EUROPEAN CYBER SECURITY ORGANISATION

GREEN PAPER

Challenges for CISO's & Threat Intelligence Sharing

WG3 I Users Committee

NOVEMBER 2020

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 wg3_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

Copyright Notice

TABLE OF CONTENTS

European Cyber Security Organisation (ECSO) • www.ecs-org.eu
Rue Ducale 29, 1000 Brussels Belgium

1. Introduction

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. The UC itself is autonomously attached to ECSO's Working Group 3 "Sectoral demand" that represents Suppliers, Users and OES from different sectors – industry 4.0 / manufacturing, energy, transportation, finance, public services/e-government, healthcare, smart cities, and telecom/media/content.

The UC members are restricted to a **network of European Chief Information Security Officers** (CISOs) (or equivalent, i.e. C-level experts working close to CISOs or in cybersecurity responsibility positions) 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.

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, though often limited to the national level, an added dialogue with the private sector is also necessary to create a direct and positive impact on the future of cybersecurity at the European level. Users/OES are key actors in the field of cybersecurity, especially since CSSP (the offer) can only provide 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 between Users/OES
- 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

The following paper leverages on the UC members' experience and expertise to shed light on key requirements and provide preliminary recommendations on improving intelligence sharing among Users/OES. It also offers a definition and consolidation of the position and role of a CISO (or equivalent).

This document is presented as a Green Paper (and not yet a White Paper) as it aims to trigger reactions and stimulate discussions with a wider CISO community from different sectors and different European countries. These represent the initial thoughts of the ECSO Users Committee and comments / suggestions are welcome.

2. Towards a more secure Europe

Threat intelligence or information sharing is a top priority for users in the cybersecurity field with several platforms or initiatives having appeared in the past few years from both the public and private sector. Stakeholders understand that in a globalised world where cybersecurity knows no borders, cooperation, trust and information sharing remain key in the battle against cyber threats and cyberattacks. However, these initiatives still have certain limitations:

Public/public: Information sharing among public entities or public institutions. European institutions, European agencies, national administrations, national agencies, national authorities, etc. regularly come to a coordinated agreement for cross-border intelligence sharing between themselves. In this case, the information is shared **only among public entities** and does not take into account the private sector perspective.

Private/private: Information sharing between **companies from the same sector**. No matter the sector (e.g. energy, finance, etc.), entities within one sector convene with entities from that same sector for information sharing in a setting restricted to sector specificities. But what happens if a Sector 1-company and a Sector 2-company get attacked by the same malware? Real-time or near real-time cross-sector information sharing mechanisms do not yet exist.

Public/private: Information sharing between entities of a country and that country's national public administration. In most cases, public/private cooperation and information sharing **remains within the national borders**. And even then, information could go unilaterally from one side to the other, but not necessarily be reciprocated, which significantly hinders the possibility of any meaningful analysis and mitigation for entities on the reporting end.

The limitations of current information sharing practices are clearly not conducive to the fact that **cyberattacks know no borders and are not limited within one sector** or vertical application area. Cybersecurity is a horizontal, cross-cutting field, so any information sharing within the field should operate within those same parameters.

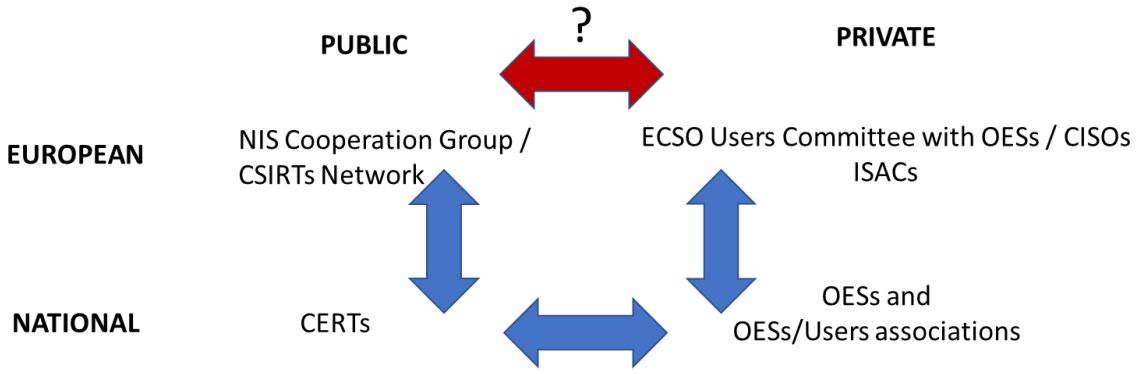
In light of this, the UC members offer the **following recommendations** to help move towards an improved threat intelligence and information sharing in Europe to be promoted and achieved by targeted legislative, operational and awareness actions and initiatives.

