EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER

European Sector-Specific ISACs

WG3 I Sectoral demand

DECEMBER 2018

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

During the past year, ECSO WG3 members have discussed the topic of European sector-specific ISACs and what should be done with respect to these in terms of their setup, what they should achieve, and how to improve their efficiency.

ISACs as they are currently set up may not have the right structure but it's clear that a body is needed where information can be shared in a trusted way. We need ISACs that can provide information in the right model with an added value that can put the intelligence between the ISAC and the final user. ISACs are also important in the context of the implementation of the NIS Directive as they can facilitate the sharing of best practices, harmonisation of specific requirements, and collaboration between Operators of Essential Services (OES).

A new and agile structure should be established for sector-based ISACs in Europe ("ISAC 2.0"), one which fits with the requirements of each sector and which is able to collaborate with national ISACs and other relevant stakeholder communities, in a trusted and operationally-driven environment. An "ISAC 2.0" should be more focused and more organised. It should be created under the right structure and governance, so information and content can be easily injected into it. A common objective is also needed for all ISACs.

A survey was conducted internally to analyse ECSO members' assessment of the needs and priorities for a European ISAC within their sector. The survey was applied to the 8 sectors currently established within ECSO WG3:

- Industry 4.0 and ICS
- Energy Systems and Smart Grids
- Transportation (road, rail, air, sea, space)
- Finance, ePayments, and Insurance
- Public Services, eGovernment, and Digital Citizenship
- Healthcare
- Smart Cities and Smart Buildings (convergence of digital services for citizens) and other Utilities
- Telecom, Media, and Content

The following paper is a consolidation of the survey results with recommendations to support existing and yet-to-be established European sector-specific ISACs that are community-driven and dynamic enough to respond to current and future needs.

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

2. ENISA 2018 study on ISACs

In February 2018, ENISA released a study entitled "Information Sharing and Analysis Centres (ISACs): Cooperative models" [1] which aims to:

- Provide information about ISACs in Europe through collecting information on the status of ISACs and to identify main models of this type of collaboration.
- Identify current challenges that both the private and the public sector face in the process of setting up and developing ISACs.
- Formulate and propose recommendations to enhance the sophistication of ISACs in Europe.
- Investigate the potential role of ENISA in the creation of Pan European ISACs.

The study makes the following recommendations to advance the role of ISACs in Europe:

- ISAC participants should invest in creating trust to ensure a right level of information sharing.
    - *ECSO comment: The "right" level of information sharing is a major aspect of ISAC activities and should be clarified*
- ISAC facilitators should ensure a right level of engagement by all ISAC participants.
- Traffic Light Protocol (TLP) is a good starting point for information sharing.
- ISACs should have a structure that motivates the private sector to participate.
- ISACs should have a structure that engages the public sector as well (finding balance).
    - *ECSO comment: The role of each member should be defined*
- All members should agree to terms of reference and a code of conduct
    - *ECSO comment: What would be the value (in terms of obligations) of "terms of reference and a code of conduct"? It's not certain that this would build trust.*
- Every ISAC should produce results periodically.
- Specific circumstances when mandatory information sharing is required should be agreed upon.
    - *ECSO comment: An ISAC should not impose any "mandatory action" to its members; ISAC activities should rely on voluntary contributions, even if definition of roles and expected contributions could be defined. In addition, this would not motivate the private sector to participate (in contradiction with the ENISA recommendation above).*
- ISACs should ensure funding mechanisms from the very beginning.
- The ISAC should stimulate cross sector ISAC collaboration.
- Law enforcement could have a specific role in the ISACs.
- Evaluation should be performed periodically.
- ISACs should develop new services based on their members' needs.

In the following, ECSO will complement the above-mentioned recommendations from ENISA with some industry-driven and sector-specific insights. Where no European ISAC exists, the community has an opportunity to set one up in a way that responds to the needs of the given sector. Where ISACs are already established, recommendations may be made on how to improve or re-structure them to ensure a well-functioning European-wide solution.

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

3. Sector-specific needs and recommendations

3.1. Industry 4.0 and ICS

There is no specific ISAC dedicated to Industry 4.0 and ICS in Europe. The recent successive criminal attacks on industrial information systems are enough to justify that one is urgently needed. Based on industrial needs, the ENISA report, and benchmarks of the US ISAC model, in the following we provide a non-exhaustive list of recommendations for the creation of a European Information Sharing and Analysis Centre for the industry 4.0 and ICS sector.

What should be shared?

An ISAC for this sector should rely on a framework dedicated to the sharing of information, knowledge, standards and tools, as follows:

Information and knowledge:

- Threat intelligence targeting industrial network infrastructures, ICS, IIOT, and any digital applications encountered in the Industry 4.0 environment.
- Guidelines and best practices on incident handling, cyber security management (processes, tools).
- Incident reports: technical details, response and mitigation, operating experience feedback and, to a certain extent, operational/business consequences.

Infrastructures and tools:

- Cyber security services proposed via the platform (e.g. vulnerability analysis, pen-testing, personalised audit, staff training, etc.).
- Common validation, qualification and certification tools, standards and methodologies.
- Data samples (large, representative, shared, real, exploitable, with privacy clearance) enabling to assess the performance of security solutions in a non-biased way.

What is needed?

As prerequisites to the creation of an ISAC for the sector, a set of tools should be developed:

- A dedicated and secured European platform managing the described information sharing functionalities, ensuring the highest authentication, identity and access management.
- A community-driven interface for cyber security professionals to report incidents, share best practices and interact on a dedicated “Questions/Answers” forum.
- A confidentiality management tool to ensure access for the right user to the right information depending on their authorisation and confidentiality level. This classification management tool is paramount to ensure trust among actors and foster user engagement.

Who are the stakeholders?

The ISAC actors should be from the demand side, the supply side and regulators. We can cluster them as follows:

- Demand side: factories & supply chains
- Supply side: automation & robotics vendors, security & IT vendors
- Regulators: authorities & certification bodies

What role for public / private actors?

The ISAC should be industry-driven. Due to their field knowledge and the fact that they are primarily concerned, industrial members are the leading force of the ISAC. Nevertheless, public support should be expected and required.

The role of public authorities is not requested in terms of funding, but rather on:

- Creating a legal framework for the exchange of information among users, contributing to building and restoring trust. The ENISA report notes that "*multinational or large cyber security companies (European or not) do not tend to participate in ISACs. This is mainly due to the lack of trust ISAC members have towards these companies based on the belief that these companies might use the information and knowledge shared for their own business interests or developments*".
- Supporting the private companies to comply with laws and regulations (e.g. implementation of NIS Directive and GDPR).
- Providing secretariat/facilitator functions (e.g. providing facilities for meetings).

How to foster user involvement?

- Identify and involve the pre-existing industry associations, standardisation bodies, expert groups, and other communities that are influential in industry security.
- Obtain the buy-in from Member States, ministries and agencies in charge of cyber security and industry.
- Run an information campaign to sensitise the private sector on the cyber security risks and raise awareness on the necessity and benefits of information sharing across industrial actors.
- Insist on the perks of having a simplified contact with public actors, especially Law Enforcement Authorities (LEAs), to help them better fulfil their legal and regulatory obligations.
- Highlight the results achieved by the US ISACs: As highlighted by the ENISA report, "*Analysis of twenty years of US experience indicates that ISACs are effective and do significantly enhance the level of cyber security. They create an ecosystem in which trust is being built among critical operators and experience can be shared. Because of this, entities less advanced in the field of cyber security could learn from others. Due to the fact that ISACs also cooperate with the public sector, they help increase the overall level of cyber security on national level and in the specific sector.*".

What funding?

- Membership fees
- Cyber security services proposed via the platform

3.2. Energy Networks and Smart Grids

The primary objective of an ISAC is the sharing of experiences related to cyber security in order to allow operators to benefit from them and increase the level of their cyber security. In the energy sector, the operators should be at the forefront of an Energy ISAC to ensure their efficiency as they have the prime responsibility of ensuring the security and safety of energy infrastructures. In parallel, all stakeholders involved in the cyber security of energy systems have to engage an Energy ISAC to enhance the cyber security of the whole ecosystem.

What information to share?

The information to be shared should mainly rely on experiences related to cyber security (technical and organisational):

- Feedback on incident management
- All kinds of known cyber security threats
- Comparison of cyber security practices
- Feedback on regulation implementation
- Feedback on cyber security technology and services use
- Feedback on cyber security awareness tools

The use of this experience-based information by an Energy ISAC should help:

- Energy operators to avoid threats, enhance incident management, enhance the implementation and operation of cyber security controls (technical and organisational), implement innovative experienced cyber security architectures and tools, enhance cyber security awareness among involved employees, etc.
- Cyber security technology and service providers to enhance their products to better meet/suit energy operational needs and constraints.
- Regulators to update cyber security regulation for better/more efficient applicability.
- Authorities involved in incident management to enhance technical and operational incident management processes.

An Energy ISAC should avoid duplicating efforts in activities or sharing of information already ensured by other organisations, e.g. CERTs, and focus on its main missions to be successful.

Who are the stakeholders?

All stakeholders dealing with the cyber security of energy infrastructures should be involved in the Energy ISAC to leverage and gather their backgrounds and experience in order to increase the cyber security level of energy infrastructures:

- Energy operators should be at the forefront of an Energy ISAC as they operate energy infrastructures and have the prime responsibility of ensuring the security and safety of infrastructures.
- Cyber security solutions/services providers should be involved to benefit from the operational/effective use of cyber security solutions/services and enhance their products.

- Authorities involved in the cyber security of energy infrastructures (incident management, audit, etc.) should be involved to share their experience and benefit from their counterparts' experience.
- Regulators should also be involved to adapt cyber security regulation for better applicability and efficiency.

What are the requirements of an Energy ISAC framework?

Many requirements should be considered to ensure the efficient functioning of Energy ISAC:

- The missions and outcomes of an Energy ISAC should be explicitly and clearly written. They should be agreed on and adopted by all its members. This will avoid the duplication and dispersion of ISAC activities which would divert it from its main objectives.
- The roles and contributions of each member should be clearly predefined to achieve the objectives of the Energy ISAC.
- As sensitive information is shared in ISACs, strict and clear governance rules should be defined and set up to build strong trust among ISAC members.
- Different levels of information exchange (or separate channels of information exchange) should be considered/defined according to the kind of information and the usability of the shared information. Indeed, a certain kind of information is only useful for energy operators while another kind could be useful to technology/services providers. The identification of the right/appropriate recipient of information would ease the exchange of sensitive information.
- Benefits of sharing each kind of information should be pre-identified and then measured by the governing body. An Energy ISAC should not be a place for vendors to promote their cyber security products.

These conditions appear necessary to foster stakeholders' involvement, particularly energy operators.

How to ensure efficiency of an Energy ISAC?

The evaluation of sharing information outcomes is the basis of an Energy ISACs success. To ensure the ISACs efficiency, means/tools should be defined and set up to measure the usefulness of shared information.

Finally, the proven efficiency of an Energy ISAC would demonstrate the good functioning of the organisation and would attract new members which will lead to increase collaborations and the global organisation performances.

Feedback on EE-ISAC (European Energy - Information Sharing & Analysis Centre)

A European ISAC for the energy sector already exists: EE-ISAC [2]. Nevertheless, EE-ISAC lacks visibility and its existence is unknown from most of European energy operators. EE-ISAC carries out many activities but the main outcomes and benefits of the organisation are not clear. In addition, EE-ISAC involves only a few energy operators whereas they should be strongly represented to drive the ISAC activities according to the energy sector's needs.

The EE-ISAC should involve many energy operators and would need restructuring to achieve expected benefits of an ISAC for the energy sector. ECSO is in contact with EE-ISAC and would be happy to support them, to the extent possible, in improving the visibility and efficiency of its activities.

3.3. Transportation

Road transportation

An automotive ISAC already exists with an industry-operated environment created to enhance cyber security awareness and collaboration across the global automotive industry—light- and heavy-duty vehicle OEMs, suppliers and the commercial vehicle sector [3]. This ISAC is considered efficient by its members and all major OEMs and Tier-1s are present and willing to exchange information. However, it was initiated and organised from the US, meaning a more physical presence in Europe is still lacking. Nevertheless, European OEMs and Tier-1s are active in the automotive ISAC also at the Board of Directors level.

The main priorities of an ISAC for the automotive sector should be:

1) Sharing information on incidents
2) Table-top exercises
3) Guidelines on incident handling

Information sharing shall be restricted to the involved parties and, if needed, regulators. An ISAC for the automotive sector should share information on the technical details about an incident and, if available, the mitigation. It should be shared through a central membership portal and funding should be provided through membership fees.

For the automotive sector, moving to a more global solution (such as the one that exists for the finance sector) should be prepared. More physical presence in Europe (e.g. legal entity, staff) would also improve a tighter exchange with European Authorities like the European Commission and ENISA.

Air transportation

An EU Aviation ISAC is being created which will exist alongside two entities: ECCSA and the US-originated Aviation ISAC.

The need for a European-based Aviation ISAC was expressed by European industry members, OEMs and Airlines who saw a need to organise and collaborate in the realm of cyber security and in the field of intelligence and analysis sharing for the aviation sector. The idea was shared with the European Institutions and relevant agencies who displayed an immediate interest.

Initial talks regarding the EU-A-ISAC creation started three years ago. It took significant time to reach a consensus regarding the legal framework in which the EU-A-ISAC would operate. Now that the European Aviation ISAC is entering its operational phase, it demonstrates its singularity: First, a European foothold to manage European sensibilities regarding the exchange of cyber security-related intelligence, the need to accompany the European model, both for the industry and the European Institutions. And second, a separate body from ECCSA where trust between a reduced number of actors has already been established. ECCSA will have the task of being a forum for a much broader audience.

3.4. Finance, ePayments and Insurance

When thinking about an ISAC 2.0 model for the financial sector, the following should be considered:

- Is there a gap?
- Existing groups, frameworks and processes in the EU provide and address an assortment of stakeholders, reporting options and threats. However, memberships are somewhat ad-hoc - not universal, and the level and roles within the parent organisation of participants varies considerably. This means that momentum, consistent leadership and improvement are difficult, and the threats being addressed generally tend to be focused on cybercrime, cyber security and fraud impacting single or multiple organisations with a retail-banking focus.
- The threats addressed should be those cybercrime, cyber security or fraud threats which are (or are potentially) of a nature and at a level to impact operational resilience and/or represent a systemic risk.
- The composition, focus, and outputs of the group should complement the ECB, ENISA, NISD aims regarding incident reporting guidelines – however, for an ISAC to be a preventative, proactive intelligence sharing and analysis effort, aimed at identifying and addressing threats and vulnerabilities, the information shared should relate to an activity before it manifests as incidents captured by incident reporting guidelines *per se*.
- We believe the global (rather than domestic) origin and impact of serious cyber-borne threats to the financial sector, the growing threat to large-ticket interbank payments and infrastructure, and the presence and systemic importance of some key critical economic functions performed by large international foreign banks in Frankfurt, Paris, Milan, Madrid and Dublin for example (and their visibility of threats, incidents and intelligence), create an environment and a requirement for the largest, most systemically important banks operating to form the initial nucleus.
- There is an increased use of technology to automate sharing.
- The stigma of being “breached” needs to be removed so that firms are encouraged to share proactively and with appropriate safe harbour mechanisms to be protected (to a certain degree) from fears of liability (breached entities are the victim after all) – for example Section 314(b) provides these institutions with immunity from private civil actions resulting from any disclosures in conformity with the US Bank Secrecy Act (“BSA”).

The primary objective of an ISAC within this sector should be the spreading of cooperation between banks within the European community and sharing of tactical intelligence (modus operandi). In this respect, the ISAC should ease the information exchange about cyber-criminal activities, vulnerabilities, technology trends and threats, and incident case-studies affecting the financial community.

The ISAC shall provide input to the financial institutions to help them to proactively address cyber threats and identify effective cyber incidents counter-measures. It should be a trusted source of information sharing that is of high value for the CERTs of the financial institutions.

Within the financial sector, there are several ISACs already active in Europe.

- **FI-ISAC** exists since 2008 as an independent organisation and is well integrated with European institutions and agencies such as Europol, European Central Bank, European Payment Council and the European Commission. The FI-ISAC is supported by ENISA.
- **FS-ISAC** (an American independent and non-profit organisation) is already active on information sharing and is enhancing its activities and efforts in the EMEA region. FS-ISAC is a well-established brand with existing capability, proven processes, globally integrated with regional components in the Americas and APAC.
- Several **national CERTfin** across Europe.
- The **Global Cyber Security Center**, with its **OF2CEN** advanced information exchange platform, is another non-profit agency, funded by Poste Italiane and based in Rome with a strong collaboration with Italian and International government institutions, private bodies, research institutions and international bodies. It is worth mentioning the related EU project EUOF2CEN.

