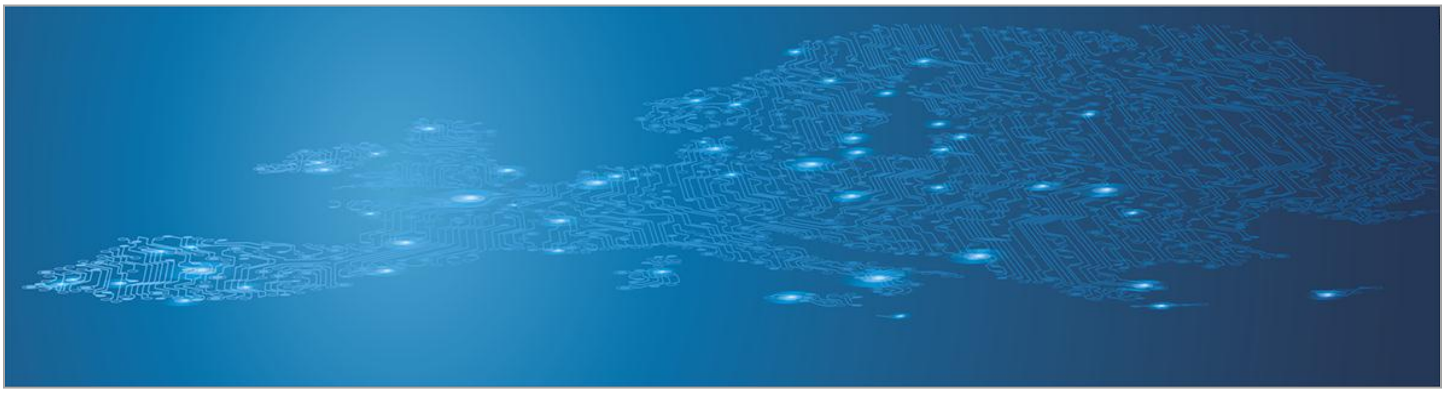


Cooperation in the Area of Cybercrime

Toolset, Document for students

September 2013

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This document was created by the CERT capability team at ENISA in consultation with:

Michael Potter and Don Stikvoort from S-CURE, The Netherlands, Mirosław Maj, Tomasz Chlebowski, Paweł Weżgowiec from ComCERT, Poland, Przemysław Skowron from Poland, Roeland Reijers from Rubicon Projects, The Netherlands and Mirko Wollenberg from DFN-CERT Services, Germany.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquiries about this document, please use press@enisa.europa.eu.

Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors:

1. Andrew Cormack from JANET, United Kingdom
2. Anna-Maria Talihärm from Estonia
3. The countless other people who reviewed this document.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, 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 526/2013. 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 978-92-79-00077-5 doi:10.2788/14231

Table of Contents

1 What you will learn

In this exercise you will explore three hacking/ cybercrime cases, in order to:

- Learn through scenarios the importance of cyber law and cyber law enforcement for the operation of the CERT and – beyond that – for its organisation and management;
- Find pragmatic ways to cooperate with all relevant parties involved in cases of cybercrime: CERT, management, legal counsel, CISO, privacy/ data protection officer, law enforcement.

2 Introduction

From the early stages of the CERT community until around the year 2000, CERT professionals hardly had to deal with cybercrime involving legal action and court cases. That is, in most countries at the time, cybercrime laws had not been written yet and so nefarious activities targeting computers sometimes fell into a grey area. Even in countries that had the beginnings of such legislation, the police had little or no experience in this area.

However, the dotcom boom that started around 1995 and made Internet the critical infrastructure that it is today, present in all layers of society, soon changed this. The Internet started to carry monetary value, personal value (including identities) and finally also cultural, social, political and military value.

Hacking thus evolved from the sport for adventurous students that it mostly was in the 1990s to the usual variety found in everyday life – all the way from small-scale offences to heavy, organised crime, and even terrorism, espionage and counter-measures like cyber defence.

CERT professionals today make an important contribution to the prevention and correction of cyber offences and cybercrime. They form a link between their organisations and constituencies on the one hand, and cyber law enforcement (and cyber defence) on the other hand.

This link is not without complication and tensions, because the CERT professional’s first loyalty is towards the organisation or constituency that he/ she serves and that employs him/ her. The natural reaction is to solve problems within the own organisation with help of management. The boundary between cyber offence and cybercrime is not always clear. Nor is it always clear if and when cyber offences should be reported to law enforcement for investigation and prosecution as cybercrime.