Enhanced cooperation & threat intelligence sharing

The key to improving information sharing practices is to ensure that, to the extent possible, information is shared directly in a single setting between private sector entities from all verticals, national public administrations from all European countries, and European institutions and agencies. Currently, **information** circulates from one setting to another (e.g. from public/public to public/private), but **the more it circulates, the less accurate it becomes**: second-hand, third-hand, fourth-hand, etc.

This type of cooperation can be efficient in the fight against cyber-fraud and phishing-related attacks, such as phishing emails, malware/phishing websites, fake websites, spoofing, SIM swapping, etc. These types of attacks require different approaches with different stakeholders in order to be of importance for all sectors and citizens alike.

In turn, the **role of law enforcement agencies and CERTs/CSIRTs should also be enhanced** so that they can effectively **support companies from the private sector** and citizens/customers in dealing with these threats. This means establishing direct cooperation and communication channels between the private sector and law enforcement, where law enforcement agencies could provide anonymised data- and malware-related information from **closed court and investigations cases to the private sector CISOs** (or equivalent) so that they can clean the cloud with reliable information, and in return, CISOs (or equivalent) could support law enforcements agencies with their investigations.



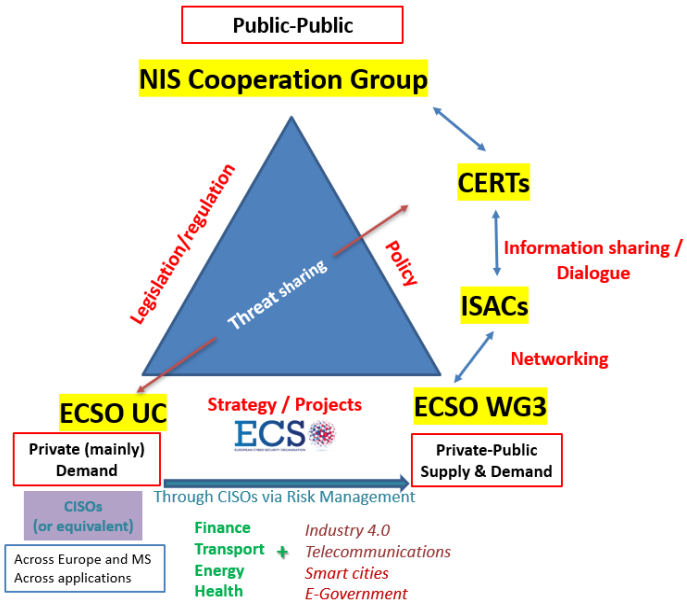
Thus, in addition to the three pre-existing types of cooperation mentioned above, more layers should be added, more stakeholders should be taken into account, and more settings should be considered:

- Public/private: This type of cooperation should go **beyond the national borders** where European-based companies and European national public administrations could indiscriminately share information among themselves.

- Private/private: Information sharing between entities within one sector/vertical should be **opened to all the other sectors**. Through such interdependencies, some sectors could directly learn from the experience of other more mature sectors and it would help all sectors with lessons learned and best practices.

- Public law enforcement/private: This type of cooperation could be the most challenging to establish since these two sectors do not necessarily evolve under the same conditions. However, both have common areas for cooperation such as the closed court and investigations cases mentioned above so an established **information sharing loop could be mutually beneficial**.

Currently, the UC is trying to achieve this type of cross-border and cross-sector cooperation and threat intelligence sharing, but it is a slow-burning process. We know that cyber-attacks do not wait but trust takes time.



Regulatory harmonisation and benchmarking

Cybersecurity is a fast-evolving field and so far, regulation at all levels remains basic or non-existent and scattered (e.g. public/private sector-specific, vertical-specific, etc.). **Regulation should not be a compliance burden** risking to slow down organisations' operations, but it should not either be generic with minimal level provisions. A suggestion would be to base regulations on risks / potential impacts of what needs to be protected against cyber-attacks.