The current FS-ISAC could perhaps be perceived as too US-focused. A key issue to acknowledge in starting to develop any information group is that developing the requisite levels of trust is hard. While the FS-ISAC has its own European based steering group and threat intelligence committee, this is likely not robust enough to build the level of trust that is needed. There needs to be a few strong personalities from the European banks to drive it, along with strong endorsement from the ECB. Second, the threat intelligence focus in the EU and for EU banks is different from the US needs. For example, EU banks have historically been more concerned on a daily basis with Eastern European criminal organisations than they were with Russia or China.

It would be appropriate to have a central European hub managing all the information received with an appropriate level of confidentiality (with a Traffic Light Protocol agreement) and helping the financial community to tackle threats and be updated on new vulnerabilities and technology trends. Such need for coordination has already been pinpointed by the NIS Directive that has foreseen the CSIRTs Network. The ISACs should collaborate among themselves and with CERTs.

It could also be useful to have information with TAXII or STIX standards, that would help the analysts to use them within a Threat Intelligence Platform. It is also advisable to mark information with sectorial and cross-sector relevance when sharing them with other organisations.

The main priorities of an ISAC for this sector should be:

1) Continuous monitoring of new threats and technology trends.
2) Constant forwarding of relevant information to the constituency.
3) Organisation of regular meetings with the financial community to exchange feedback and ideas to improve cyber resilience.
4) Sharing of recent threats and attacks in other financial institutions that could help to mitigate or be proactive against those future threats and attacks.
5) Sharing of vector attacks in an anonymous way, so as to foster more information sharing and collaboration between the financial institutions.

6) Sharing of best practices to become more resilient.
7) Online banking fraud.
8) Fraud prevention in post PSD2 financial world.
9) Attacks at bank employees (e.g. SWIFT attacks).

The ideal structure of an ISAC for the financial sector is one in which there is more control and participation in key decisions from the financial institutions. It should also be governed by the banks and the financial institutions. Participants should be trusted members of the financial sector, mainly coming from approved contacts from the financial CERT. There could be some exceptions regarding LEAs and other institutions that are interested in threats affecting critical infrastructures.

However, when we think of a pan-European ISAC, we would suggest that it does not follow an "ISAC" model. The value of a pan-European ISAC is to act as a holistic, top-down view into the requirements coming from global, regional, country, and sector levels. This would then enable organisations (both public and private sector) to look at how to build the right structures to meet those requirements in the most coherent way.

Best practices can be drawn from the Dutch ISAC model. The Dutch ISACs, established by the Government's National Cyber Security Centre (which also acts as their Secretariat) operate effectively with physical meetings six or seven times per year and regular teleconferences, bilateral meetings and information sharing via chats or closed channels/email lists. All information is shared voluntarily, but members are subject to certain rules:

- To become a member of an ISAC, organisations need to be accepted by the other members.
- Members have to sign a Memorandum of Understanding which states that the information shared within the ISAC cannot be shared onwards with other parties. While the contract is not legally enforceable, its violation may result in a warning or the firm being banned from the ISAC.
- All ISACs use the TLP to indicate the permitted distribution of information and some limit the number of members of the group to build trust.

As evidenced by the Dutch model, the advantage of county-based ISACs is their geographical proximity and accessibility, and the fact that it is generally a small group which enables information sharing. Therefore, a layered model works best.

It is also worth looking at the Global Resilience Federation (GRF), a standalone not-for-profit that was formed by FS-ISAC and acts to coordinate multi-industry sharing, and to share best practices regarding standing-up new sharing communities and incorporating them into a voluntary sharing architecture.

ECSO should not operate the information and intelligence sharing as this requires secure infrastructure etc. What ECSO can do is ensure that ISACs (through pan-European ISAC coordination) are properly connected with the relevant Member State bodies, other associations, EU institutions such as ENISA and law enforcement. ECSO can play a crucial role in ensuring that the purpose of this ISAC is properly communicated, and particularly for financial services and payments, that the reasoning for having a small group is understood. Once a core pan-European ISAC coordination is set up, there may be a role for ECSO to then disseminate amongst wider financial services information and reports on trends and indicators i.e. not real-time information sharing.

There is room for a variety of entities to function in the information sharing space. Trying to crowd out or supplant existing associations with a single model that is expected to be universal is neither a good idea or possible. It will be important for the topic of incentives to be explored. To ensure firms engage in information sharing groups and proactively and meaningfully contribute to these groups, there will need to be encouragement from regulators and governments. Further we encourage governments to extend and create incentives for firms to implement cyber risk management principles and share information.

Incentives may include:

- Tax incentives, government procurement incentives, public recognition programmes, greater regulatory support (analogous to regulatory 'FinTech bridges' and sandboxes).
- Rewards to firms demonstrating "best-in-class" processes, for example the Heritage Foundation has advocated rewarding market leaders with the most 'cyber-secure' supply chains (as identified via a certificate scheme), and the Obama Administration suggested the Government may offer rewards to firms that have done the best job of instilling and spreading knowledge of the NIST Framework.

How should information be shared?

- It is very important to ensure that the information confidentiality is guaranteed with a TLP protocol (advisable) or similar. The ISACs should share information with both local CERTs (private sector) and local Law Enforcement Agencies (LEA) (public sector). It is also appropriate to define cryptographic and profile authorisation tools. Information should be shared in a decentralized way and only with trusted members of financial institutions.
- Capability has to exist to protect sensitive information otherwise contributing firms will not feel comfortable sharing, however much information is not sensitive and can be shared widely to include with other ISACs, government partners, other associations, etc. Use of information handling caveats can achieve capability to share both restricted and widely disseminated information, these are not mutually exclusive. Information should be shared via multiple avenues including in person meetings, multilaterally via email listservs, bi-laterally between members, regular conference calls open to membership, alerts from the ISAC itself, repository of indicators and other data housed at ISAC portal, etc.
- ECSO should promote a common set of standards and protocols. The VERIS model advocated by Verizon or STIX-TAXII model advocated by the Department of Homeland Security (DHS) (and Mandient) are two examples of information sharing protocols (both US centric). While neither is perfect, they are a good starting point. Additionally, for information classification the Traffic Light Protocol (TLP) is a good tool, and for ensuing a common language for easy communication there is the US Cyber Incident Severity Schema [5]. ECSO and ENISA can help by providing or investing in tooling that enables the good functioning of ISACs and cross-sector and cross-country information sharing, while every sector handles its own ISAC.