On top of these conflicting interests and confusing circumstances for CERT professionals, the situation is yet more complex. The law not only offers options to punish cybercrime, it also places demands on organisations and companies. The law demands the protection of privacy as employees usually have some form of privacy protection even in their workplace, and system administrators or CERT professionals do not have full investigatory rights by default. Additionally, there may be legal demands on what an organisation must keep in regard to records and for how long, and also what they are not allowed to log or keep, especially when it comes to personal data. So these professionals work in a complex environment, not just technically, but also legally.

And then in those still-rare cases where the police may do a raid and seize computers, or even simply ask for logfiles or data, the CERT professionals and their management often do not know for sure what they must do and what they must not do. What to log? How to treat the logs? What other evidence to gather? How to gather it? The questions seem endless.

Therefore, cooperation in the area of cybercrime and cyber law is increasingly important today, and CERT professionals as well as their management, legal counsel or corporate lawyer, CISO and privacy / data protection officers need to be informed and trained in these issues and questions.

For this reason, a course like the TRANSITS I training for CERT professionals, supported by ENISA, offers a 'legal module', which presents and discusses the legal and law enforcement cooperation aspects of CERT work. This legal module starts off with the 'why' question, using some scenarios to make clear the pressing need for CERT professionals to be aware of cyber legislation and cyber law enforcement – and how to translate this to their own organisation and constituency.

The current exercise builds on that same 'why' question by exploring three real-life hacking/ cybercrime cases and focusing on their content and the questions involved, from a formal/ legal standpoint, and from the standpoint of cooperating with cyber law enforcement.

