EUROPEAN UNION AGENCY
FOR CYBERSECURITY

LEGAL AND ORGANISATIONAL ASPECTS OF COOPERATION BETWEEN CSIRTS AND LE

Toolset, Document for trainees

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

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-335-3, DOI: 10.2824/48838

TABLE OF CONTENTS

1. WHAT YOU WILL LEARN

1.1 THEMATIC AREA

In 2017, ENISA presented technical as well as legal and organisational aspects of the cooperation between CSIRTs -in particular national and governmental CSIRTs, and Law Enforcement (LE) and provide 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.

- **Learning outcomes**

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

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

2. CASE STUDIES

2.1 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.

2.1.1 Summary

Figure 1: Main objectives 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 related to a 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 the LE
Task 5	Identify legal limitations to the information sharing

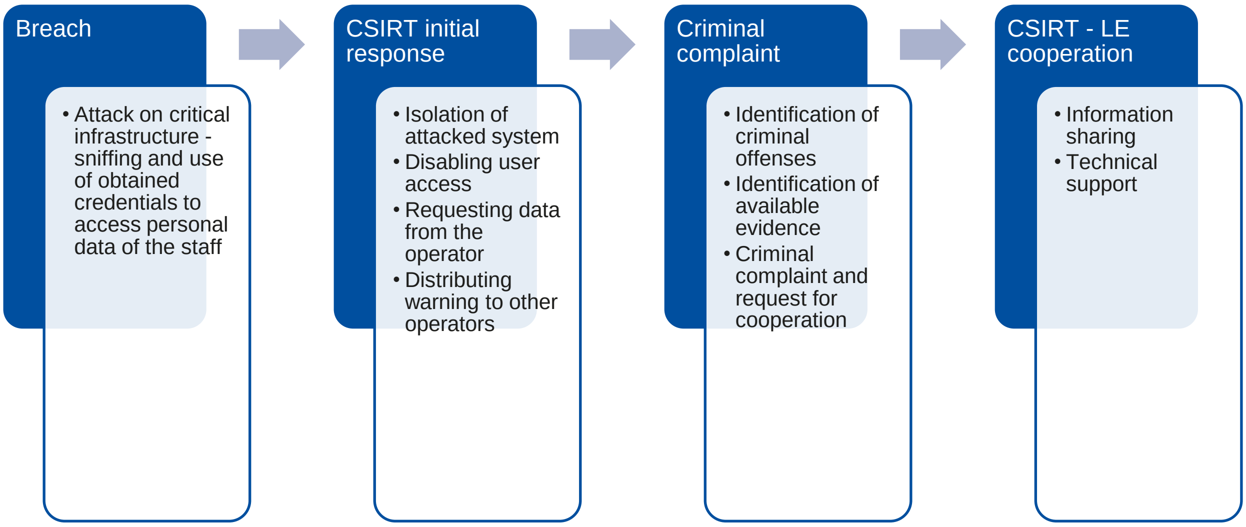
2.1.2 Objectives

- 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 the LE
- To evaluate your ability to identify information and data that could be useful for the 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

2.1.3 Scenario

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

Figure 2: Case study scenario


Breach
• Attack on critical infrastructure - sniffing and use of obtained credentials to access personal data of the staff
CSIRT initial response
• Isolation of attacked system
• Disabling user access
• Requesting data from the operator
• Distributing warning to other operators
Criminal complaint
• Identification of criminal offenses
• Identification of available evidence
• Criminal complaint and request for cooperation
CSIRT - LE cooperation
• Information sharing
• Technical support

2.1.3.1 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.

2.1.3.2 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.

2.1.3.3 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 more 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 attack's details and how to protect relevant systems.
- The CSIRT identified, that the attacker probably committed an offence.

2.1.4 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.

2.1.4.1 SoD matrix

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.

2.1.4.2 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 3: List of the identified criminal offences

Criminal offense	Provision of the criminal code and Directive 2013/40/EU

2.1.4.3 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/ CSIRT and for what purposes.

Figure 4: List of the evidence collected

Available evidence	Uses for LE

Figure 5: List of the available data

Available data	Uses for CSIRT

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

2.1.4.4 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 7: Draft of the criminal complaint

Criminal complaint

2.1.4.5 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 can be managed.

Figure 8: List of the identified limitations

Limitations	Solution

2.1.4.6 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 the LE in the form of a criminal complaint. You also should also be able to identify legal and procedural limitations that prevent or complicate effective cooperation between CSIRTs and LE.

2.1.5 Lessons learned

- Cooperation between CSIRT and LE communities is sometimes necessary to both successfully prosecute cybercriminal and ensure 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. 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
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
SoD	Segregation (or separation) of Duties

TP-01-20-176-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: 978-92-9204-335-3
DOI: 10.2824/48838