What kind of information should be shared?

- The ISAC should share information about cybercriminal activities, technological trends and threats, and incident cases including possible remediation whenever available (e.g. available patches to overcome vulnerabilities), as well as information about threats, common vulnerabilities, common risk scenarios prioritised by level of risk, best mitigation practices, vectors of attacks; all following a taxonomy which should be based on international ones so as to avoid having to create a new one. Also, information should be shared anonymously where required. No sensitive information regarding financial institutions should be shared or stored.
- Generally, the most useful information for an ISAC to share is related to current threat indicators observed by one or more of its members. Other types of data may include analysis of operational and strategic level threats, vulnerability assessments, tactics/techniques/procedures of malicious actors, mitigation best practices, executive/board level summaries and communications, etc.

Within the financial sector, law enforcement agencies (LEAs) and the intelligence community could collaborate with national CERTs to tackle fraud and increase the security of the payment services value chain. The information shared could be bi-directional and the community may help LEAs in counter-terrorism operations.

The ISAC should involve relevant stakeholders in its activities by creating and proving trust on the sharing and anonymous mechanisms as well as value on the information provided.

In terms of collaboration with national ISACs, the Financial ISAC could receive input but no output would be created to other ISACs so as to avoid giving away information to non-trusted sources that could leak information into the wrong hands. An international council of ISACs could be created/fostered which provides for a venue for cross border collaborative efforts.

The LEA and intelligence community should be involved by providing information into the Financial ISAC in an automatic and intelligent way, as well as collaborating where required in threat campaigns and against threat actors. It should continue to build opportunities for government centres to host private sector representatives from the ISAC. Enable processes for requests for information to flow both ways. Develop processes for anonymity of ISAC information, encourage LEA and intelligence community partners to consider the lowest possible classification of information to enable its use by private sector in defence.

However, we do need to progress the conversation on the sharing of classified detailed threat information. While the public sector can share classified contextual information with private sector individuals who have the adequate security clearance, those individuals can often only take limited action (for example share with relevant colleagues) due to restrictions. This is a key issue for CNI firms who need access to classified threat information in a timelier manner. EU governments and agencies could consider best practices from the US such as granting temporary clearances.

Further, sharing Indicators of Compromise is often insufficient to inform private sector incident response efforts. For example, at times, quickly sharing full malware samples instead of derived indicators and analysis will be key. We encourage ECSO to focus on working with industry and the

EU institutions and Member States on the exploration of tools to share detailed threat data, including malware samples and contextual information, while protecting privacy and firm-specific identifiers.

In order to involve stakeholders in ISAC activities, it must be ensured that the ISAC provides a tangible, measurable and useful service and outputs from commencement. Regional and country specific regulators can/should encourage (not necessarily mandate) participation in information sharing groups as a way to improve information security posture of the individual firm. For example, in November 2014 the Federal Financial Institutions Examination Council (FFIEC) recommended regulated financial institutions participate in FS-ISAC, following the Federal Deposit Insurance Corporation (FDIC) statement on the importance of public/private partnerships, specifically referencing FS-ISAC in April 2014, which then led to over 420 new members in the weeks following. Low barriers to entry (cost/dues) is also important.

Every ISAC member could participate with an annual fee. The model should be primarily based on membership dues, with resource support from government entities if/where appropriate. Another way could be to have public funding for the research of the mechanisms and infrastructure needed to share but privately owned and managed by financial institutions.

3.5. Public Services, eGovernment, and Digital Citizenship

A sharing mechanism exists in France which is the mailing List of CISO's in Higher Education and Research (Liste des RSSI de l'enseignement supérieur et de la recherche) : https://listes.recherche.gouv.fr/sympa/info/rssi. The advantages of this mechanism are:

- Fast sharing of information on active attacks
- Sector Specific Alerts
- Participation in a Community Listserv
- Access to a Sector Exclusive Portal
- Ability to Send/Receive Requests for Information
- Access to Member Meetings, Events, and Networking Opportunities
- Participation in Member Committees

However, there is a poor quality of IOCs (indicators of compromise), no cross-sector sharing or community chat, and it's in French only.

The main objectives of an ISAC in this sector should be to:

- Enhance information sharing between members
- Help in analysis
- Help sharing of best practices
- Help in detection and early alerts

Information-sharing should be restricted to ISAC members. Some information may be shared widely without problems but most of exchanges require confidentiality. The information to be shared includes:

- Targeted Phishing Campaigns
- Malicious IP Addresses
- Intrusion Methods used by hackers

Information should be shared via Listserv / Wiki / Blog / RSS.

In France, the current model is a service operated by RENATER, which is a state operator in charge of the French National Research and Education Network (NREN) [4]. In Higher Education and Research, RENATER operates what is close to an ISAC in France. Each country NREN could operate the same ISAC. GÉANT could operate an ISAC which would be the sum of all NREN-related ISACs. At the European scale, GÉANT (https://www.geant.org/About) should be a central actor as they aggregate all NRENs. They do have some activities in security, but not an ISAC [7].