Regulators at national and European level should consider **cybersecurity priorities that are common for all sectors**, such as the protection of critical infrastructure, protection of networks and communication channels, data protection, common criteria for software updates, more compelling requirements for verifying the opening of domains/websites, etc. These are horizontal topics that should be applied in a harmonised way across Europe.

On **data protection**, the European Union has already taken a step towards a harmonised approach with the General Data Protection Regulation (GDPR) [1]. But the GDPR itself is not perfect and has loopholes, for example **not covering the transfer of data between b2b**. On the other side of the spectrum, intelligence and information sharing requires a certain level of free flow of data to help enhance cyber-readiness and cyber resilience, especially cross-border and cross-sector. This complexity should therefore be kept in mind when drafting European data regulation (both general and sectoral).

In the private sector, the establishment of **Key Performance Indicators (KPIs) for benchmarking purposes** could be considered. These could cover the voluntary and confidential benchmarking of third-party vendors based on objective criteria to avoid antitrust issues. KPIs could also be used as a company-internal tool to measure their maturity and improve their security. Such a KPI framework, if coming from the European Institutions, could offer a common ground for all European or European-based companies and help them in their own efficiency, productivity and (cyber)security protection. This, in turn, would increase Europe's market competitiveness at the global level.

European strategic autonomy

Users/OES express their needs and requirements in terms of cybersecurity, whether they be general cross-sector requirements or sector specificities. In this sense, Users/OES are the adaptive innovation drivers in Europe. However, European Users/OES still remain largely **dependent on non-European cybersecurity solutions and services**. This could be an issue, in particular, for those critical infrastructures that need to be sure that data are transmitted, stored and managed according to high security criteria and for this would need trusted solutions certified by national administrations.

For Europe to become an independent major actor in cybersecurity, it needs to enforce its leadership by pushing for **European cybersecurity products, solutions, technologies, and standards** for them to be globally recognised. European cybersecurity strategic autonomy is paramount to position it in a leadership role, especially when rising to the same level as US and Asian "tech giants".

In this sense, the **European Digital Sovereignty would be showcased by the public sector and spearheaded by the private sector** for a more efficient and comprehensive approach. Additionally, the creation of an EU Cloud, initiated and carried out by the European private sector with funding from the European Union would limit the flow of data to the US or Asia and enforce Europe's independence and sovereignty. It is worth mentioning that Europe is already taking steps in this direction with the GAIA-X [2] initiative, the "EU-cloud initiative that aims to establish an interoperable data exchange through which businesses can share data under the protection of European laws." [3]

Yet, the issue of data management remains, and even though avenues are being explored, such as GAIA-X, we are only at the inception of the topic. Once the exploration stage is over, EU Member States and the European industry could have a clearer vision and under-standing of the needs and expectations for an EU Cloud.

The same criteria apply at a more general level in the aim towards a European strategic autonomy. However, questions remain as to how it would be achieved and especially what would be the criteria and preferences of those on the front lines, such as the Chief Information Security Officers (CISOs). These questions will be tackled in the next section of this paper but it is already worth mentioning that, currently, the **biggest incentive remains the costs** that drive European industry decision-makers towards non-European products and solutions, more times than not with no guarantee of quality.

Exercises and awareness

Another way to build trust and establish ongoing cooperation within the European ecosystem is to organise regular cybersecurity exercises. Of course, the effort in conducting joint exercises for responding to cyber-attacks and similar **scenarios should be done cross-sector with cross-border actors from all over Europe**. These exercises could cover topics such as how to regain customers' stolen data after successful phishing attacks, or how to close or block in advance fake websites created to mislead customers and citizens.

The beneficial role of such exercises would be two-fold. On the one hand, it will **promote collaboration** among European cybersecurity stakeholders creating a **European-wide exercise and awareness ecosystem**. Knowing each other and collaborating on a frequent basis will facilitate the build-up of trust and in turn, encourage free threat intelligence and information sharing. On the other hand, it could create **cyber awareness with the general public** especially if these cyber exercises are supported by European campaigns for the citizens, and are defined, prepared and distributed in a joint way by all actors.