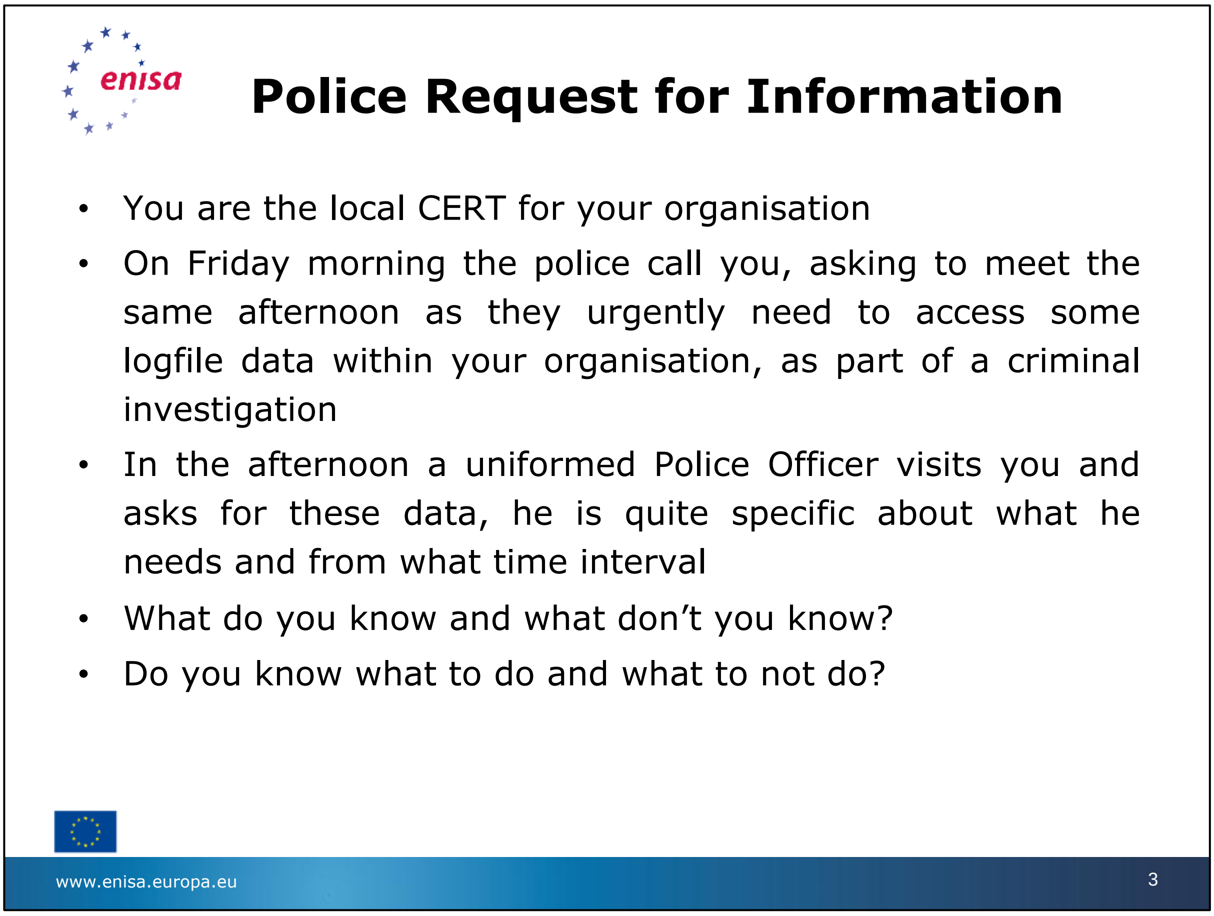
3 Exercise Tasks

The trainer explains the exercise goals and setup.

You are allowed to use laptops or handhelds to connect with the Internet during the exercise, whenever this supports the exercise. The trainer will make clear when and how. Please remember that the use of computers and the Internet during role-plays is meant as fallback and background activity, as the main activities are discussion and role-play!

3.1 Case 1 – Request for Information

Starting point:



Police Request for Information

- You are the local CERT for your organisation
- On Friday morning the police call you, asking to meet the same afternoon as they urgently need to access some logfile data within your organisation, as part of a criminal investigation
- In the afternoon a uniformed Police Officer visits you and asks for these data, he is quite specific about what he needs and from what time interval
- What do you know and what don't you know?
- Do you know what to do and what to not do?

www.enisa.europa.eu 3

3.1.1 Task 1 – role-play

The above slide is the starting scene of a role-play. The organisation involved is a company by the name of Lightning Telecom (LT). LT is an emerging medium-size telecom operator offering the whole range from telephone to Internet and TV services to end users plus a range of IT services to businesses. Their own infrastructure is mostly based on fibre all the way to the customers with an IP infrastructure that carries all services. LT offer state-of-the-art connection services and their business model is to mirror that in the quality of all their services. Thus they take security seriously; they have recently established their CERT, made it a member of TF-CSIRT/Trusted-Introducer and FIRST and they started cooperating with other CERTs in their country and outside. LT promises their customers that they will protect privacy and confidentiality as best they can and as far as the law allows. LT is based in country X and offers its services primarily in the same country. The trainer will tell you what country X will be.

You work in 6 groups; each group is allocated one of the following roles (each group will receive a more detailed role description):

- Jack, LT's CERT duty officer
- Sue, LT's head of IT and CERT line manager (Sue is not the CERT chair)
- Henk, LT's company lawyer
- Marie-Claire, LT's CIO (the CISO is on holiday)
- Claudia, the police officer in charge of the case
- Heinz, the examining magistrate who oversees the case and allowed the local investigation

3.1.2 Task 2 – plenary guided discussion

The following questions are discussed in a general plenary session:

Legal: 'How do I check that this person is a policeman?'

Legal: 'Is the information traffic data (i.e. about traffic: where from, where to, what type, what time) or content (i.e. what was communicated)?' (laws are generally different)

Operational: 'Do I have authority to release the information or does it need to be checked by legal/management?'

Legal: 'What legal power is the policeman using, i.e. how do I know he/ she has sufficient legal grounds to acquire the data he/ she asks for?'

Legal: 'Does that mean I "have" to release the information? Or only that I "may" release it?'

Legal: 'And what conditions apply?' (e.g. under UK data protection law, one can only release information if one is persuaded that it's necessary for the prevention/detection/investigation of a crime: If one is not persuaded then one mustn't disclose it)

Legal: 'Can I tell others about this request?'

Operational: 'Who do I need to inform internally?'

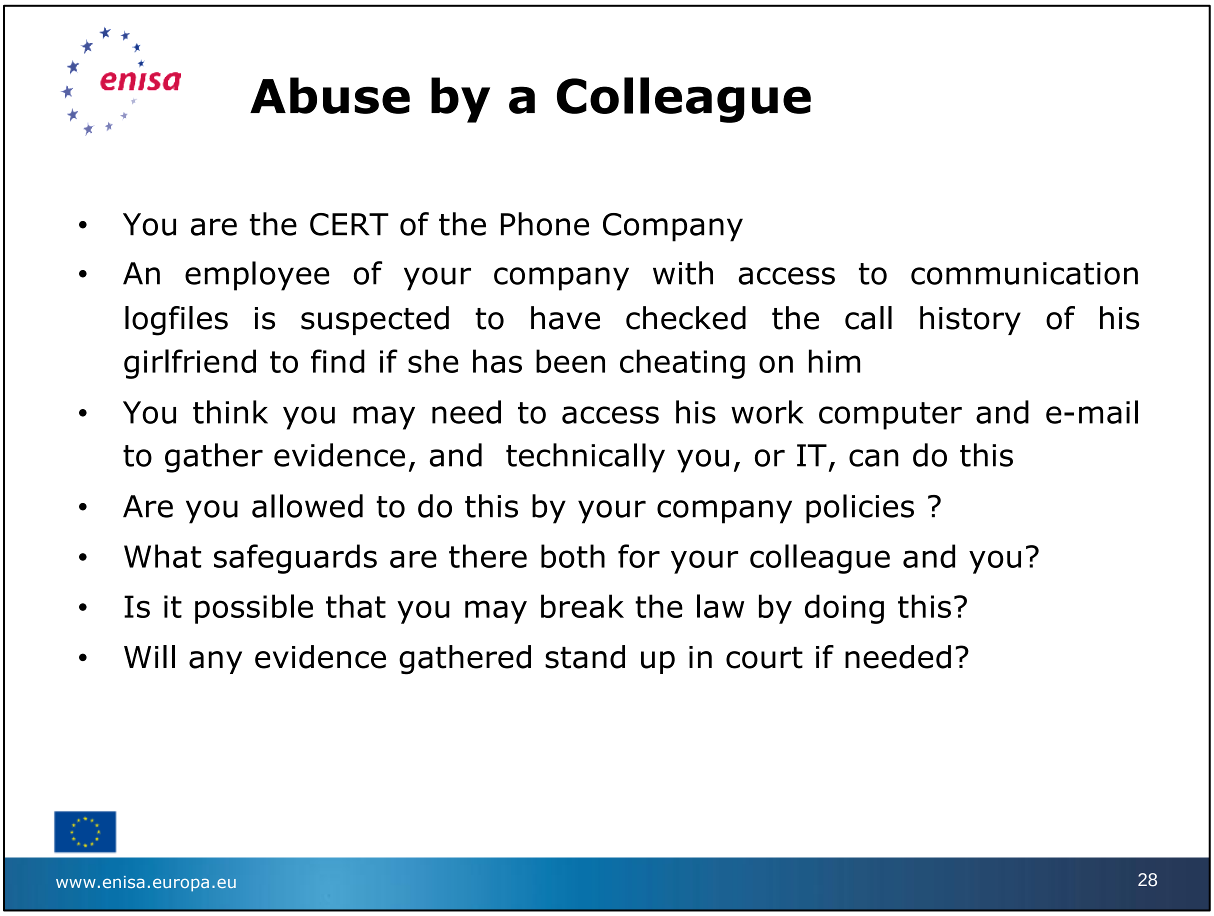
Legal: 'What paperwork is required/offered?'

Legal: 'Is the information to be used as evidence, or only intelligence?' 'Will I be asked/told if that changes?'

Operational: 'What is the appropriate way to release it?' (e.g. handed to policeman on encrypted USB is good, sent via unencrypted email isn't).

3.2 Case 2 – Abuse by a Colleague

Starting point:



Abuse by a Colleague

- You are the CERT of the Phone Company
- An employee of your company with access to communication logfiles is suspected to have checked the call history of his girlfriend to find if she has been cheating on him
- You think you may need to access his work computer and e-mail to gather evidence, and technically you, or IT, can do this
- Are you allowed to do this by your company policies ?
- What safeguards are there both for your colleague and you?
- Is it possible that you may break the law by doing this?
- Will any evidence gathered stand up in court if needed?

www.enisa.europa.eu 28

3.2.1 Task 1 – group discussion

In groups, you discuss the questions from the slide above, plus the following one:

'Even if your company policies or your boss allow you to do this, at what point does this become a matter for the police – who takes that decision, and once it is made, who reports to the police?'