3.6. Healthcare

An ISAC for the healthcare sector does not currently exist in Europe.

The main objective should be collaborative improvement under a public-private structure, chaired by a public organisation. The top 3 priorities of a Healthcare ISAC in Europe should be to:

1) Identify threats and attacks
2) Exchange of experiences on efficient solutions
3) Highlight needs and foster solutions

Information sharing should be restricted to ISAC members. Trust is an important aspect to facilitate information sharing. For this reason, wider sharing is not advisable although ISAC participation should be open to all organisations in the sector.

ISAC members should share information about threats, attacks, solutions, and cyber security needs which should be shared either openly during ISAC meetings to discuss about a particular subject, or anonymously for sensitive items.

The only efficient way to convince relevant stakeholders to participate in the activities of a healthcare ISAC is to highlight the benefits of joining which should be focused on little effort and substantial benefit. Awareness and communication campaigns would be advisable to promote the ISAC. Public healthcare organisations should lead the ISAC, as this would foster the participation of private healthcare organisations.

In terms of collaboration with national ISACs, there should be different hierarchical levels or just a single pan-European ISAC to avoid overlapping. National ISACs can periodically report to the pan-European ISAC. Members of the national and pan-European ISAC should preferably not be the same to also avoid overlapping activities. Hierarchical levels are beneficial in terms of meetings as it is cheaper to meet more often at the national level than at the pan-European level, while language

can also be a barrier. Frequent national ISAC meetings combined with yearly pan-European ISAC meetings should be held.

A healthcare ISAC should engage with law enforcement and the intelligence community by organising specific sessions once or twice per year so that those aspects more closely related with their field of activity can be discussed.

The ideal funding structure for a healthcare ISAC would be mixed public and private funding. If the membership quote is too high this would discourage participation.

3.7. Smart Cities and Smart Buildings

An ISAC for the smart cities sector does not currently exist in Europe.

The main objective should be similar to those identified for the healthcare sector (Identify threat and attacks, define best practices or a CMM (capability maturity model), and a cost-benefit spending framework, and foster solutions and test benchmarks).

Information sharing should be restricted to ISAC members as trust is an important element to ease the sharing of events and information, in a controlled environment. ISAC members should share information about threats, attacks, solutions, cybersecurity needs, best practices, and CMM models.

In order to engage stakeholders in the activities of the ISAC, it should offer a trusted and concrete community where to exchange ideas, facts, best practices and tools. A possible model to mirror which is already adopted in the US is the Microsoft Digital Crime Community (DCC).

In the era of transition to GDPR it is fundamental to also have legal experts, to ensure cross-fertilisation and foster the breaking of existing barriers among disciplines that weaken security.

Funding for the ISAC should come from membership fees.

3.8. Telecom, Media, and Content

There is a major difference between these vertical industries. In this section we will split between Telecom respectively and Media and Content as different industries, albeit from an industrial perspective there is convergence happening in the domains.

Telecom

The telecom industry has developed early on a model of information sharing in parallel with the development of the ISACs. Incident sharing is happening in a structured way through the various

CERTs and CSIRTs of the respective operators throughout Europe. These platforms and the collaboration with ENISA have been reported regularly [6]. The sector's incident and sharing reporting responsibilities have partially been regulated through the legal framework in Article 13a of the Framework Directive (2009/140/EC).

Incident sharing is largely on a voluntary basis and differs predominantly on the basis of the maturity of the operating teams involved, and the size and competitive position of the operators in each country. For this purpose, additional ISACs could be welcomed on specific operator activities.

What should be shared?

Information and knowledge:

- Threat intelligence targeting critical internet and telecom infrastructures.
- Guidelines and best practices on infrastructure vulnerabilities, takedowns, incident handling, cyber security management (processes, tools).
- Incident reports: technical details, arbitration details, involved infrastructures, response and mitigation, operating experience feedback and, to a certain extent, operational/business consequences.
- Incidents and intelligence with other ISACs, since telecoms are likely amongst the most mature in the market.

Infrastructures and tools:

- Common platforms and interactions with other CERTs/CSIRTs.
- Incident Management Platforms, Common validation, qualification and certification tools, standards and methodologies.
- Data samples (large, representative, shared, real, exploitable, with privacy clearance) enabling to assess the performance of security solutions in a non-biased way and for research purposes.
- Common training and education (e.g. vulnerability analysis, pen-testing, personalised audit, staff training, etc.).

What is needed?

As prerequisites to the creation of additional ISACs:

- ISACs on specific challenges: backhaul networks, interconnection, transmission, internet, mobile, cloud, etc.
- A dedicated and secured platform(s) managing the described information sharing functionalities, ensuring the highest authentication, identity and access management; capable of reaching out to other domains.
- A community-driven interface for cyber security professionals to report incidents, share best practices and interact on a dedicated "Questions/Answers" forum.
- A confidentiality management tool to ensure access for the right user to the right information depending on their authorisation and confidentiality level. This classification management tool is paramount to ensure trust among actors and foster user engagement.

Who are the stakeholders?

The ISAC actors can be extended beyond the operators:

- Operators in Europe: operators, MVNO's, mobile, backhaul, ISP's, cloud, etc.
- Supply side: equipment suppliers, international ISP's, international cloud providers.
- Security industry at large: MSSPs, security advisory, ethical hackers, community of security specialists, security communities per country and internationally.
- Large customers: other industry ISACs, top customers, critical infrastructure.
- Law enforcement: Europol/EC3, local police.
- Regulators: regulators.

What role for public / private actors?

The ISAC should be industry-driven but supported by public authorities. The role of public authorities is not requested in terms of funding, but rather on:

- Encouraging (other) private operators with increasing market powers to take part, facilitating interaction.
- Encouraging participation of security industry to take part in discussions, interactions, activities (on a voluntary – interest basis, upon additional qualification).
- Enhancing the legal framework for the exchange of information among users, contributing to building and restoring trust.
- Supporting the private companies to comply with laws and regulations (e.g. implementation of NIS Directive and GDPR).
- Providing secretariat/facilitator functions (e.g. administration and coordination, ledger of participants).
- Be point of interaction with other public authorities (law enforcement, justice, policy, intelligence services, etc.).

How to foster user involvement?

- Identify and involve other pre-existing CERTs/CSIRTs, operators, relevant or interested market players, industry associations, standardisation bodies, expert groups, and other communities that are influential in industry security.
- Level playing field definition of intelligence sharing, using common identifiers (observables) and security clearance. Obtain the buy-in from Member States, ministries and agencies in charge of cyber security and industry.
- Insist on the perks of having a simplified contact with public actors, especially Law Enforcement Authorities (LEAs), to help them better fulfil their legal and regulatory obligations; focus incident management on the internal actions rather than lawful intercept.
- Highlight the results achieved by the other industry ISACs.
- Create common European ISAC exchange activities, best practices and discuss about incidents, challenges, opportunities.

What funding?

- Government supported
- Existing collaboration platforms and organisations
- Private sector (supply side) obligation to participate and contribute

Media and Content

The media / content industry is maturing in cyber security but has not yet adapted fully to the different ongoing developments, including cyber security incident management, collection reporting and exchange. Public broadcaster and internet media companies are typically more advanced than many of the traditional commercial media companies. Incident sharing is rarely taking place within the media sector. If at all, it is on a case by case basis, without any form of structured approach or active participation with a large number of participants.

The media sector is a particular target, as there might be limited financial gain but could heavily impact the society as a whole, the security of the state and the geo-political landscape. Impacts on media, being social media or public broadcast through manipulation could distort the societal balance and disrupt the society and economy.

Media companies have increasingly started developing interest in personal data protection capabilities. Leakage of data usage trends and other metadata could be exploited for social engineering. Targeting specific Member State media companies can be intended to discredit specific persons or organisations. Data integrity as such is becoming more important.

What should be shared?

Information and knowledge:

- Threat intelligence on media companies as targets, personal data targets, media disruption, media systems and technologies, DDOS
- Guidelines and best practices on infrastructure vulnerabilities, incident handling, cyber security management (processes, tools)
- Incident reports: types of attacks, to different media, types of actors (likely nation states), types of collaboration with public authorities
- Incidents and intelligence with other ISACs

Infrastructures and tools:

- Administrative support both on Member State and EU-level to coordinate ISAC, organise sessions, align interests and people, awareness to support companies and organisations in having their security officers and incident teams participating.
- Administrative support both on Member State and EU level to report on incidents via internal channels (state security & intelligence) and external publications, creating awareness on impact of media.
- Incident Management Platforms, common validation, qualification and certification tools, standards and methodologies.
- DPP – Digital Production Partnership cyber security requirements & data protection technologies.
- Common training and education (e.g. vulnerability analysis, pen-testing, personalised audit, staff training, etc.).

What is needed?

- Start-up of exchange platform, bringing CISO's and security managers of media and content companies together at regional and European level, as well as collaboration with the European Broadcast Union.
- Differentiating different media types and their carriers: broadcast, internet broadcast media, mobile, internet, cloud, etc.
- Specific observables to be generated for media and content, specifically on privileged accounts, types of content contributors and their respective access rights, types of distribution platforms and restricted access.
- (de)centralised data collection system to record historical activities and events, a community-driven interface for cyber security professionals to report incidents, share best practices and interact on a dedicated "Questions/Answers" forum.
- Scenario development, supporting broad understanding and identification of potential vulnerabilities and the way they could be exploited.
- A confidentiality management tool to ensure access for the right user to the right information depending on their authorisation and confidentiality level. This classification management tool is paramount to ensure trust among actors and foster user engagement.

Who are the stakeholders?

The ISAC actors can be extended beyond the media companies themselves:

- Broadcast Media companies: public & private broadcasters, distribution networks (including ISP's/telco operators, ca-tv distribution networks, internet broadcasters, Content Delivery Networks, etc.).
- Social Media companies: both European and non-European, with European members and customers.
- Print – Hybrid Media companies: newspapers, journals, magazines both collecting personal data, preparing for targeted customer approach and transmitting media over mobile and internet (digital magazines, newspapers, etc.).
- Content Creators: journalists and news gathering companies, on the road, transmitting data with nomadic users.
- Advertisement: economics of online advertising is of massive value to hackers, financial crime and fraud related.
- Security industry at large: MSSPs, security advisory, ethical hackers, community of security specialists, security communities per country and internationally.
- Law enforcement: Europol/EC3, local police.
- Regulators: regulators.

What role for public / private actors?

The role of public and private actors should be the same as stated above for telecom.

How to foster user involvement?

- Identify and involve IT-security teams with media companies, gather involvement and support with security industry expertise to drive and gain interest.
- Develop joint incident materials to be shared across media and participants.

- Involve other operators, relevant or interested market players, industry associations, standardisation bodies, expert groups, and other communities that are influential in industry security.
- Level playing field definition of intelligence sharing, using common identifiers (observables) and security clearance. Obtain the buy-in from Member States, ministries and agencies in charge of cyber security and industry.
- Highlight the results achieved by the other industry ISACs.
- Create common European ISAC exchange activities, best practices and discuss about incidents, challenges, opportunities.

What funding?

- Government supported and operationalised to drive the operations.
- Existing collaboration platforms and organisations.
- Private sector (media companies) obligation to participate and contribute.

