)? If so, which ones?

*4 Does your organisation have a dedicated CISO position?
If yes, mark N/A and skip to next question.
If no, who is responsible for cybersecurity in your organisation?

5 In your opinion, what are the top 5 cybersecurity threats your organisation is facing?

6 What are the main challenges you face in implementing cybersecurity in/across your organisation?

7 Do you feel you have enough authority / Board level support to enforce cybersecurity policies within your organisation?

8 A CISO's working lifecycle is said to revolve around Identify/Protect/Detect/Respond/Recover. Would you agree and how would you rank those in order of importance?

Board investment / Business continuity

1 Cybersecurity, beyond the technical challenges, brings up business-related and financial challenges (e.g. the costs of modernising the infrastructure). To what extent is cybersecurity considered crucial for business continuity in your organisation?

2 While executives may say cybersecurity is a priority, they need to follow through with strategic investments. In your opinion, what are the main reasons that Boards do not invest sufficiently in cybersecurity?

3 Executive Board perceptions can restrict cybersecurity effectiveness. If CISOs want to expand their influence and align cybersecurity with business priorities, they must "manage up" to Executive Boards and "manage across" to all employees.
To which extent do you agree with this statement? And how should such a business process be implemented?

4 When it comes to business continuity, we talk a lot about corporate social responsibility, business risk management strategy, insurance, protection of assets, etc. What do you think are the main disruptive aspects and financial impacts of cyberattacks on companies and Operators of Essential Services (OES)?

Information sharing – Threat intelligence – Crisis management

1 Geopolitics play a major role on security but policy developments in cybersecurity often happen behind closed doors, thus hiding the depth of security and the types of threats that need to be faced. How can we better share information and threats across sectors and countries? And how do we make such solutions visible to CISO's in Europe?

2 Information sharing platforms such as MISP typically only share TLP amber or TLP green information at a technical level (e.g. IP addresses, file names, hashes, etc.). In your opinion, how can we better facilitate the sharing of information that is relevant for CISO's (i.e. strategic, geopolitical, new hacking techniques)?

3 To what extent would you consider collaboration with law enforcement (local/national/Europol) useful for addressing the more pervasive and crime-relevant issues facing organisations? Do you know of any best practice cases of collaboration between CISO's and law enforcement?

3

4 Does your organisation use cyber ranges or technical exercises to conduct simulated attacks or crises responses? Is the CISO involved in these activities?

Certification

1 How involved are you with certification in your organisation? In your opinion, what more needs to be done on this front?

2 Certification often needs to be balanced with agility. What is the most effective way to strike this balance?

3 Do you think that it would be useful to have a mandatory Code in place, i.e. to ensure cybersecurity posture and Corporate Social Responsibility in organisations (example of Canadian approach), and are penalties an effective way of ensuring that organisations implement such measures and apply remedies where needed?

Authentication

1 When it comes to authentication, a holistic approach is needed including the authentication of users, services, IoT, instances, computers, people, M2M (critical), and processes inside machines. The management of this process and the identification across services is also very important.
Do you agree and how do you manage this inside your organisation?

Liability & Governance

1 It is often said that there is an absence of dialogue and trust between CISOs and their Boards. Even if legal liability is made compulsory for CISOs, Boards in most cases are not aware of it nor do they understand cybersecurity and its problems. As such, CISOs usually communicate their decisions to Boards without a discussion or dialogue to make them understand the why's.
What do you think could be put in place to better frame that way in which you report to your Board about risks (financial, digital, cybersecurity, etc.)?

2 A good governance structure is also needed for the evaluation of the risks and of the budget. GDPR brings the awareness to the Board, NIS makes reporting compulsory, but nothing is done for governance. There is no method of approval of a governance.
In general, a good governance structure has 3 pillars:

- Bring profits
- Optimise (not eliminate) the risks
- Optimise/manage the resources

A majority of companies put a lot of money, effort and energy into optimising/managing resources, some of them also tackle brining in profits, but in general, very few companies focus on optimising the risk. Many Boards think that by doing what CISOs tell them, they're immune to any risk.
How do you think this governance issue could be best handled?

European, Regulatory & Cross-sector aspects

1 To what extent do you rely on the regulatory aspects and actions done at the European level for the protection of critical infrastructure and the implementation of the NIS Directive? What more can be done / what should be improved in your opinion?

2 In order to improve operational resilience, cross-border and cross-sector aspects need to be further optimised. How to fight cross-border and cross-sector fragmentation? What lessons can be learned from the more mature sectors in this area?

3 What are your criteria of choice for the procurement and use of cybersecurity solutions and services? (e. g. performance, costs, made in Europe, other)

4 How much is important for you to rely on certified or validated European solutions (c.f. sovereignty and autonomy issues) for a trusted management of your sensitive data?

Additional Comments or Remarks

1 Do not hesitate to let us know any other insights you might have:

5

Acknowledgments

ECSO and the Users Committee would like to give a particular thank you to all CISOs (and equivalent) who have taken the time to read and complete the survey that was at the inception of the present analysis report. Without their provided feedback and comments, we would not have been able to come up with a comprehensive and consolidated document to act as a foundation for the issues to be tackled.

MAIN EDITOR and ANALYST - ECSO Secretariat	
Nina HASRATYAN	Policy Manager

MAIN CONTRIBUTORS – ECSO Members	
Giorgio CUSMA LORENZO	Intesa Sanpaolo (Co-Chair of the UC)
Olivier LIGNEUL	Electricité de France (EDF) (CO-Chair of the UC)
Nelly BACHELET	Electricité de France (EDF)
Igor KRANJEC	Engineering (formerly)
Maria SORLINI	Intesa Sanpaolo

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU