EUROPEAN UNION AGENCY
FOR CYBERSECURITY

LEGAL AND ORGANISATIONAL ASPECTS OF COOPERATION BETWEEN CSIRTS AND LE

Handbook, Document for trainers

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

CONTACT

For contacting the authors please use CSIRT-LE-cooperation@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Alexandra Michota (ENISA), Andreas Mitrakas (ENISA), Constantinos Patsakis, Václav Stupka

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-334-6, DOI: 10.2824/85709

TABLE OF CONTENTS

1. INTRODUCTION

1.1 THEMATIC AREA

In 2017, ENISA presented technical as well as legal and organisational aspects of the cooperation between Computer Security Incident Response Teams (CSIRTs) -in particular national and governmental CSIRTs, and Law Enforcement (LE) and provided some recommendations to help them cooperate closer to fight against cybercrime.

ENISA confirmed that CSIRTs and LE often exchange information during incident handling and criminal investigations, both formally and informally, and that trust is the key success factor to their cooperation. However, it is clear that there are challenges related to the diversity of legal systems and legal provisions of the Member States. Adding further complexity is the diversity of communication channels between the various Member States, which hinders the effectiveness of fighting cybercrime.

Figure 1: ENISA training on CSIRT-LE cooperation - Syllabus

ENISA Training on CSIRT-LE Cooperation - Syllabus	
Keywords:	Computer Security Incident Response Teams (CSIRTs), Law Enforcement (LE), Cooperation, Information exchange, Legal aspects, Organisational aspects
Background:	This module intends to provide trainees with an understanding of the legal and organizational aspects that could enhance this cooperation. Trainees further acquire a better understanding of the procedures for their information sharing.
Method of teaching and learning:	• Class lectures, interactive learning (class discussions, group work) and practical problems solved in class. • Case studies are assigned to the trainees and are reviewed in class.
Recommended material:	• ENISA reports • ENISA presentations • Trainer's notes based on recommended material and sources

- **Learning outcomes**

  As a result of attending this course, the trainee should be able to:

  - Analyse sample legal and organisational aspects of cooperation between CSIRT and LE
  - Identify the key drivers of this cooperation
  - Identify the key inhibiting factors of this cooperation

- **Target audience**

  The intended target audience are CSIRTs (mainly national and governmental CSIRTs but not limited to them), LE, as well as individuals and organisations with an interest in Cybersecurity.

- **Course Duration**

  4 hours

- **Frequency**

  At least yearly

2. GENERAL DESCRIPTION

2.1 IMPORTANCE OF COOPERATION BETWEEN CSIRTs AND LE

CSIRTs do not have the powers of LE and respectively, LE does not have access to intelligence and expertise held by CSIRTs. It is therefore important for these communities to cooperate. However, technical, legal, organisational and cultural challenges can render this cooperation complicated. In addition, those challenges are managed differently in each country. A comparison of these different approaches is rather valuable when examining this cooperation. The studies developed by ENISA provide valuable insight into the current state of cooperation and recommendations on how to improve it. (ENISA, 2017) (ENISA, 2017a) (ENISA, 2019) (ENISA, 2019a)

Taking into consideration that cybersecurity incidents do not always correspond to cybercrimes, cooperation between these entities does not take place in all cases.

Cybercrimes sometimes indeed relate to cybersecurity incidents. Nonetheless, in other cases cybercrimes occur, which are not related to cybersecurity incidents or which eventually are not reported.

The CSIRT community has materially different duties and objectives than the LE community, depending as well on the type of each CSIRT community (governmental, national, sectoral, etc.) and LE (regional, national, federal, international, etc.). However, when dealing with a potential cybersecurity incident, each community should consider the outreach to other actors that could be involved, keeping in mind the multiple ways of cooperation and the importance of receiving reciprocal feedback on a case. Additional stakeholders may be approached in this cooperation process, such as the judiciary, service operators and service providers, intelligence services, military and international agencies.

Both formal and informal procedures may be followed in this cooperation process with the purpose of achieving each community's objectives for mitigating incidents and prosecuting crimes, depending also on each community's hierarchical or flat structure, the classification level and the sophistication of the exchanged information. Formal procedure may have the form of an official written request for information regarding a specific case, while informal could have the form of information shared orally during a phone call. This cooperation channel may be direct or supported through appointed liaison officers, whose role sometimes has been pointed out as a very important one.

2.1.1 Segregation of Duties (SoD)

In order to support the key actors of a cybercrime investigation, i.e. the CSIRT and LE communities as well as the judiciary to reach a better understanding of each other's duties based on the roles each community plays, a SoD matrix (see Figure 2 — Example of segregation of duties matrix) could be drafted at national level. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more. As shown in the SoD template below, the CSIRTs, LE, judges and prosecutors have to identify the key responsibilities for their communities and then link them with the skills required in order to fulfil these duties. SoD matrices usually serve to ensure compliance with laws and regulations.

Figure 2: Example of 'Segregation of Duties' matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutor	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
During the incident/crime					
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Duty to inform other stakeholders/authorities	✓				Obligations and rules for information sharing among communities.
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
Post incident/crime					
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

2.2 RELEVANT LEGAL & POLICY FRAMEWORK

The core European legal and policy framework on the cooperation of competent authorities in the field countering cybercrime is described below:

2.2.1 EU Strategies

- The "Europe 2020" Strategy, (E2020): the EU's growth strategy for a smart, sustainable and inclusive economy. E2020 sets objectives for the growth of EU; one of the pillars is the digital agenda.
- The European Agenda on Security (EAS): the fight against international cybercrime is listed as one of the main goals.
- The Digital Agenda for Europe (DA): DA sets action points to enable full potential of ICTs within internal EU market. It is aiming at boosting Europe's economy by delivering sustainable economic and social benefits from a digital single market.
- The Digital Single Market Strategy for Europe (DSM Strategy): creating DSM is one of seven goals of the DA. DSM strategy has 3 pillars: 1) better access to online goods (support for online market development), 2) environment for digital networks and services (effective rules and support to infrastructure development), 3) economy and society (enabling economy, industry and employment to take full advantage of digitalisation). DSM strategy explains also the importance of trust and security for achieving set goals.
- The European Commission Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence - Building strong cybersecurity for the EU: 1. Building EU resilience to cyberattacks 2. Creating effective EU cyber deterrence 3. Strengthening international cooperation on cybersecurity. Public-private cooperation and information sharing identified as extremely important.

2.2.2 Cybercrime

- Council of Europe Convention on Cybercrime, 2001, (CETS No.185), "The Budapest Convention": The most relevant international treaty on cybercrime and electronic evidence, ratified so far by 63 countries. The Convention has provisions on substantive law (criminalization of cybercrimes), procedural law (investigative powers for LE including legal safeguards), international cooperation (24/7 network, provisions on

cross-border evidence collection, jurisdiction, voluntary cooperation, etc.). The finalization and adoption of a 2nd Additional Protocol dealing in detail with cross-border evidence in the light of new technologies and services is expected.

- The EU Directive 2013/40, on Attacks Against Information Systems: Substantive provisions very similar to the ones of the Budapest Convention, regarding the criminalization of cybercrimes.
- The EU Directive 2014/41, regarding the European Investigation Order in criminal matters: The European Investigation Order (EIO) Directive is based on mutual recognition, deadlines for acceptance and execution of the EIO. An effective tool that can be used for the collection of evidence located but only within the EU.
- Proposal for Regulation (EU) on European Production and Preservation Orders for Electronic Evidence in Criminal Matters: A proposed effective tool to collect evidence directly from service providers located abroad. Any Member State's LE body should be able to directly order any ISP to freeze/produce data from their service.
- The EU Regulation 2017/1939 Implementing Enhanced Cooperation on the Establishment of the European Public Prosecutor's Office ('the EPPO'): An Independent EU Body, focused on the prosecution of offences against EU financial interests and on improving transnational investigations – could likely play a role in facilitating cooperation between LE and CSIRTs of different countries.

2.2.3 Cybersecurity

- The EU Directive 2016/1148, Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, "NIS Directive": The Directive aims at promoting a high level of network and information systems security within EU. The provisions are driven by a cross sectoral approach that requires operators of essential and digital services to take appropriate security measures and to notify serious security incidents to public authorities of the Member States. It also requires Member States to implement cybersecurity strategies and creates new mechanisms for cooperation among them (cooperation network – strategic cooperation, and CSIRTs network – operational cooperation).
- The Cybersecurity Strategy of the EU (CSS): one of the initiatives of the DSM strategy and the first EU-level strategic document dealing with cybersecurity. Achieving cyber resilience and reducing cybercrime are some of the main goals. The document stresses out the importance of cooperation of different stakeholders.
- The European Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ("Blueprint"): The goals identified are: 1) Stepping up cooperation to enhance preparedness and deal with cyber incidents 2) Addressing challenges facing Europe's cybersecurity Single Market 3) Nurturing industrial capabilities in the field of cybersecurity. Focusing on cooperation and training - within and between member states.

2.2.4 Data protection

- The EU Regulation 2016/679, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, "General Data Protection Regulation - GDPR": The GDPR provides protection to personal data and empowers citizens to control processing of their personal data. GDPR has a broad definition of personal data, increased jurisdiction and introduces significant fines and strict rules on when, why and for what purposes the processing of personal data can take place. Obligations on security of systems used to process personal data (privacy by default and design), mandatory notification of personal data breaches are also provided by the GDPR. Possibility of restriction of GDPR provisions based on national security, defence, public security and/or prosecution of criminal offences is of great importance especially when information sharing is required. CSIRTs need to consider

GDPR limitations when sharing personal data among their constituency and with other authorities.

- The EU Directive 2002/58 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications): The Directive is focused specifically on electronic communication operators and will be replaced by an equivalent Regulation, which foresees protection of metadata, that should be only processed based on the data subject's consent.
- The EU Directive 2016/680 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data (Law Enforcement Data Protection Directive - LE DP Directive): The Directive serves as a basis for processing of personal data by LE. Data can be processed only within the local legal framework, and with appropriate safeguards for the rights and freedoms of data subjects.
- The EU Directive 2016/681 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (Directive on the Use of Passenger Name Record – PNR - Data): The Directive focuses on terrorist offences and serious crimes. Some cybercrimes may be considered as serious crimes; sharing PNR data between carriers and LE is allowed only by means of push method.

2.2.5 Institutions

- The EU Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), (New ENISA Regulation).
- The EU Regulation 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol), (Europol Regulation).
- The EU Regulation 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA.

2.2.6 Case-law

- Court of Justice of the European Union, Judgement of the 6 November 2003, Bodil Lindqvist v Åklagarkammaren i Jönköping, C-101/01, EU:C:2003:596: The Court interpreted a broad definition of what consists personal data by defining the term as any data referring to an identified/identifiable person.
- Court of Justice of the European Union, Judgement of the 24 November 2011, Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, EU:C:2011:771. An Internet Service Provider (ISP), Scarlet Extended SA, could not be compelled to install a filtering system for all electronic communications, both incoming and outgoing, passing via its services that aimed at detecting and preventing an unlawful exchange of copyrighted works. The Belgian national Court ordered Scarlet Extended SA to install a filtering system aiming at preventing copyright infringements. However, the measure requested would result in the identification of end user's IP addresses and in the monitoring of the content of their communications. The case was brought before the Court of Justice of the European Union, which ruled that the measure requested, infringed the fundamental rights of the Internet users, notably the right of protection of personal data and the freedom of expression (articles 8 and 11 of the EU Charter of Fundamental Rights).
- Court of Justice of the European Union, Judgement of the 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, EU:C:2016:779: The dynamic IP

address is considered as personal data of the internet user in relation to the ISP which has legal means that enable to identify the person using the dynamic IP.

- Court of Justice of the European Union, Judgement of the 8 April 2014, Digital Rights Ireland Ltd (C-293/12), v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General; Intervener: Irish Human Rights Commission and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others; Joined cases C-293/12 and C-594/12, EU:C:2014:238. Repealed data retention Directive for the following motives: no relationship required between retained data and public security, no criterion limiting access of the public authorities and their employees to retained data, no substantive or procedural rules for accessing retained data, no time limit applying on the retention period.
- Court of Justice of the European Union, Judgement of the 21 December 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Joined Cases C-203/15 and C-698/15, EU:C:2016:970. The retention of data for the purpose of combating crime falls within the scope of Directive 2002/58/EC (privacy in electronic communications). Every access to the retained data by public authorities can only be performed following a decision of a competent court/independent body with the exception of urgent matters.

2.3 KEY CHALLENGES

2.3.1 Legal

The diversity of national legal frameworks and the complexity in the transposition, implementation and enforcement of EU law are the main legal challenges hindering the cross-border and cross-sectoral cooperation between CSIRTs and LE. For example, the substantive laws of Member States may define differently a specific incident, which in certain jurisdictions may be not considered as a criminal offense. Moreover, data retention periods and the scope of data retention may vary significantly in addition to the procedural powers of LE in obtaining electronic evidence.

During the transposition period, efforts and adjustments of the national legal frameworks are required in order to implement newly introduced EU legislation. In addition, there might be some challenges related to the implementation of specific pieces of legislation itself. Notably, examples of such implications arise from the transposition of the NIS Directive and the LE Data Protection Directive, as well as from the implementation of the GDPR:

- NIS Directive: All Member States have published a national cybersecurity strategy. It remains thus to be seen whether all member states provide sufficient resources to CSIRTs and competent authorities to ensure a high level of network security.
- LE Data Protection Directive: increased cost requirements both in terms of staffing and technical means necessary to ensure conformity with the Directive's provisions.
- GDPR: Proper application of Article 23 and Recital 49, that allows for the collection and processing of personal data by CSIRTs without the data subject's consent. Without due account of the recital, the CSIRT-LE cooperation could become more difficult.

2.3.2 Organisational

The causes of organisational challenges met in the cooperation between the stakeholder entities have been identified as follows:

- ***Lack of skilled personnel:*** Limited skilled staff positioned both on the side of LE and CSIRTs as the demand on cybersecurity professionals in the private sector is higher.

- ***Insufficient training:*** Limited training opportunities and resources especially for conducting common training for both communities. The trainings should be focused both on technical, organisational and legal aspects.
- ***Lack of agreed procedures on information sharing:*** There are often no defined procedures to identify criminal offenses or to fulfil the obligation to share information/data.
- ***Lack of knowledge of international standards:*** Very limited knowledge of the available ETSI, ISO, and NIST standards, which could facilitate cooperation.
- ***Lack of trust:*** This is the main reason hindering cooperation. Building and maintaining trust is a process that requires investment of resources and time.

2.4 RECOMMENDATIONS

2.4.1 Intelligence exchange

Implementing a regular formalised exchange of intelligence information and statistics between CSIRTs and LE can improve their cooperation efforts, support them in conducting an effective assessment of the threat landscape and gradually facilitate the trust building process.

This regular exchange of intelligence is better established by developing a methodology on evaluating data quality and adopting practices on data collection accordingly. Promoting the use of the Traffic Light Protocol (TLP), maintaining and publishing statistics and finally engaging liaison officers in the process, are the additional recommended steps for building this intelligence exchange.

2.4.2 Liaison officers

Placed within each organisation, liaison officers can provide mutual support and expertise; develop a uniform approach to cooperation and information sharing and promote a trust building culture. Nevertheless, for their effective contribution, their roles need to be properly aligned with their working procedures and the applied legal framework. From an organizational perspective, appointing liaison officers requires the allocation of appropriate resources along with the identification of the competent profiles.

2.4.3 Skills development

Through joint trainings and exercises, both communities can gain practical experience and benefit from building a higher level of skills and a better knowledge of standardized procedures on collaboration and information sharing. In addition, adopting a common language and terminology can be rather advantageous in facilitating the mutual understanding. The competent agencies should therefore facilitate and organise joint CSIRT-LE training sessions, prepare common exercise scenarios and utilize the available training materials as provided by ENISA, EUROPOL, UNODC and other institutions.

2.4.4 Formalise data requests and information sharing

Formalising data requests and information sharing is an additional recommendation to improve the cooperation between CSIRTs and LE. This can be achieved by developing simplified forms for data requests based on a common taxonomy, meaning clear and simplified methods for requesting cooperation and information and common understanding of terms, contents and definitions. Each entity should first identify the content requirements, the form and procedures to be used and onwards ensure effective implementation and adoption of these forms within the concerned communities.

2.4.5 Trust building and networking events

Lack of trust is one of the main causes when examining the lack of effective cooperation. Members of both communities have acknowledged that personal connections are very useful in supporting cooperation and in ensuring reciprocal feedback. Both communities can benefit from opportunities to identify synergies and ways to further improve their cooperation. To this end, organising networking events for CSIRTs and LE, both at national and international level, can be advantageous. Sessions and side-events dedicated to cross-sectoral cooperation should be set-up during conferences, taking into account that safe environment for open discussion should be provided. Last but not least, it is also recommended to compile and utilize relevant studies focused on cooperation.

2.4.6 Implement NIS Directive and apply GDPR

The implementation of the NIS Directive and of the GDPR can positively influence the envisaged cooperation. CSIRTs and LE can improve their ability to develop effective procedures for cooperation and information sharing, safely share personal data in compliance with the applicable framework and strengthen their mutual trust as a result of higher legal certainty. The transposition of the NIS Directive to the national level can establish the mandate and the position of CSIRTs and public authorities and at the same time, the application of the GDPR can provide the required specific legal means to enable cooperation (rec. 49 of the GDPR). Awareness of these legislative provisions is necessary for both CSIRT and LE communities.

2.4.7 Identify shareable information

Identifying the information that CSIRTs and LE are allowed or required to share is recommended. The entities have to identify and clearly classify the shareable information and data as well as the conditions for sharing certain datasets and groups of information. Conducting studies to better understand the kind of information that they can both provide to each other may be necessary and further assist in identifying potential legislative gaps.

2.4.8 Update legislation

Ensuring that national legislation, as related to information sharing and cooperation between communities, is updated and in conformity with the EU developments is a necessary step for enhanced cooperation. Updating the legislation by promoting accountability and clearly defined obligations can generate higher legal certainty and thus higher levels of trust in cross-sectoral cooperation. Cooperation and information sharing should also be stimulated through appropriate legislative measures.

The competent authorities should identify the gaps in legislation that could prevent cooperation and information sharing and implement or update the necessary provisions to allow voluntary or even require mandatory sharing of information.

2.4.9 Promote a culture of information sharing

A culture of information sharing should be promoted within both at national and cross-border level, aiming to allow a better understanding of cooperation benefits and provide a better knowledge of successful methods of cooperation, while increasing the levels of trust. The communities can achieve that by organising joint meetings and trainings, developing cases studies and promoting best practices on CSIRT-LE cooperation.

2.4.10 Improve maturity of communities

The application of effective organisation maturity models through appropriate new procedures and methods could improve the ability of cooperation and information sharing by taking into account not only the people but also the processes and the technologies applied.

The key steps for this procedure would be to assess existing organisation maturity models (i.e. the ENISA online maturity assessment in case of national/governmental CSIRTs) and promote their use as well as develop new ones for LE. Assistance can be provided to communities in improving their maturity level through the competent institutions. (Europol, ENISA, etc.).

2.4.11 Develop internal security policies

Permitting and supporting information sharing between CSIRTs and their LE counterparts can be better framed through internal security policies regulating the process in conformity with the applicable legislation. Internal security policies should identify the boundaries of cooperation and information sharing.

2.4.12 Make available relevant information

Sharing large amounts of information requires that organisations also have suitable means to do so. LE could benefit from gaining better access to intelligence retained by CSIRTs. Indeed some relevant information could be effectively shared with LE also through automated means of access to data sets via APIs (Application Programming Interfaces). The CSIRT community should identity available and shareable data sets relevant to the LE community and provide the latter one with contacts of available experts. However, policies should be developed to enable the sharing of valuable information along with appropriate standards and APIs for data transfers.

2.5 SUMMARY

Previous ENISA studies that focus on improving the cooperation between CSIRTs and LE show that the level of trust, maturity, scope and effectiveness is varying between individual Member States. Through the adoption of the appropriate legal and organizational measures, better levels of cooperation and information sharing could be achieved. Suggested recommendations attempt to address the legal and organizational challenges occurring in this cross-sectoral dialogue. The measures proposed focus on trust building, awareness raising, improvements of legal certainty and development of procedural and technical tools aiming to support both counterparts.

3. CASE STUDY

3.1 CASE STUDY – CSIRT APPROACH

The objective of this case study is to present the main limitations to the cooperation between CSIRTs and LE due to the diversity of current legislation in different Member States.

For this case study, it is recommended to divide the trainees in groups; thus, the results and approaches of each group can be compared. This should lead to discussions of the advantages and disadvantages of the individual solutions.

Figure 3: Main objective of the case study

Main Objective	
Targeted Audience	CISOs, security staff, CSIRT members, etc.
Total Duration	30 minutes
Scenario	Trainee is a member of a CSIRT team dealing with cybersecurity incidents, which is likely caused by criminal offence.
Task 1	Identify expected activities of relevant stakeholders by filling in the SoD matrix
Task 2	Identify criminal offences committed by the attacker
Task 3	Identify relevant evidence/information
Task 4	Prepare criminal complaint, and request for cooperation to LE
Task 5	Identify legal limitations to the information sharing

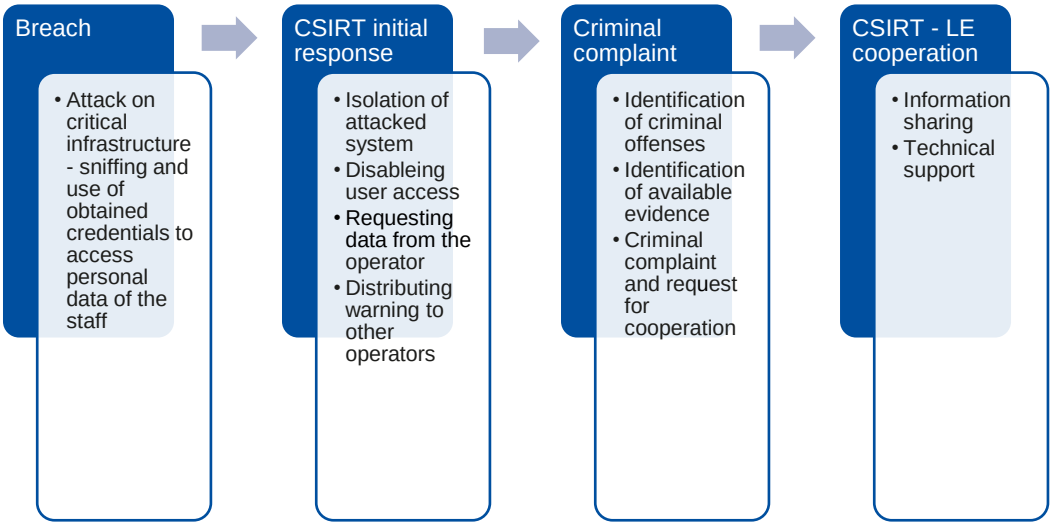
3.1.1 Objectives

- To learn how to use common taxonomy for CSIRTs and LE and identify criminal offenses
- To learn how to prepare criminal complaints and how to request cooperation from LE
- To evaluate your ability to identify information and data that could be useful for LE in criminal investigation
- To evaluate your ability to identify legal limitations to the sharing of relevant information and data
- To compare legal procedures for sharing of information and data in different legal cultures

3.1.2 Scenario

The scenario of the case study is presented in the next page.

Figure 4: Case study scenario



3.1.2.1 Organisational profile

Your organisation is a national CSIRT team responsible for detection and mitigation of cybersecurity incidents within your constituency, which consists of public and private organisations including operators of critical information systems. You are expected to provide support to your constituency and cooperation to other relevant governmental bodies including law enforcement authorities. In your internal policies, it is stated that your staff should report any identified crimes to the LE and also provide any necessary support and assistance during the criminal investigation.

3.1.2.2 Before the breach

Your CSIRT provided your constituency with guidelines on how to identify and report incidents. These guidelines explain how to identify and report a cyber-attack. Your constituency is required by law to identify and report such attacks and to provide necessary cooperation in order to mitigate incidents.

3.1.2.3 Initial response

Breach notification

- Your CSIRT team received a report of an attempted hacking attack on the critical information infrastructure within your constituency.
- The attacker apparently took advantage of a system vulnerability to sniff access credentials of the operator's employees and attempted to use these credentials to access personal data about the staff.
- In the report, the operator states that they are not aware of any data being compromised or stolen.
- In the report, the operator provided attacker's IP address and information about information systems, exploits and attack vectors used.

Response of the CSIRT team

- The CSIRT advised the operator to isolate the attacked system and disable access to all relevant users.
- The CSIRT requested the operator to provide additional detailed information about the attacker and any metadata and logs that may be relevant.

- The CSIRT also distributed a note within the constituency explaining the details of the attack and how to protect relevant systems.
- The CSIRT identified, that the attacker probably committed an offence.

3.1.3 Tasks

You, as member of the CSIRT, are required to initiate and lead the cooperation with the LE. Your goal is to provide help to the LE.

3.1.3.1 Segregation of Duties

Please use the SoD matrix (Figure 6) to identify, what activities can be performed or facilitated by your CSIRT, and what you expect from LE and the judiciary. The SoD matrix should help you to identify expected activities of relevant stakeholders throughout the cybercrime investigation lifecycle. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more.

3.1.3.2 Identify criminal offenses

Use the attached common taxonomy to identify which criminal offenses were likely committed by the attacker. You should keep in mind that one cybersecurity incident could be caused by multiple criminal offenses described in the criminal code or other legislation. Please also identify relevant provisions of your criminal code and of the Directive 2013/40/EU on attacks against information systems defining identified criminal offenses.

Figure 5: List of the identified criminal offences

Criminal offense	Provision of the criminal code and Directive
Tools used for committing offences	Art. 7 of the Directive
Illegal interception	Art. 6 of the Directive
Illegal access to information systems	Art. 3 of the Directive

Figure 6: 'Segregation of Duties' matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
Collecting cyber threat intelligence	✓	✓		✓	Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats	✓	✓		✓	Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats	✓				Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime	✓	✓			Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime	✓	✓			Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime	✓	✓		✓	Incident and crime classification and identification
Identify the type and severity of the compromise	✓	✓		✓	Knowledge of cyber threats and incident response procedures
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Providing technical expertise	✓				Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial	✓	✓		✓	Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)	✓			✓	Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime	✓	✓		✓	Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)	✓				Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling	✓				Communication skills; communication channels
Mitigation of an incident	✓				Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation		✓		✓	Knowledge of the legal framework; decision-making skills
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation			✓	✓	Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE		✓	✓	✓	Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution	✓	✓	✓	✓	Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery	✓				Technical skills
Protecting the constituency	✓				Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view	✓				Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence		✓	✓	✓	Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE			✓	✓	Testimonies in a criminal trial
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Judging who committed a crime			✓		Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost	✓	✓	✓	✓	Evaluation skills
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

**Differences may be highlighted in this matrix depending on the legal framework of each Member State.*

This is just an indicative example.

3.1.3.3 Identify relevant evidence/information

You or members of your constituency might be able to provide LE with important evidence that could help them to identify and prosecute the attacker. At the same time, LE might be able to obtain data (from public authorities/operators/other sources that might be useful to you for mitigating the incident). Please, use the tables below to identify such evidence/data and explain whether these data might be useful to LE/your CSIRT and for what purposes.

Figure 7: List of the evidence collected

Available evidence	Uses for LE
IP addresses	Identify attacker, track attack vector
Metadata/traffic data	dtto
Used sniffing tool	Forensic examination of the tool
Characteristics and configuration files of the attacked system	Analysis of the attack vector

Figure 8: List of the available data

Available data	Uses for CSIRT
Information about the source of the attack	Firewall settings, etc.
Outcome of the forensic examination of the sniffing tool	Closing gaps in the attacked system based on identified vulnerabilities exploited
Forensic tools/data	

3.1.3.4 Prepare criminal complaint and request for cooperation

Please prepare criminal complaint in which you explain what has happened, what criminal offenses have been committed, what kinds of evidence (information and data) you can provide to support your claim, what kinds of cooperation your CSIRT can provide to LE, and what kind of cooperation you expect from the LE.

The structure of the complaint should be the following:

- Identification of relevant LE body
- Explanation of the situation and state of play
- Identification of criminal offences, with links to the criminal code
- Available evidence
- Request for cooperation

Figure 9: Draft of the criminal complaint

Criminal complaint

3.1.3.5 Identify legal limitations to the information sharing

Identify the relevant legal framework that governs cooperation and information sharing, as well as sharing and cooperation limitations provided by the applicable legislation or the internal rules of your CSIRT. Specific rules may apply, related to information protection (personal data, confidential information, trade secrets), infrastructure protection (limitations of emergency legislation), procedural rules (criminal procedure, internal rules) etc. A legal framework may also exist that specifically allows or requires cooperation and/or information sharing (cybersecurity legislation, criminal procedure code, etc.). Please also identify limitations that are not of a legal nature, but which result from established practices or standard procedures of the CSIRT or LE.

Please list identified limitations and explain how these limitations can be managed.

Figure 10: List of the identified limitations

Limitations	Solution
GDPR	DPIA on cooperation and information sharing
Restricting internal guidelines	
Criminal procedure rules	Liaison officer

3.1.3.6 Outcomes

After completing all the tasks, you should be able to use the SoD to identify the responsibilities of both CSIRT and LE. You should also use common taxonomy to identify criminal offenses committed by the attacker and report them to LE in the form of a criminal complaint. You should also be able to identify legal and procedural limitations that prevent or complicate effective cooperation between CSIRTs and LE.

3.1.4 Lessons learned

- Cooperation between CSIRT and LE communities is sometimes necessary to both successfully prosecute cybercriminals and ensure the security of attacked infrastructures and systems.
- The table of ‘Segregation of Duties’ may help you to identify which community should be responsible for what as well as to learn how to avoid duplication of tasks and interference between activities of individual communities.
- The common taxonomy developed by ENISA in cooperation with Europol could be useful to identify and classify criminal offenses committed by the attacker and in preparation of criminal complaints to be submitted to LE.
- There are data available to you that could be used as evidence by LE; LE could also have access to information or contacts that might be useful to CSIRTs for mitigating the incident.
- Cooperation and information sharing between LE and CSIRTs is sometimes complicated due to lack of specific legislation that would allow closer cooperation.

3.2 CASE STUDY – LE APPROACH

The objective of this case study is to present the main limitations to the cooperation between CSIRTs and LE due to the diversity of current legislation in different Member States.

For this case study, it is recommended to divide the trainees in groups; thus, the results and approaches of each group can be compared. This should lead to discussions of the advantages and disadvantages of the individual solutions.

Figure 11: Main objective of the case study

Main Objective	
Targeted Audience	LE, investigators etc.
Total Duration	30 minutes
Scenario	Trainee is a police investigator who deals with cybercrimes.
Task 1	Identify expected activities of relevant stakeholders by filling in the SoD matrix
Task 2	Identify data to be shared with the CSIRT
Task 3	Identify the procedures should be followed for appointing a CSIRT member as forensic expert
Task 4	Request and use information from the CSIRT cooperation network

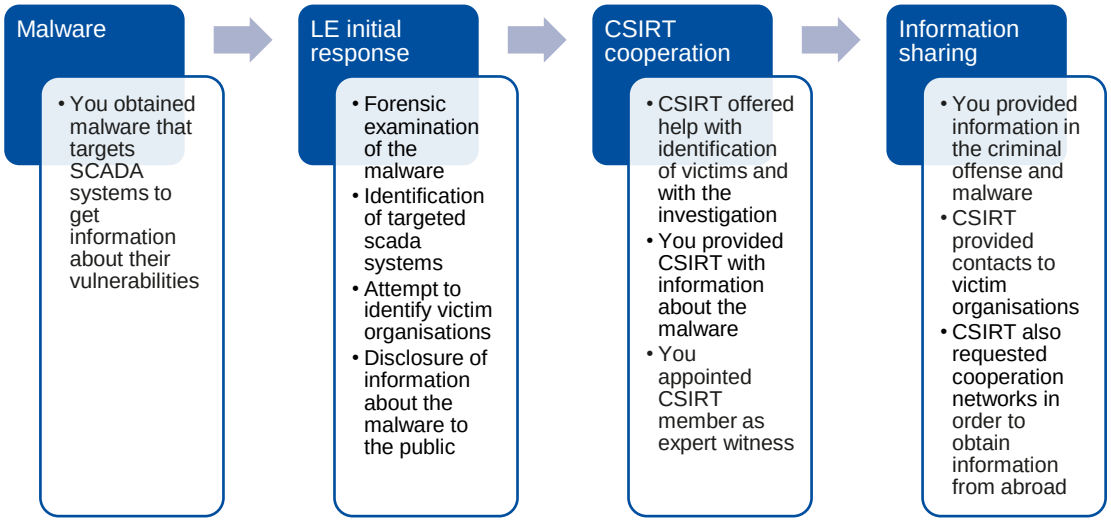
3.2.1 Objectives

- To learn what kind of cooperation and support you can expect from the CSIRT
- To learn how to properly request cooperation and information from the CSIRT
- To evaluate what data and information can be provided by the CSIRT
- To evaluate what data and information you can provide to the CSIRT
- To compare legal procedures for sharing of information and data in different legal cultures

3.2.2 Scenario

The scenario of the case study is presented in the following page.

Figure 12: Case study scenario



3.2.2.1 Organisational profile

You are a police investigator dealing with cybercrime, specifically focused on investigation of organised crime. Your department's jurisdiction is nationwide and deals with cross-border incident cases. LE in your country cooperates with the national and governmental CSIRT via a liaison who is a police officer.

3.2.2.2 Before the breach

You are investigating a crime committed by a foreign perpetrator, which consists of making customized computer viruses. As part of the investigation, you have obtained several malicious programs created by the attacker, including their source code. During the forensic analysis, you have determined that they are designed to attack critical infrastructure in your country, and they collect information about systems' vulnerabilities; this information is uploaded to a server with IP within your national range.

3.2.2.3 Initial response

- Malware collects information about the vulnerabilities of specific SCADA systems.
- You have contacted several critical infrastructure operators, but none of them is using such systems.
- Therefore, you have published in the media information about the vulnerable systems.
- After releasing the information, you are contacting the national CSIRT, which offered you cooperation and help.

3.2.3 Tasks

You, as the lead investigator of the case decided to initiate and lead the cooperation with the CSIRT. Your goal is to both collect as much evidence as possible and help the CSIRT to identify possible attacked operators and help them with the mitigation of any incidents caused by the malware.

3.2.3.1 Segregation of Duties

Please use the SoD matrix (Figure 13) to identify, what activities can be performed or facilitated by your Law Enforcement Agency (LEA), and what you expect from the CSIRT and the judiciary. The SoD matrix should help you to identify expected activities of relevant stakeholders throughout the cybercrime investigation lifecycle. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more.

Figure 13: 'Segregation of Duties' matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training	✓	✓	✓	✓	Problem-solving and critical thinking skills
Collecting cyber threat intelligence	✓	✓		✓	Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats	✓	✓		✓	Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats	✓				Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime	✓	✓			Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime	✓	✓			Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime	✓	✓		✓	Incident and crime classification and identification
Identify the type and severity of the compromise	✓	✓		✓	Knowledge of cyber threats and incident response procedures
Evidence collection	✓	✓		✓	Knowledge of what kind of data to collect; organisation skills
Providing technical expertise	✓				Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial	✓	✓		✓	Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)	✓			✓	Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime	✓	✓		✓	Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)	✓				Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling	✓				Communication skills; communication channels
Mitigation of an incident	✓				Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation		✓		✓	Knowledge of the legal framework; decision-making skills
Leading the criminal investigation			✓	✓	Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation			✓	✓	Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE		✓	✓	✓	Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution	✓	✓	✓	✓	Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery	✓				Technical skills
Protecting the constituency	✓				Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view	✓				Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence		✓	✓	✓	Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE			✓	✓	Testimonies in a criminal trial
Admitting and assessing the evidence			✓	✓	Evidence in a criminal trial
Judging who committed a crime			✓		Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost	✓	✓	✓	✓	Evaluation skills
Reviewing the response and update policies and procedures	✓				Knowledge how to draft an incident response and procedures

**Differences may be highlighted in this matrix depending on the legal framework of each Member State.*

This is just an indicative example.

3.2.3.2 Provide information to CSIRT

Your goal is to identify possible harmed infrastructure operators, to prevent possible damage and to prevent losing valuable evidence. In order to identify the victims, you need to provide the CSIRT team with detailed information about the malware, the type of systems it is targeting, and the type of incidents that may arise from its use. For this purpose, you can use the common taxonomy developed by ENISA in cooperation with Europol, which links criminal offenses to specific types of incidents. Please identify data you can share with the CSIRT. If there are any legal restrictions preventing you from sharing specific data, please explain them.

Figure 14: List of information provided to the CSIRT

Information provided to CSIRT
Any information on:
The malware:
Targeted SCADA systems:
Outcomes of the forensic examination:
Information about the source of the malware:
Legal limitations vary between MS:

3.2.3.3 Appoint a CSIRT member as forensic expert

Since none of forensic experts who are available has experience with targeted SCADA systems, you would like to appoint a CSIRT member who is able to provide valuable input about specifics and target vectors implemented by the malware. The CSIRT member is however not listed in any national forensic experts' list nor does he have any experience with criminal procedure. Please explain if it is possible to appoint the CSIRT member as expert witness and what procedure you need to follow. If there are legal restrictions preventing you from appointing him, please propose other ways on how to make use of his knowledge and experience in the criminal investigation.

Figure 15: List of procedures for CSIRT members as expert witnesses

CSIRT member as expert witness
Member state specific

3.2.3.4 Request and use information from CSIRT cooperation network

You have found out that the creator of the malware is operating abroad in a country where there is no informal police and judicial cooperation and formal mutual legal assistance is ineffective. Therefore, you would like to take advantage of the CSIRT cooperative networks through which unofficial information can be obtained and help to identify the attacker. Please describe in what legal ways such information could be obtained and for what purposes it could be used in criminal proceedings.

Figure 16: Use of information obtained from the CSIRT network

Use of informal information from CSIRT cooperation networks
Member State specific

3.2.3.5 Outcomes

After completing the tasks, you should be able to make use of SoD and common taxonomy for cooperation with the CSIRT. You should also know more ways how CSIRTs can help LE and vice versa. Main advantages of cooperation and information sharing is the possibility of use of specific knowledge and information sources of both communities. It is also clear, that there are often legal limitations to the cooperation, which however vary from country to country.

3.2.4 Lessons learned

- Cooperation between CSIRT and LE communities is sometimes necessary to both successfully prosecute cybercriminal and ensure security of attacked infrastructures and systems.
- Table of 'Segregation of Duties' may help you to identify which community should be responsible for what as well as to learn how to avoid duplication of tasks and interference between activities of individual communities.
- Cooperation and information sharing between LE and CSIRTs is sometimes complicated due to lack of specific legislation that would allow closer cooperation.
- There are legal limitations to what kind of information can be shared between CSIRTs and LE; these limitations vary from country to country.
- It could be useful to appoint CSIRT members as expert witnesses; however, there might be legal or procedural limitations.
- CSIRTs are members of cooperative international networks, which may be used in some cases for obtaining valuable information or even evidence.

4. REFERENCES

ENISA. (2017). *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects.* Retrieved from https://www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement

A ANNEX: ABBREVIATIONS

Abbreviation	Description
APIs	Application Programming Interface
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service (attack)
GDPR	General Data Protection Regulation
IOC	Indicators Of Compromise
IP	Internet Protocol
LE	Law Enforcement
LEA	Law Enforcement Agency
SoD	Segregation (or separation) of Duties

TP-01-20-175-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-334-6
DOI: 10.2824/85709