3. CISO-specific needs and challenges

The ECSO UC members are CISOs (or equivalent) from Users/OES. The information/intelligence exchanged among them is at the strategic level as opposed to the technical and operational information sharing level. The rationale is for companies' representatives to share threat information/intelligence on a voluntary basis and be able to take quick action if critical information/intelligence is received. CISOs (or equivalent) have this level of decision-making both to choose the type of information/intelligence to share and to take prompt action. However, the position of a CISO itself remains non-defined, non-consolidated and in some cases, even precarious when it comes to the liability aspects.

In the following, we tackle the **three main challenges experienced by CISOs** (or equivalent) and brainstorm possible suggestions and recommendations.

Liability and dialogue

CISOs and their Boards of Directors often experience differences in points of views and priorities, with both struggling to convey their messages. The issue is two-sided. On the one hand, most CISOs focus on the technical aspects of their work, leaving aside the managerial and communication parts. On the other hand, very few Boards fully grasp these technical aspects and the issues related to cybersecurity. In order to optimally secure their companies, **Boards must understand the full extent of the damages that a cyberattack can incur and ensure the allocation of the appropriate budgets to support CISOs in their responsibilities to prevent and / or mitigate the effects of them**.

Two recommendations can be made to move towards an improvement of the current situation:

- The European institutions, such as the European Commissions or regulatory standardisation bodies supported by the European Parliament could **issue a set of requirements for CISOs to comply with in their position**. These requirements could include giving CISOs job immunity/safety for compulsory incident reporting to protect them vis-à-vis their Boards; but also for CISOs to prioritise European services and solutions, and to choose the quality solutions instead of the cheapest ones to secure the company.

- A **generalised European reporting framework** should also be established for CISOs when they report to their Boards that would include a multi-level perspective of their needs and requests: financial, digital, cybersecurity, etc. This would help CISOs to better pass on the right messages to their Boards who in turn, would have a better understanding of the issues and implications.

Governance

A good company governance structure with regards to Board and management roles and responsibilities is also needed for the evaluation of the risks and of the budget. While GDPR brings awareness to the Boards and the NIS Directive [4] makes reporting compulsory, nothing is done for governance to ensure accountability and efficiency of decision-making processes. A **clear governance framework** would:

1) Make profits

2) Optimise the reduction of (not eliminate) risks

3) Optimise/manage the resources for swift business continuity

Currently, a **large majority of companies invest a lot of money, effort and energy on the third pillar**, with the obvious motivation to reach the objectives of the first pillar. However, in general, companies do not pay enough attention to the second pillar. This is even more true with the increased acceleration of the digitalisation of our economy due to the COVID-19 crisis, and it is the **second pillar that is covered by the position and role of a CISO**. Awareness of Board decision makers and investors on the risks due to cyber threats could cause major issues to the other two pillars. Not tackling adequately the second pillar means not securing the company against attacks, thus not giving the CISOs the right means to defend the company.

The CISO/cybersecurity function should be re-evaluated in terms of **structure positioning and overall organisational role** in order to be independent and to follow the evolution of regulation and the digital path of the company. Each organisation should be free of evaluating the more suitable positioning, but it is crucial to help them in the definition of the right role with guidelines based on best practices.

Usually, Boards believe that by just applying the recommendations given by their CISOs, the company is completely secure and immune to attacks, while at the same time, CISOs need to juggle securing the company with reporting to the Boards with limited expenses. Cybersecurity is important to protect not only the company's assets but also to maintain the entire supply chain integrity and business continuity of the company. From this perspective, **Boards could consider including cybersecurity into the company's risk management plan and cost-benefit analysis**.

Professional profile of an Information Security Manager

For cybersecurity professionals in general, common and recognised certifications are a must-have in order to work in the sector and such certifications should be issued by a European body (e.g. ENISA) while being recognised in other continents.

For CISOs however, beyond the technical skills covered by certifications, a whole set of hard and soft skills together are required. There are **4 mains aspects** that are needed for the CISO position:

- Governance: CISOs need to know what they are protecting, the roles and responsibilities of each employee, the person in charge of the budget, etc.

- Risk management with regards to the objectives of the company and the planification of the mitigations.

- Project implementation management (directly in line with the Risk Management aspect).

- Incident management: to take in the damages if the first three points have not been handled correctly.

A lot of companies do not do well with or even implement the first three points, which explains why most of them are bogged down by the incident management aspect.

CISOs need a proper definition of their portfolio of responsibilities, expectations and required skills for the position. Currently, the existing disparity is counter-productive with some companies not even having implemented a CISO position. Here again, the European institutions could work on guidelines making the position of CISO compulsory and providing a framework for their obligations and liabilities.

4. Next steps

Strategic threat intelligence is the reason that the ECSO UC was created and remains its raison d'être. However, a healthy and forward-looking European ecosystem cannot ignore the issues and challenges encountered by CISOs. They are on the frontlines protecting our digital infrastructure and if Europe is to become truly digitally autonomous and one of the drivers of cybersecurity globally, then CISOs need their positions consolidated and to be supported from all fronts, industry and political alike.

This is why, **in addition to the European cross-border and cross-sector strategic threat intelligence sharing issue, the ECSO UC is going to focus on the issue of CISOs and how to support them**. In the coming months, ECSO will launch a European-wide **survey** targeting CISOs from all European countries and from different sectors (e.g. health, finance, transport, energy, manufacturing, etc.) in order to further its knowledge and understanding of the position and challenges encountered by CISOs. Different aspects will be tackled in the survey:

- General aspects, such as the existence of a CISO position inside a company, or the content of their portfolio of responsibilities
- Board investment and business continuity
- Information sharing and threat intelligence
- Certification
- Authentication
- Liability and governance
- European, regulatory and cross-sector aspects

The survey will remain online for several weeks, following which the results will be analysed and published in a comprehensive report in 2021. The report will be publicly available and sent to European national public administrations, the European Commission, as well European industry representatives.

The ECSO UC works to bring awareness on these issues but it is certain that the necessary political support needs to follow behind, and ECSO will strive towards that goal to represent its Community.

5. Conclusion

As highlighted in this paper, when it comes to cooperation and establishing a healthy and resilient European cybersecurity ecosystem, there are still improvements to be made and measures to be undertaken This position paper was written based on the primary experience and observations of the CISOs that are members of the UC and of some ECSO members, from a Users/OES perspective.

For the strategic threat intelligence part, the ECSO UC is currently working on improving cooperation, creating the European network of CISOs and adding layers of stakeholders involved in the information sharing process.

The UC is working on becoming this unique setting adopting a European cross-border and cross-sector/vertical approach. However, as previously mentioned, it is a **slow-burning process**, especially when it comes to **building up trust**, with direct contacts across sectors and countries a critical component and something that we are suffering from in this period due to the limitations brought on by COVID-19.

As a next step, the ECSO UC will launch and carry out a survey in Autumn 2020 targeting CISOs all over Europe to deepen its understanding of their needs and challenges. A full analysis of the survey's outcomes can be expected in a report to be published in 2021.

In the meantime, this Green Paper aims to serve as a basis to be shared among the European institutions, Members States and the cybersecurity community to bring awareness, stimulate discussions, and initiate action on the priorities mentioned, especially as regards the consolidation of a CISO's position.

European Cyber Security Organisation (ECSO) • www.ecs-org.eu
Rue Ducale 29, 1000 Brussels Belgium

References

[1] European Parliament, General Data Protection Regulation (GDPR), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN

[2] German Federal Ministry for Economic Affairs and Energy (BMWi), “GAIA-X: Driver of digital innovation in Europe”, https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-driver-of-digital-innovation-in-europe.pdf?__blob=publicationFile&v=8

[3] TechRepublic, “What is Gaia-X? A guide to Europe's cloud computing fight-back plan”, https://www.techrepublic.com/article/what-is-gaia-x-a-guide-to-europes-cloud-computing-fight-back-plan/#:~:text=Gaia%2DX%20is%20an%20initiative,vessel%20for%20data%20across%20industries.

[4] European Parliament, The Directive on security of network and information systems (NIS Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Acknowledgments

This report was completed in September 2020. Its publication has been possible thanks to information and contributions provided by ECSO and its Users Committee members.

MAIN EDITOR - ECSO Secretariat	
Nina HASRATYAN	Policy Manager

MAIN CONTRIBUTORS – ECSO's Users Committee Members	
Giorgio CUSMA LORENZO	Intesa Sanpaolo (*Co-Chair of the Users Committee)*
Olivier LIGNEUL	Electricité de France (EDF) (*Co-Chair of the Users Committee)*
Ulrich FLEGEL	Infineon Technologies

MAIN CONTRIBUTORS – ECSO Members	
Georges ATAYA	Solvay Brussels School of Economics and Management

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