Make sure you back up your group's answers with legal references, quoting or specifically citing them when possible!

3.2.2 Task 2 – group discussion

Each group has to draw up a basic internal policy to deal with deep investigations of staff computers. This policy:

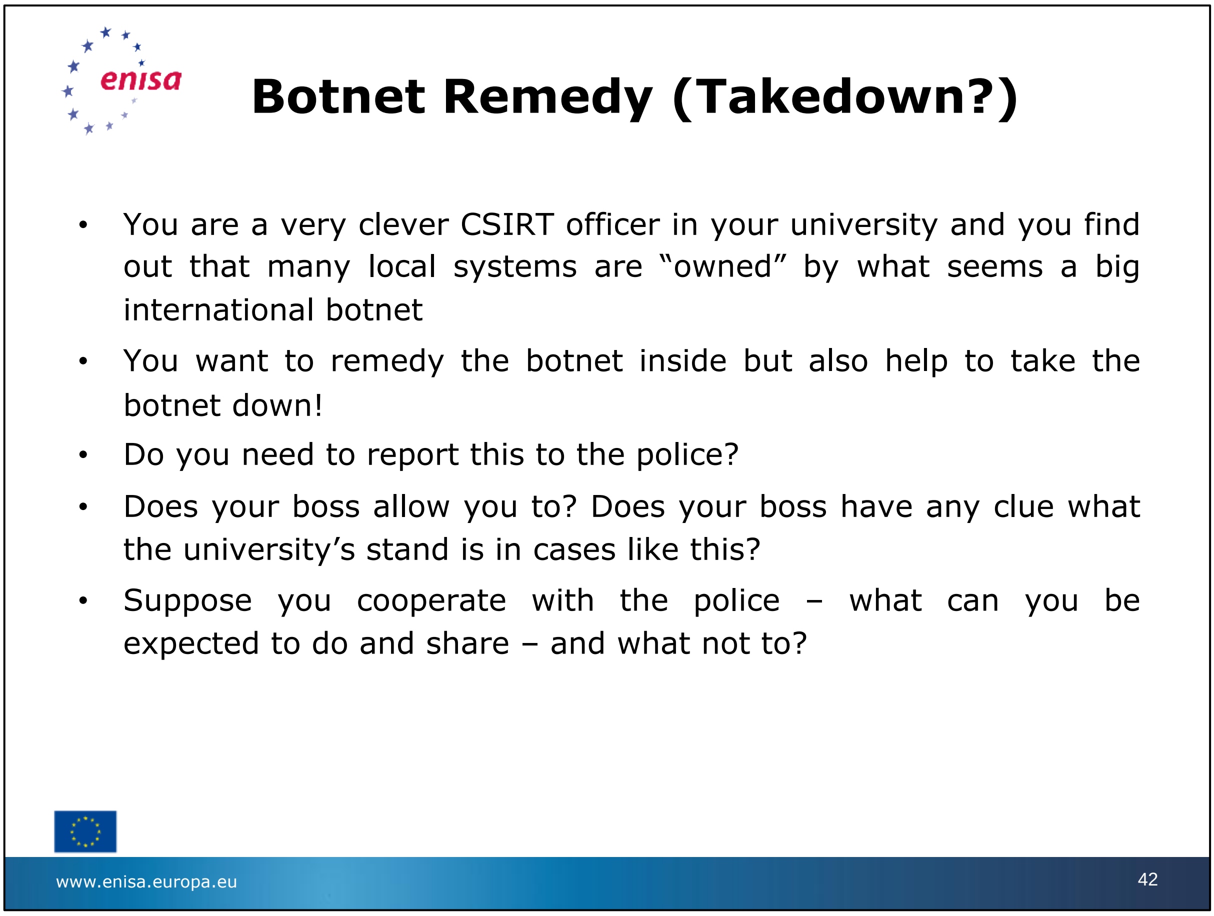
- must include the CERT, CISO, board level, HR department, legal counsel
- must be legally valid.

3.2.3 Task 3 – group discussion

Each group has to draw up an internal guideline on how to secure evidence in cases such as the one discussed here.

3.3 Case 3 – Botnet Remedy: 90 minutes plenary/role-play

Starting point:



Botnet Remedy (Takedown?)