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

4. Conclusions and recommendations

Based on the sector-specific insights and recommendations provided by ECSO members in this paper, **the following global conclusions are made**:

- The implementation of ISACs differs per sector with Finance and Energy being ahead of the rest (some sectors do not currently have an ISAC). The maturity of ISACs also differs per sector and per country.
- To be able to share information, there needs to be trust between members of an ISAC. In general, this means small groups with people who have known each other a long time. In addition to juridical parts like NDA's, trust must also be shown by not abusing information etc.
- The disadvantage of the current way of working is that it is not scalable. It is hard to share information between sectors and countries directly and, in general, there is little to no structural cross-sector information sharing.
- Although many of the sector-specific ISACs are already essential drivers of effective cyber security collaboration, some organisations do not fit within a specific sector or have unique needs. These organisations run the risk of being left out of essential discussions and information.

This leads to the following recommendations:

- A network of European sector-specific ISACs should be interconnected with Member States' local infrastructure (national sector-specific ISACs where available or intersectoral ISACs) in terms of ISAC and be flexible/adaptive taking into consideration their model/structure and modus operandi.
- The introduction of tools and solutions that facilitate trust, a simple and anonymous exchange of information and a simple and understandable re-use of information exchanged would be beneficial for all stakeholders.
- An "ISAC 2.0" should have a user-friendly interface within a web application, easy to use and well-structured, helping its community with information which must be well readable, up-to-date and easy to use.
- A European ISAC landscape should be comprised of a distributed number of national ISACs based on a sector or industry that are self-sufficient but are able to receive and send intelligence and information in an anonymous way without revealing compromising information but providing sufficient information on vector attacks so as to react proactively or become more resilient. This system should be based on AI and pattern and behaviour recognition.
- Different levels of information exchange (or separate channels of information exchange) should be defined by sector-specific ISACs according to the kind of information and the usability of the shared information. Certain kinds of information are only useful for operators while other kinds could be useful for technology/services providers. The identification of the appropriate recipient of information would ease the exchange of sensitive information. Benefits of sharing each kind of information should be pre-identified and then measured.

- Those organisations that cannot join a sector-specific ISAC but have a need for cyber threat information could benefit from participating in intersectoral ISACs established at national level, functioning as an umbrella and cooperation platform for sector ISACs. Sharing of specific information is vital among members of a group but also between industry as a whole. The flow of information should be facilitated in such a manner that reaches different sectors-specific ISACs, as information on one sector can be useful for others too (i.e. financial sector information can be relevant for several other industries that have regular business with the sector and therefore can be affected).
- ECSO could envisage the development, with its members, of an independent platform for secure information-sharing in a cross-sector environment (adopting the best practices with regards to TLP and anonymisation). In this way, ECSO would act as a secondary hub (i.e. beyond the normal discussion level in WG's) between the ECSO members. In this task, ECSO could be linked to ENISA and, through this platform, provide hub services to the private sector, reaching out also to SMEs.
- A pan-European coordination ISAC should be promoted, to act as an EU steering group that defines a standard for intelligence and information sharing and then uses that steering group to keep things federated and synchronised, fitting in more easily with existing domestic sharing structures, and with ENISA, Europol/EC3 and the NISD CSIRT Network
- Special attention should be paid to the status of the relationship between the industry and the law enforcement agencies (LEA's) at national and European level. Trust must be further enhanced between the parties. A model of cooperation should be developed, defining a standard for information sharing between LEA's and ISACs/industry.
- There is no more space for isolated pillars in modern cyber security because attackers do not work that way. Therefore, a full involvement of different stakeholders, supported also by ECSO is advisable. ECSO can support ISACs by promoting them and, to the extent possible, supporting their organisation/coordination, etc. Other stakeholders coming from different disciplines, such as safety, should also be involved to cross-fertilise and break down these barriers.
- ECSO and other involved stakeholders should support the building up of ISACs and other information-sharing platforms through the usage of R&I funding to develop the needed tools, platforms, and knowledge.

The following design principles for the ISAC environment should be used:

- They should by global by design, meaning they should be able to communicate with other ISACs.
- They should be able to communicate cross sector. Public ISACs at national level are starting to build this communication but they are not connected efficiently with the private ones.
- They should be able to communicate with the same taxonomies based on international best practices so as to avoid fragmentation and the burden to translate and maintain different formats.
- They should be able to communicate critical or essential information in real time when there is a crisis, for example IP addresses when under a current DDOS, phishing campaign or mule

accounts info. Presently, the GDPR prevents private ISACs from doing so directly with other private or public ISACs.

- They should be able to build trust and to anonymise data being shared in an automated way so as to increase real-time.
- They should be able to co-exist with other ISACs in a centralised and/or a decentralised way.
- They should be able to differentiate specific sector scenarios which are cross sector or sector specific so as to be more target specific. Language specific or translation mechanisms could also facilitate the understanding of the intelligence information.
- They should behave like an immune system which means they should not only be mere transmitters of information but also include AI to detect and react under specific scenarios or system risk (example of WannaCry, a scenario that could have been detected in a very tiny event occurring in private ISACs or reports to public ISACs by end-users or SMEs, before it escalated to a massive virulent event).

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

References

[1] ENISA, Information Sharing and Analysis Centres (ISACs): Cooperative models, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

[2] EE-ISAC, European Energy - Information Sharing & Analysis Centre, http://www.ee-isac.eu

[3] AUTO-ISAC: Automotive Information Sharing and Analysis Center, https://www.automotiveisac.com/

[4] French National Research and Education Network (NREN): https://www.renater.fr/securite

[5] White House, US Cyber Incident Severity Schema, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf

[6] ENISA, Incident Reporting for Telcos, https://www.enisa.europa.eu/topics/incident-reporting/for-telcos

[7] GÉANT, Trust, Identity and Security, https://www.geant.org/Services/Trust_identity_and_security

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

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