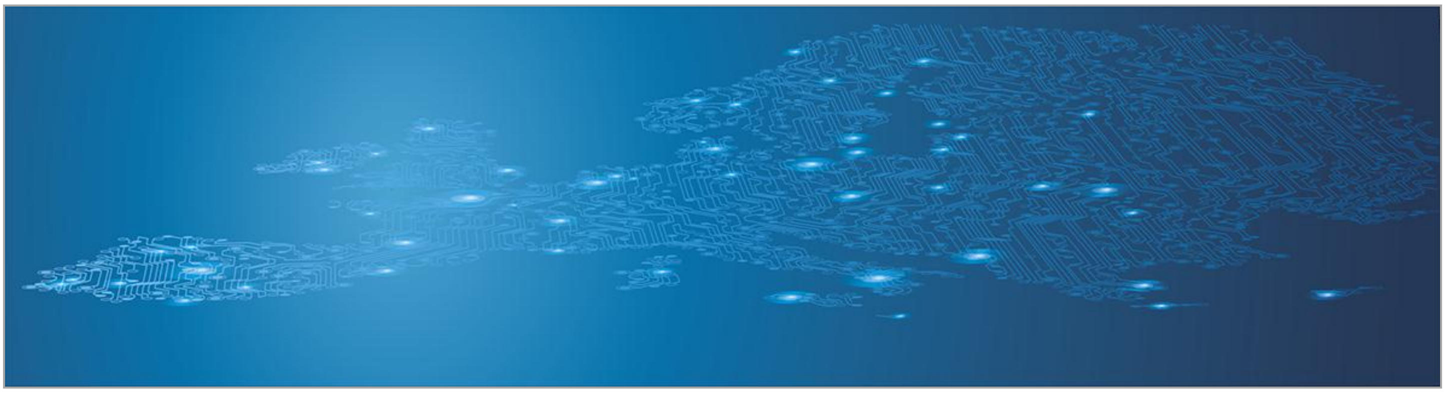


Cooperation in the Area of Cybercrime

Handbook, Document for teachers

September 2013

enisa

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

Main Objective	The exercise covers three different cybercrime related cases. All of them involve investigatory and legal aspects, but each of them requires participants to analyse them from different perspectives. All cases involve very common incidents for CERTs and organisations that could lead to law enforcement actions and court cases. Cooperation among the various parties involved is therefore essential and is the goal of this exercise – rather than exploring the techniques involved. NOTE: this exercise is a follow-up to ENISA exercise 12 'Cooperation with Law Enforcement Agencies'	
Targeted Audience	This exercise is useful for incident responders of all experience levels. It is particularly useful for team leaders and other team members with leading roles. If possible, also involve a representative from the management layer above your team, your corporate lawyer, the CISO and your corporate privacy officer. It is highly recommended to have a law enforcement officer from the cybercrime squad participate, as this will prove very valuable for all involved.	
Total Duration	345 minutes content plus 60 minutes of breaks	
Time Schedule	Introduction to the exercise	15 min.
	Case 1: Request for Information	90 min.
	Break	30 min.
	Case 2: Abuse by a Colleague	130 min.
	Break	30 min.
	Case 3: Botnet Remedy	90 min.
	Summary	20 min.
Frequency	Highly recommended for the majority of organisational CERTs to do at least once, and then repeat once every three years.	

1 General Description

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 the 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 sport for adventurous students, 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 cyber-crime, 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 log files 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 on these issues and questions.

For this reason, a course like the TRANSITS I training for CERT professionals,[1] 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 making them the subject of an exercise which serves to show almost hands-on

[1] http://www.terena.org/activities/transits/

that the aspects of cyber law (enforcement) are essential to a CERT’s business and processes. These aspects will be explored more deeply here with special focus on the cooperation aspects involved.

We now present these three cases and the exercises based on them.

2 Exercise Course

This exercise is best conducted by a trainer plus a co-trainer.

The exercise allows the trainees to discover how essential it is to know about cyber law, cyber law enforcement and cooperation in this area. This will be done in the form of role-plays and guided step-by-step discussions, inspired by three real-life hacking/ cybercrime cases. The trainees will not only discover concepts and ideas, but also find pragmatic answers to real-life questions about how to apply cyber law.

Trainer and co-trainer need to prepare for the exercise well. This is best done by reading this handbook text thoroughly and thinking through the changing physical requirements for seating and tables and the accompanying materials, hand-outs and projected slides. When you conduct the exercise for the first time, we advise trainer and co-trainer to do a (shortened!) dry-run with the trainer in the trainer role, and the co-trainer in the attendee's role, seeing how the exercise works in practice. Also, it is advisable for the co-trainer to take care of the timings, physical aspects and hand-outs, so that the trainer can focus on the trainees and the few slides he or she needs to present. Once the trainer and co-trainer have done this exercise once or twice, it will flow naturally. This is based on experience from similar role-play/ discussion exercises such as those used in the courses TRANSITS I and II.

Trainees are allowed to use laptops or handhelds to connect with the Internet during the exercise, whenever this supports the exercise. This will be indicated below by the text 'Internet use allowed'. **However, the trainer needs to make clear to the students that the use of computers and the Internet during role-plays is meant as fall-back and background activity, as the main activity is the role-play – not screen work! The trainer needs to keep an eye out during the role-plays and correct groups which become too 'screen focused'.**

3 Introduction: 15 minutes plenary

The trainer explains to the trainees the goal of the exercise, which is exploring three hacking/ cybercrime cases, in order to:

- Demonstrate 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.

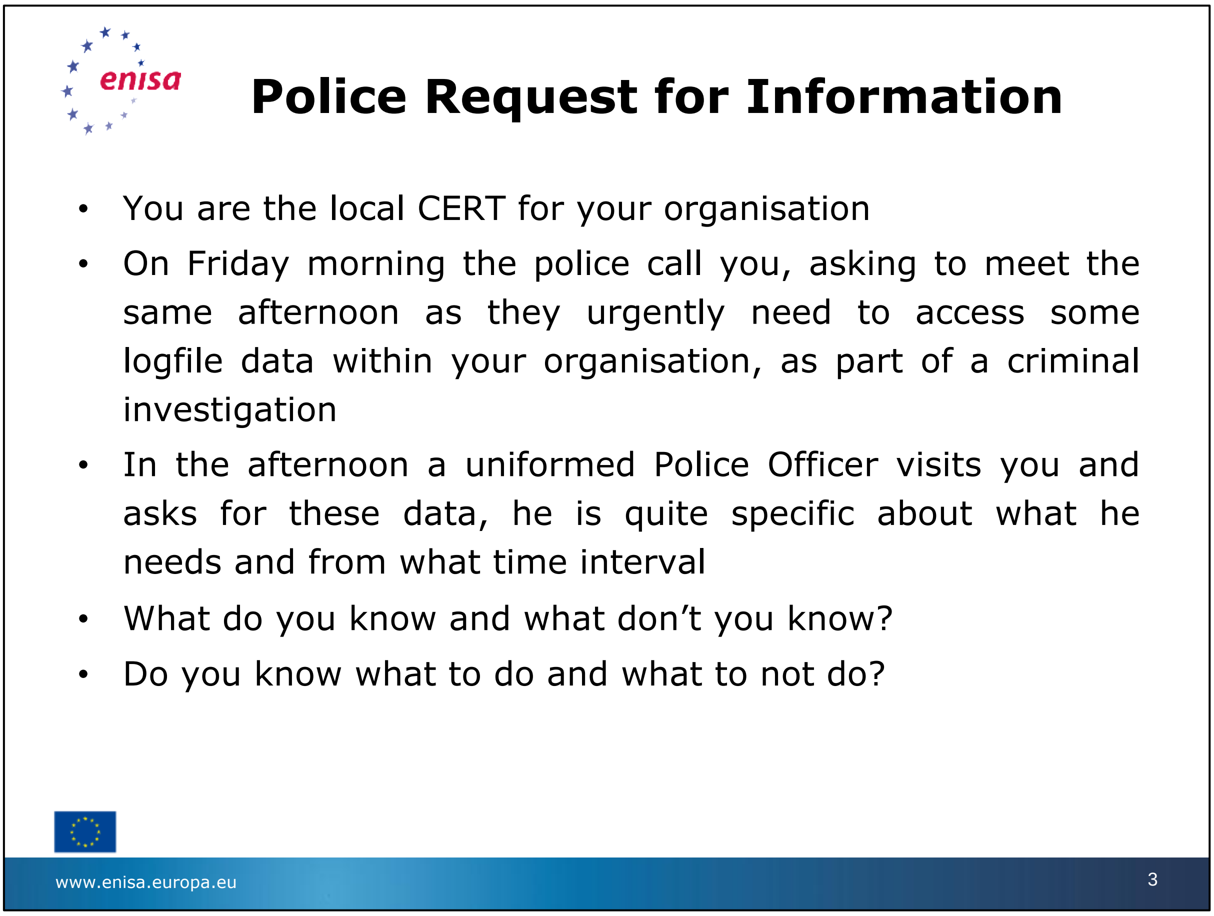
The trainer continues to explain the set-up used to reach these goals:

- Depending on the case and task at hand do a role-play together, hold a general discussion with all trainees or work in 'small groups' which here means 3–4 trainees;
- The trainer, assisted by the co-trainer, will guide the various cases and tasks and can at any time steer discussions or events (e.g. in a role-play) in any direction – the trainees can regard the trainer and co-trainer as the directors of the play they are all in;
- When working in small groups, one trainee is to take notes in each group – and other[2] group members will be asked to present these notes and/or participate in a guided plenary discussion following the group work.

[2] *If possible the one taking notes should not be the one presenting them, to maximise the participation of the trainees.*

4 Case 1 – Request for Information: 90 minutes plenary/role-play + 30-minute break

The trainer displays the following case without explanation and the co-trainer hands it out to all in printed form as a reminder:[3]



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] *In case the question is asked: 'what kind of logfiles' – the answer is: 'logs about the activity of a specific employee, when the employee was working, what connections were set up to where, etc.'*

4.1 Task 1 – role-play: 45 minutes plenary

The trainer turns the scenario from the slide into the starting scene of a role-play.

He explains that 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 offers 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 – more about X below.

The trainer then explains there are 6 roles:

- 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.

Furthermore, the trainer explains in which country the scenario primarily takes place. If all trainees are from country X, then it will be country X. If the trainees are an international group, then the trainer picks for X the country of origin of a subset of the trainees.[4]

The trainer then divides the group into 6 equal sized subgroups. The co-trainer makes sure that each subgroup sits together, and if possible the 6 groups locate themselves at equal distances spread over an imaginary circle. For each group there is a small table. The co-trainer gives each group their role description to read, while the trainer puts up a slide which displays the six roles – this slide stays on display. The grouping process and role reading takes around 10 minutes.

Internet use is allowed to find the right approach when this might happen in real life.

The role-play is kicked off with the slide and lasts around 30 minutes. Trainer and co-trainer allow the play to flow, but provide guidance (see below) when necessary to avoid dead ends or to provide inspiration. They can freeze time, rewind, insert new circumstances, erase events – whatever is required to stimulate the best learning. However, providing too much direction will kill the play; the players need to have enough freedom to improvise and learn 'on the job'.

In order to guide the role-play, trainer and co-trainer need to know the following guidelines for what to do when faced with a police request/ order:

- Try to have a witness present
- Make the requester state their identity and capacity
- Ask whether cooperation is mandatory or voluntary
- Ask under what legal power the request is made
- Determine your own capacity in this case
- If appropriate, comply (possibly under protest), or direct the requester to a more appropriate person

[4] *Preferably use for X a country about which one or more of the trainees have working knowledge in regard to cyber law enforcement*

- In all cases record all answers and actions
    - Date, requester, witnesses, other relevant info

This section ends with a 5-minute open evaluation.

During the evaluation, trainees should share and trainers should note any online references the trainees found useful during the exercise. Below are several that should be shared with the trainees if they were not already identified:

- *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*[5]
- ENISA Fight against Cybercrime – Good Practice Guide webpage[6]

4.2 Task 2 – plenary guided discussion: 45 minutes plenary

The co-trainer re-arranges the physical layout **only** insofar is necessary for the trainer to be able to conduct a plenary discussion with the whole group. There is no need to all go back to a classroom-style layout. The trainer needs a whiteboard and/or flipchart, for all to see.

The trainer then guides the group through the following questions. Stimulate discussion and find answers together and write them down in brief, while the co-trainer takes notes of the results. Internet use is allowed. The trainer and co-trainer should only insert their knowledge when necessary to move on. For UK and Dutch legislation, sample answers are provided in the slides.[7]

Questions: (2–4 minutes per question)

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 must not 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?’

[5] *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).*

[6] *https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime*

[7] *Answers based on, for the UK, https://www.ja.net/support-advice/advice/legal-regulatory-information/working-law-enforcement and for The Netherlands (only available in Dutch), https://www.ncsc.nl/binaries/nl/actueel/nieuwsberichten/publicatie-cybercrime/1/Handreiking%2BCybercrime.pdf (very complete and up-to-date source) and http://www.iusmentis.com*

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)

Together a 'modus operandi' is developed to handle cases like this – this is especially powerful when all trainees are from the same country, as the modus operandi can then become quite specific. As the co-trainer has taken notes, he/ she will send these around to all trainees in a polished version within 1 week after the exercise.

At the end of the discussion, spend 5–10 minutes discussing the importance of creating cooperation with your legal counsel and law enforcement **before** incidents happen. Discuss the following three scopes of cooperation:

- local cooperation (inside your organisation and with local cyber law enforcement)
- national cooperation (set up if needed: special role for n/g teams)
- international cooperation (if needed explain TF-CSIRT, FIRST, Europol, Interpol)

As mentioned above, there are several resources that are useful for trainees to have including:

- *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*[8]
- ENISA Fight against Cybercrime – Good Practice Guide webpage[9]
- *Electronic Evidence Guide from Council of Europe Cybercrime project*[10]
- *Cybercrime Legislation – Country profiles* website, Council of Europe[11]
- *Convention on Cybercrime (ETS No. 185)*[12]

30-minute break

This 30-minute break is foreseen when the group continues with case 2.

[8] *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).*

[9] *https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime*

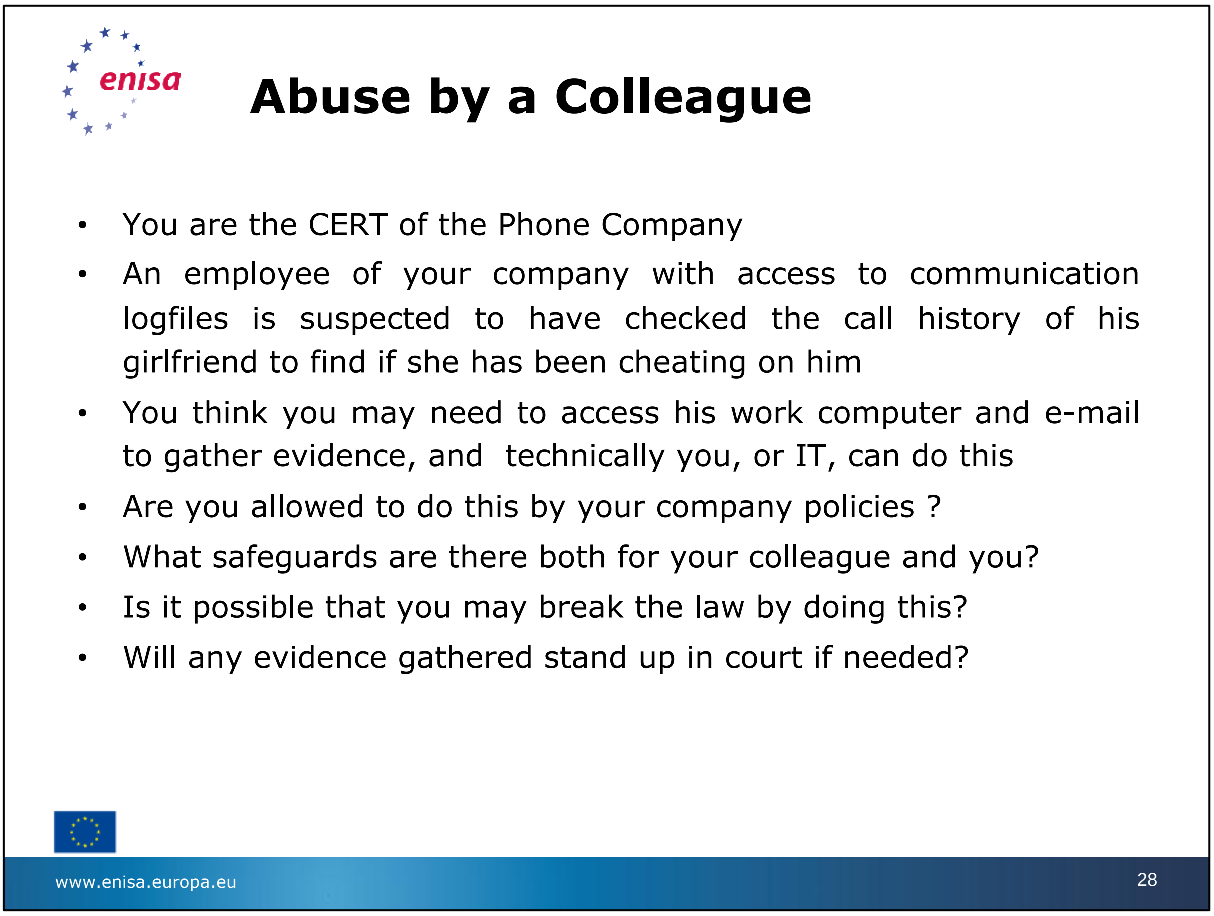
[10] *Electronic Evidence Guide, Council of Europe, 18 March 2013 : http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp)*

[11] *http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp*

[12] *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG*

5 Case 2 – Abuse by a Colleague: 130 minutes in small groups + 30/60-minute break

The trainer displays the introductory slide without explanation and the co-trainer hands it out to all in printed form as a reminder:



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

5.1 Task 1 – group discussion: 45 minutes in small groups

The co-trainer gets the trainees to sit together in small groups. Each group needs at least one table. These groups will be used until the end of this case. Any plenary discussions will be carried out with the trainees sitting in their groups, so the trainer and whiteboard or flipchart need to be in a place where everyone can see them.

Each group is assigned by the trainer to discuss and answer the 4 questions in the presented slide, plus the following one as number 5 – the co-trainer is to hand out the 5 questions to each group in printed form:

‘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?’ (Background information for trainers: even if it's only disciplinary, in countries like Germany, the UK and The Netherlands you can get into serious trouble if you don't follow a documented, appropriate procedure. If the procedure isn’t followed, any employee dismissal could be ruled unfair and that the former employee might receive additional compensation.)

This makes 5 questions for 35 minutes maximum, so 7 minutes per question. It is each group's responsibility to go through the questions and make notes – each group should back up its answers with legal references, quoting or specifically citing them when possible! The trainer and co-trainer should walk around to monitor the groups, seeing how they are progressing and helping when needed. Internet use is allowed.

The last 10 minutes is spent on presenting the answers in plenary with discussion guided by the trainer. If the trainees are in 5 groups, each group covers one of the 5 questions.

5.2 Task 2 – group discussion: 40 minutes in small groups

The exercise continues in the same small groups. All groups are assigned by the trainer 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.

A further resource for guidance on writing policies involving the investigation of employees is:

- 'Internal Investigations: The Basics' from CSO Online magazine.[13]

Make the group aware that legislation differs from country to country. Ideally, the members of a group are all from one country and can focus on their local legal context. In more international settings, it is advised that each group treats the case for one of the countries represented in the group. If one trainee in the group is more aware of these legal issues (simply ask in each group), then use that trainee's country in that group. One resource to use to investigate the distinctions of different countries' legal systems is the Council of Europe's Cybercrime Legislations – country profiles.[14]

Allow the group 25 minutes to discuss. The trainer and co-trainer should walk around the groups again to monitor their progress. Internet use is allowed.

The last 15 minutes is spent on presenting one, at most two, answers in plenary with discussion guided by the trainer. In the discussion, pose the question 'and what if the company is international, what does that mean for a policy like this?' The slides provide some help. The trainer and co-trainer together decide which groups will present.

5.3 Task 3 – group discussion: 45 minutes in small groups

The exercise continues in the same small groups. All groups are assigned by the trainer to draw up an internal guideline on how to secure evidence in cases such as the one discussed here.

The trainer first indicates in maximum 10 minutes some basic concepts for such a guideline for a specific national legislation (the slides offer basic concepts for UK legislation) as illustration and to kick-start the discussion. The trainer should also point out these considerations:

- does the CERT/organisation do this themselves, or hire experts
- when and how to cooperate with law enforcement.

The following are several online resources that discuss concepts of evidence collection and national and international legislation:

- *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*[15]

[13] *http://www.csoonline.com/article/523413/internal-investigations-the-basics*

[14] *http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp*

[15] *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).*

- *Electronic Evidence Guide from Council of Europe Cybercrime project*[16]
- *Cybercrime training for judges and prosecutors*[17]
- *UK: ACPO guide*[18]

Next, the groups have 25 minutes to discuss. Use the same countries as in task 2 – if a group has a good reason to do another country, allow this. The trainer and co-trainer walk around the groups again to monitor their progress. Internet use is allowed.

The last 10 minutes is spent on presenting one, at most two, answers in plenary with discussion guided by the trainer. The trainer and co-trainer together decide which groups will present.

30 minute break

This 30-minute break is foreseen when the group continues with case 3.

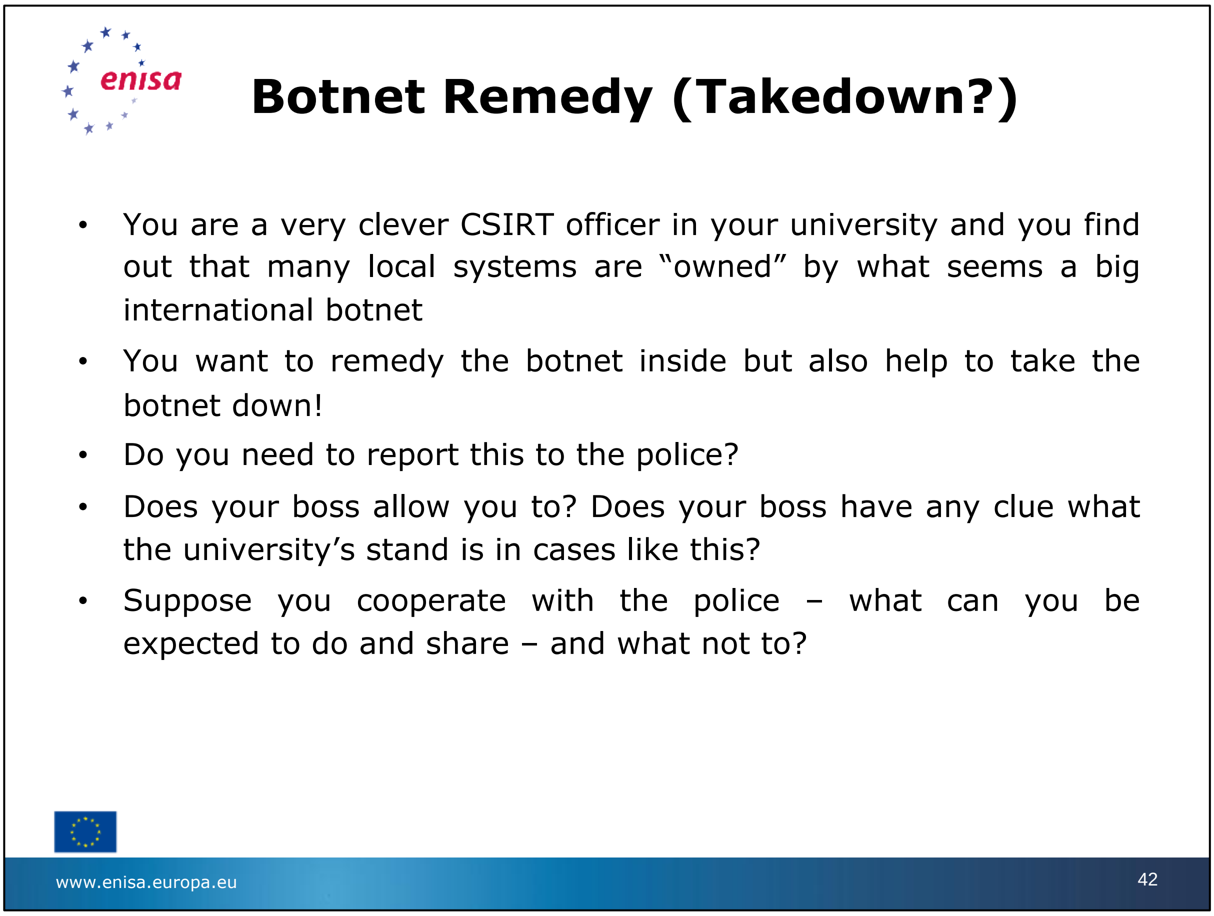
[16] *Electronic Evidence Guide, Council of Europe, 18 March 2013: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp*

[17] *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*

[18] *http://library.npia.police.uk/docs/acpo/digital-evidence-2012.pdf*

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

The trainer displays the introductory slide without explanation and the co-trainer hands it out to all in printed form as a reminder:



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

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

6.1 Task 1 – role-play: 90 minutes plenary

The trainer turns the scenario from the slide into the starting scene of a role-play. He explains there are 7 roles. Four roles are the same as for Case 1, only this time in the setting of Da Vinci University (DVU), a well-established and internationally respected university in country X:

- 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

- If e.g. the national neutral Internet exchange needs to act, or a normal police officer, the (co) trainer can play these roles

Furthermore, the trainer explains in which country the scenario primarily takes place. The same reasoning applies as in case 1. Therefore, most likely country X will be the same country – but with an international body of trainees, it can be beneficial to select another country for this case.[19]

The trainer then divides the group into 7 subgroups with equal numbers of trainees. The co-trainer makes sure that each subgroup sits together, and if possible the 7 groups locate themselves at equal distances spread over an imaginary circle. For each group there is a small table. The co-trainer gives each group their role description to read, while the trainer puts up a slide which displays the 7 roles – this slide stays on display. The grouping process and role reading takes around 10 minutes.

Internet use is allowed to find the right approach when this might happen in real life.

The role-play is kicked off with the slide and lasts a maximum 60 minutes. Trainer and co-trainer allow the play to flow freely, but provide guidance when necessary to avoid dead ends or to provide inspiration. They can freeze time, rewind, insert new circumstances, erase events, whatever is required to stimulate the best learning. However, too much direction will kill the play; the players need to have enough freedom to improvise and learn 'on the job'.

This section ends with a 20-minute open evaluation, guided by the trainer. The co-trainer re-arranges the physical layout **only** insofar as necessary for the trainer to be able to do this plenary evaluation with the whole group. There is no need to go back to a classroom-style layout. The trainer needs a whiteboard or flipchart that all trainees can see.

In the evaluation the trainer focuses on what can be learned **in addition** to what was already learned in case 1 of this exercise:

- Possibly sectoral cooperation?
- Cooperation with ISPs?
- Role of national/government/CIIP team?
- Stress how international the issues of a botnet takedown is
    - use a real case like 'ghostclick' to illustrate[20]

The co-trainer takes notes of the evaluation and adds those to the notes that he or she will send to all trainees in a polished version within 1 week after the exercise.

[19] Preferably use for X a country about which one or more of the trainees have working knowledge in regard to cyber law enforcement

[20] see http://arstechnica.com/tech-policy/2011/11/how-the-most-massive-botnet-scam-ever-made-millions-for-estonian-hackers/ and http://arstechnica.com/tech-policy/2011/11/seven-charged-in-botnet-driven-click-fraud-case/

7 Summary

During the summary section, the trainer asks various trainees ‘what is the most significant lesson that you learned in this exercise?’ Discuss each answer briefly. If the trainees give answers that are too similar, the trainer will need to challenge the trainees more by asking them what specifically they learned from case 1, or 2, or 3. If the answers are still repetitive, use the question ‘and apart from that, what was the next most significant lesson you learned?’

8 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