- You are a very clever CSIRT officer in your university and you find out that many local systems are "owned" by what seems a big international botnet
- You want to remedy the botnet inside but also help to take the botnet down!
- Do you need to report this to the police?
- Does your boss allow you to? Does your boss have any clue what the university's stand is in cases like this?
- Suppose you cooperate with the police – what can you be expected to do and share – and what not to?

www.enisa.europa.eu 42

Extra information: your university hosts the Command and Control server and you have been notified of this. You asked the local sysadmin for a copy of the network traffic of that server and file system.

3.3.1 Task 1 – role-play

The above slide is the starting scene of a role-play. The organisation involved is the Da Vinci University (DVU), a well established and internationally respected university in country X – country X is again decided by the trainer.

There are 7 roles this time, for 7 groups. Four roles are the same as for Case 1, only this time in the setting of DVU (each group will receive more detailed role descriptions):

- Jack, DVU's CERT duty officer
- Sue, DVU's head of IT and CERT line manager
- Henk, DVU's lawyer
- Claudia, cyber police officer

New roles are:

- Maestros, the dean of DVU
- Guenther, CERT duty officer of CERT of DVU's ISP, XIS (X Internet Services)
- Jane, CERT duty officer of XCERT, the national CERT of country X

After the role-play we evaluate. The evaluation will include the following aspects:

- Possibly sectoral cooperation?
- Cooperation with ISPs?
- Role of national/government/CIIP team?
- The international aspect of e.g. a botnet takedown like ‘ghostclick’

4 Summary

You need to ask yourself, what is the most significant lesson that you learned in this exercise? And apart from that, what was the next most significant lesson you learned?

Do you know what to do when the police ask you politely to cooperate, or when they raid you?

Do you know what you can do and cannot do in internal investigations against colleagues of yours, or clients of your company?

Do you know what to do, who to contact, and what you are expected to do when computers inside your organisation turn out to be zombies in a botnet?

5 References

1. Convention on Cybercrime (ETS No. 185), Council of Europe, entry into force 1 July 2004, (http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG).
[full text of Council Of Europe's Convention on Cybercrime, the first in the world in 2004, to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation]
2. Cybercrime Legislation – Country profiles website, Council of Europe, (http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp)
[Concise list of many countries with profiles of their computer law with links to relevant resources and contact information.]
3. Cybercrime training for judges and prosecutors: a concept, Council of Europe Project on Cybercrime and the Lisbon Network, 8 October 2009, (http://www.coe.int/t/DGHL/cooperation/LisbonNetwork/meetings/Autre/2079_train_concept_4_provisional_8oct09_en.pdf).
4. Electronic Evidence Guide, Council of Europe, 18 March 2013, (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp)
5. ENISA Fight against Cybercrime – Good Practice Guide webpage, (https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime).
[ENISA references for legal information sharing, good practice guide for addressing network and info security aspects of cybercrime, how to interact with law enforcement]
6. Handbook of Legal Procedures of Computer and Network Misuse in EU Countries, Lorenzo Valeri, Geert Somers, Neil Robinson, Hans Graux, Jos Dumortier, 2006, (http://www.rand.org/pubs/technical_reports/TR337).
[legal procedures for situations of computer misuse including all EU country regulations and laws, evidence handling guidelines, when to contact authorities]
7. Internal Investigations: The Basics, Slater, Derek, CSO Online, (http://www.csoonline.com/article/523413/internal-investigations-the-basics).
8. TRANSITS: CERT Training website (http://www.terena.org/activities/transits/).
9. Working with Law Enforcement (in the United Kingdom): JANET report (https://www.ja.net/support-advice/advice/legal-regulatory-information/working-law-enforcement)
10. Cybercrime, van herkenning tot aangifte: National Cyber Security Centre, January 2012 (Dutch only)
https://www.ncsc.nl/binaries/nl/actueel/nieuwsberichten/publicatie-cybercrime/1/Handreiking%2BCybercrime.pdf
[Detailed and helpful guide from the Dutch national CERT and the police about how to deal with cybercrime, from recognition all the way to reporting to the police – and the role and authority of the police.]
11. Ius Mentis, law and technology explained: website reference (Dutch only)
http://www.iusmentis.com
[350 articles on Internet law and intellectual property rights, written by legal people, but with the aim of explaining the legal aspects to technical people, and the technical aspects to legal people.]

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu