Achieving Global Cyber Security Through Collaboration

Steve Purser
Head of Core Operations Department

December 2013

Agenda

- About ENISA
- The EU Cyber Security Strategy
- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification

ENISA

- The European Network & Information Security Agency (ENISA) was formed in 2004.
- The Agency is a Centre of Expertise that supports the Commission and the EU Member States in the area of information security.
- We facilitate the exchange of information between EU institutions, the public sector and the private sector.

Agenda

- About ENISA
- The EU Cyber Security Strategy
- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

EU Cyber Security Strategy

- The Five strategic objectives of the strategy:
  - Achieving cyber resilience
  - Drastically reducing cybercrime
  - Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
  - Developing the industrial and technological resources for cybersecurity
  - Establishing a coherent international cyberspace policy for the European Union and promote core EU values.

🟥 ENISA explicitly called upon.

Agenda

- About ENISA
- The EU Cyber Security Strategy
- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

The ENISA Threat Landscape

- The ENISA Threat Landscape provides an overview of threats and current and emerging trends.
- It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends.
- Over 120 recent reports from a variety of resources have been analysed.

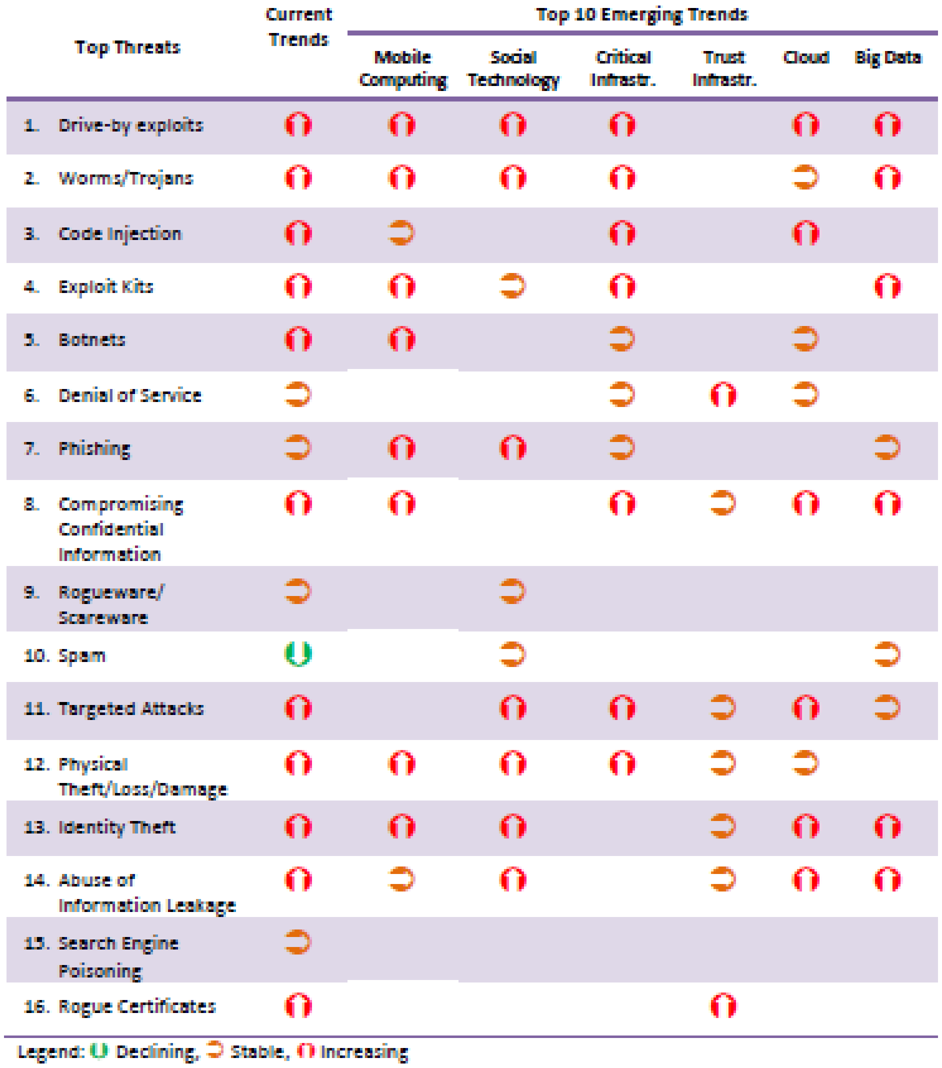
enisa
European Network and Information Security Agency

ENISA Threat Landscape

Responding to the Evolving Threat Environment

[Deliverable – 2012-09-28]

Developed overview



Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	∩	∩	∩	∩		∩	∩
2. Worms/Trojans	∩	∩	∩	∩		⊃	∩
3. Code Injection	∩	⊃		∩		∩	
4. Exploit Kits	∩	∩	⊃	∩			∩
5. Botnets	∩	∩		⊃		⊃	
6. Denial of Service	⊃			⊃	∩	⊃	
7. Phishing	⊃	∩	∩	⊃			⊃
8. Compromising Confidential Information	∩	∩		∩	⊃	∩	∩
9. Rogueware/ Scareware	⊃		⊃				
10. Spam	∪		⊃				⊃
11. Targeted Attacks	∩		∩	∩	⊃	∩	⊃
12. Physical Theft/Loss/Damage	∩	∩	∩	∩	⊃	⊃	
13. Identity Theft	∩	∩	∩		⊃	∩	∩
14. Abuse of Information Leakage	∩	⊃	∩		⊃	∩	∩
15. Search Engine Poisoning	⊃						
16. Rogue Certificates	∩				∩		

Legend: ∪ Declining, ⊃ Stable, ∩ Increasing

Table 1: Overview of Threats and Trends of the ENISA Landscape[2]

Cyber Exercises

- Cyber Europe 2010.
  - Europe's first ever international cyber security exercise
- EU-US exercise, 2011.
  - Also a first : work with COM & MS to build transatlantic cooperation
- Cyber Europe 2012.
  - Developed from 2010 & 2011 exercises.
  - Involves MS, private sector and EU institutions.
  - Highly realistic exercise, Oct 2012

Securing New Technologies

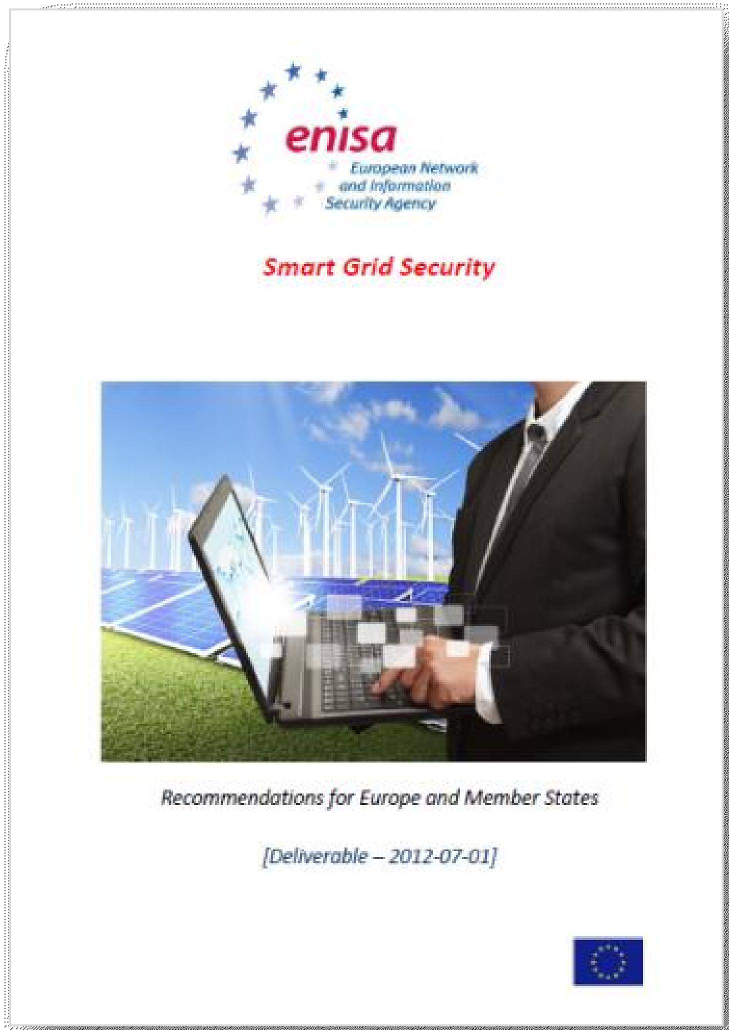
Cloud Computing

November | 09

Benefits, risks and recommendations for information security

enisa

European Network and Information Security Agency



enisa

European Network and Information Security Agency

Smart Grid Security

Recommendations for Europe and Member States

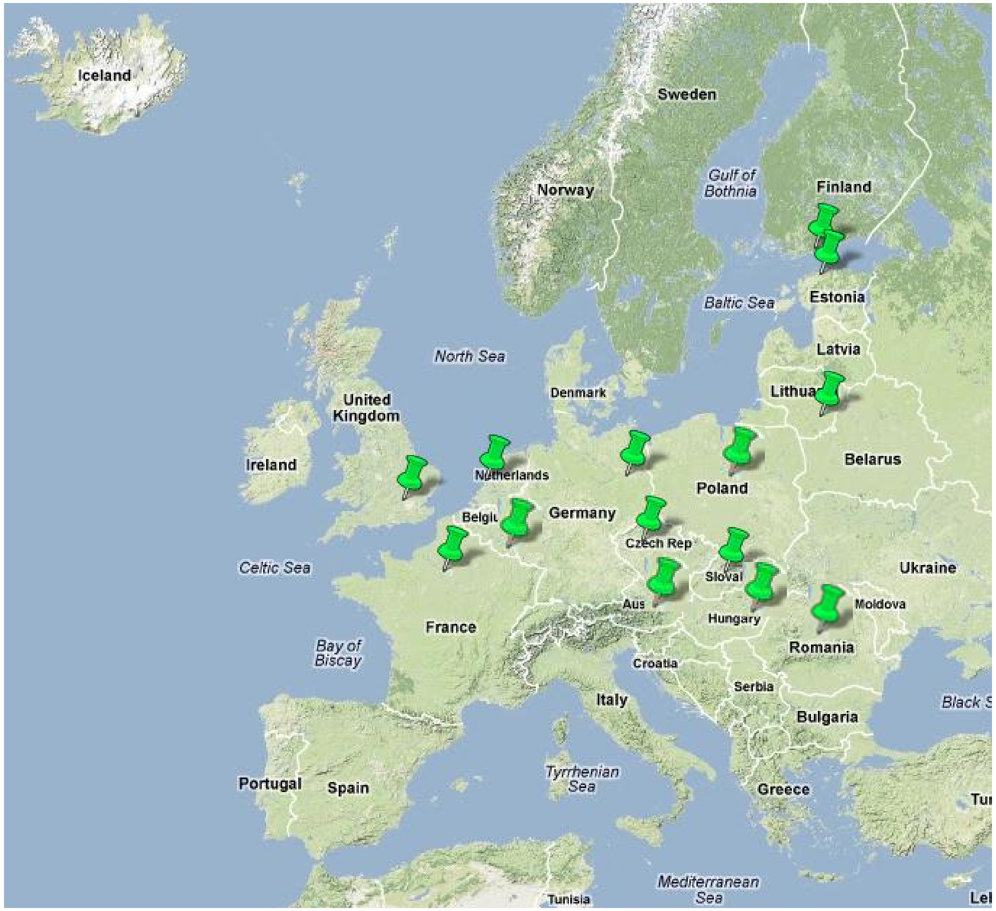
[Deliverable – 2012-07-01]

Agenda

- About ENISA
- The EU Cyber Security Strategy
- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

Member States with NCSS

- ✓ Austria
- ✓ Czech Republic
- ✓ Estonia
- ✓ Finland
- ✓ France
- ✓ Germany
- ✓ Hungary
- ✓ Lithuania
- ✓ Luxemburg
- ✓ Netherlands
- ✓ Poland
- ✓ Romania
- ✓ Slovakia
- ✓ United Kingdom



Good Practice Guide

- ENISA deliverable of 2012
- Describes:
  - Known good practices, standards and policies
  - The elements of a good Cyber Security Strategy
  - Institutions and roles identified in a Strategy
  - Parties involved in the development lifecycle
  - Challenges in developing and maintaining a Strategy

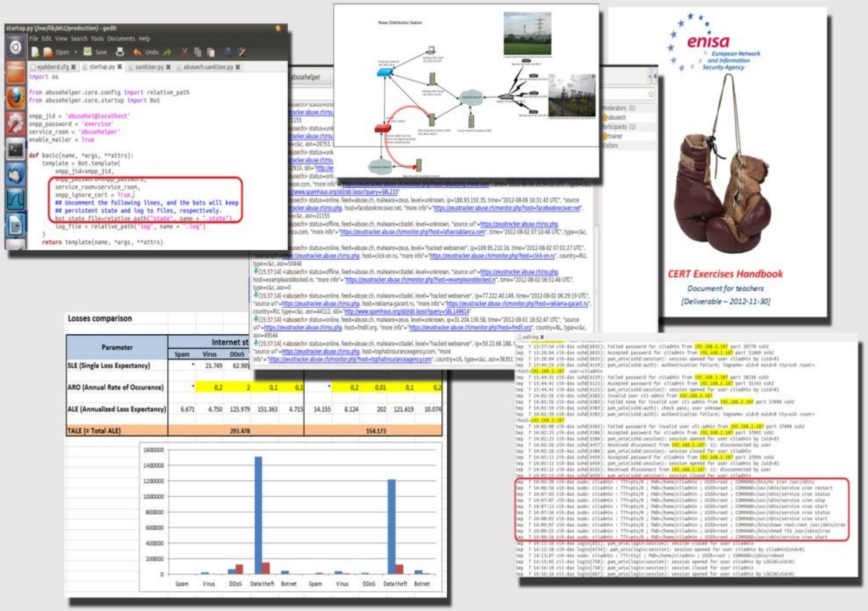
Agenda

- About ENISA
- The EU Cyber Security Strategy
- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

Supporting Operational Communities - Overview

Supporting the CERT community

ENISA Annual CERT workshops focus on national and governmental CERTs preparedness and response capabilities



```
import os

from abusehelper.core.config import relative_path
from abusehelper.core.startup import Bot

xmpp_jid = 'abusehel@localhost'
xmpp_password = 'exercise'
service_room = 'abusehelper'
enable_mailer = True

def basic(name, *args, **attrs):
    template = Bot.template(
        xmpp_jid=xmpp_jid,
        xmpp_password=xmpp_password,
        service_room=service_room,
        xmpp_ignore_cert = True,
        ## Uncomment the following lines, and the bots will keep
        ## persistent state and log to files, respectively.
        bot_state_file=relative_path("state", name + ".state"),
        log_file = relative_path("log", name + ".log")
    )
    return template(name, *args, **attrs)
```

Losses comparison

Parameter	Internet st									
	Spam	Virus	DDoS							
SLE (Single Loss Expectancy)	*	23.749	62.98							
ARO (Annual Rate of Occurence)	*	0,2	2	0,1	0,1	*	0,2	0,01	0,1	0,2
ALE (Annualized Loss Expectancy)	6.671	4.750	125.979	151.363	4.715	14.155	8.124	202	121.619	10.074
TALE (= Total ALE)	293.478					154.173				

enisa
European Network and Information Security Agency

CERT Exercises Handbook

Document for teachers

[Deliverable – 2012-11-30]

FIRST – to improve CERT capabilities

FIRST Improving Security Together

Lecc. FIRST SIG

CSIRT Metrics FIRST SIG

New Exercise material 2012
- Technical trainings for CERTs
- Handbook for teachers
- Toolset for students
- SW ready to use from our website: www.enisa.europa.eu/activities/cert/support

TRANSITS

TRANSITS framework: support the basic and advanced training courses for CERTs

Cross-communities Support

INTERPOL
Atomic exercise 2012

INTERPOL

ENISA-EUROPOL joint workshop: "Addressing NIS aspects of cybercrime"

EUROPOL

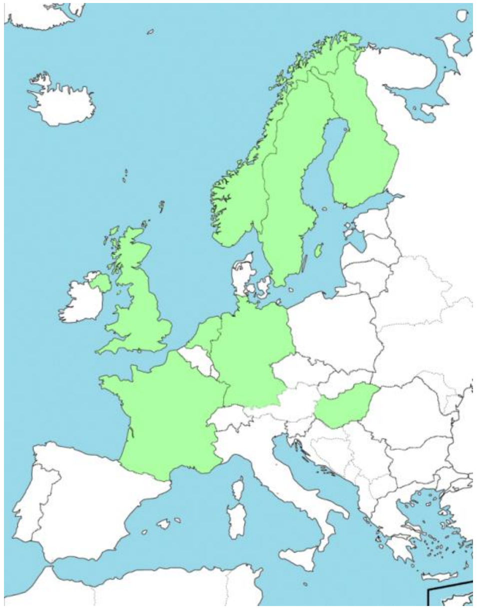
EU FI-ISAC exercise for CERTs, LEA and banks

CEPOL
European Police College

CEPOL courses: (operational security unit supports cyber work-shops for police)

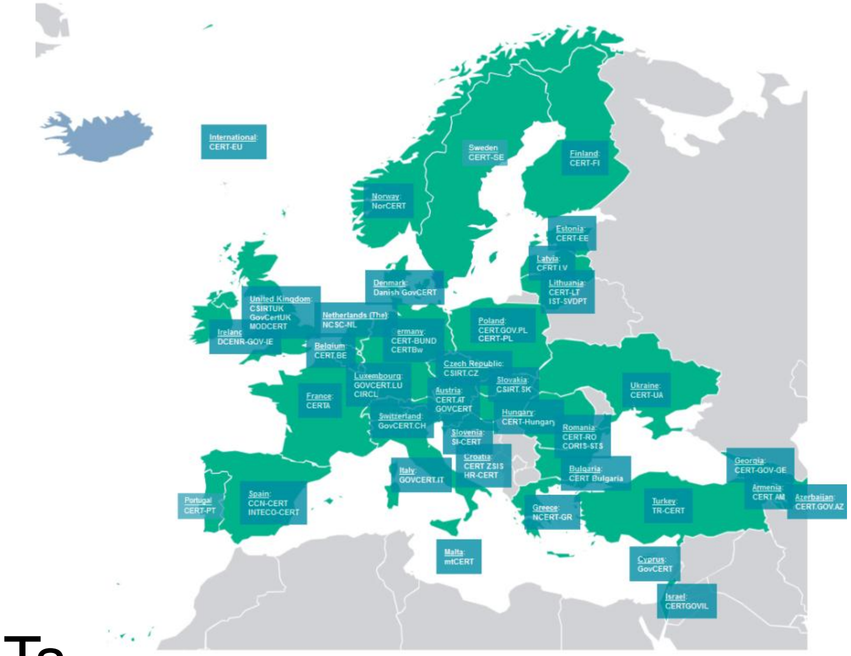
National/governmental CERTs
the situation has changed…

in 2005



in 2013

ESTABLISHED IN 2005:
Finland
France
Germany
Hungary
The Netherlands
Norway
Sweden
UK



CERTs in Europe interactive Map, 2012 v3.0 © European Network and Information Security Agency (ENISA)

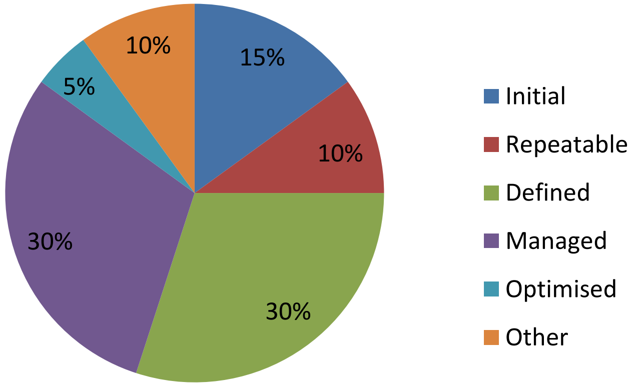
Baseline capabilities of n/g CERTs

- Initially defined in 2009 (operational aspects)
- In 2010 Policy recommendations drafted
- In 2012 ENISA continues to work on a harmonisation together with MS
- Status Report 2012
- National/governmental CERT capabilities – updated recommendations 2012

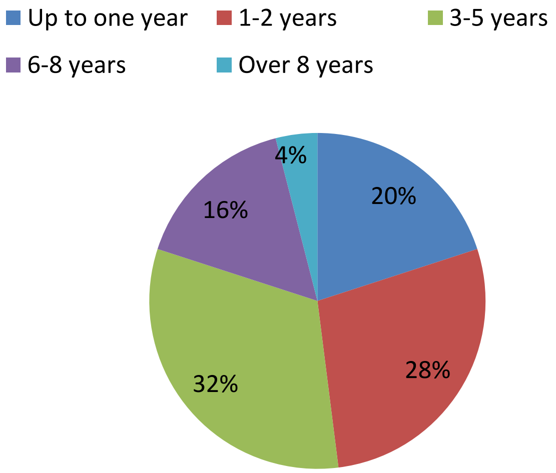
CERT Status Report 2012

Total: 45 responses to the questionnaire (25 from n/g CERTs; 20 from other CERTs and other stakeholders)

Self-Assessment of the Maturity Status of National / Governmental CERTs



Years of Operation of National / Governmental CERT

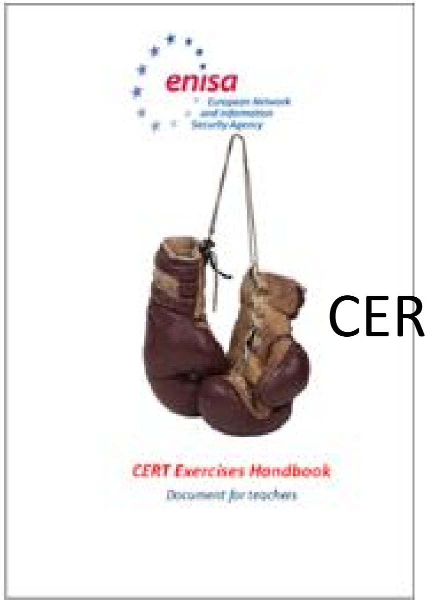


Interviewed teams assessed themselves as either governmental or national/governmental CERTs indicated the years of operations between: 4 months and 11 years.
(France, Germany, Norway, Hungary, Denmark, Sweden, Spain, Ireland, Latvia, Czech Republic, Slovakia, Romania, CERT-EU)

CERT Exercises and training material

- ENISA CERT training/exercise material, used since 2009, was extended to host 23 different topics and training exercises including:
  - Technical aspects
  - Organisational aspects
  - Operational aspects

- Additionally a Roadmap was created to answer the question ‘How could ENISA provide more proactive and efficient training?



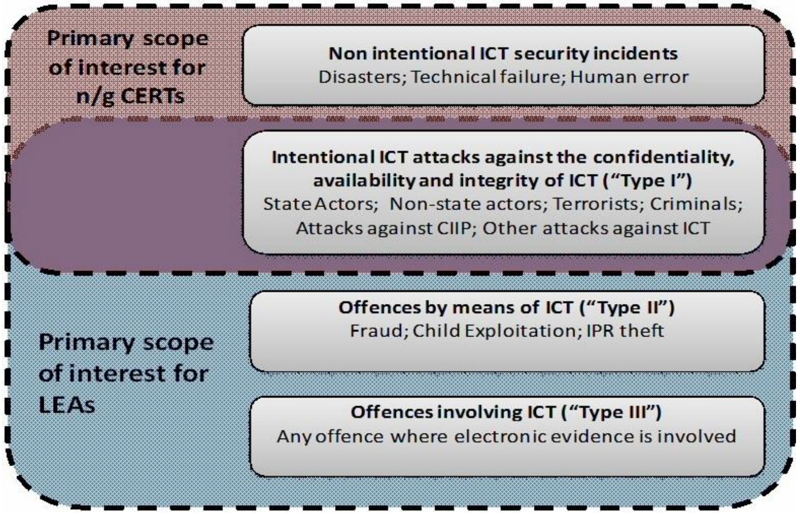
enisa
European Network and Information Security Agency

CERT Exercises Handbook
Document for teachers

CERT

Fostering CERT-LEA Collaboration

- Main goals:
  - Define key concepts
  - Describe the technical and legal/regulatory aspects of the fight against cybercrime
  - Compile an inventory of operational, legal/regulatory and procedural barriers and challenges and possible ways to overcome these challenges
  - Collect existing good and best practices
  - Develop recommendations
- Focus on CERT-LEA



Primary scope of interest for n/g CERTs

Non intentional ICT security incidents
Disasters; Technical failure; Human error

Intentional ICT attacks against the confidentiality, availability and integrity of ICT ("Type I")
State Actors; Non-state actors; Terrorists; Criminals; Attacks against CIIP; Other attacks against ICT

Primary scope of interest for LEAs

Offences by means of ICT ("Type II")
Fraud; Child Exploitation; IPR theft

Offences involving ICT ("Type III")
Any offence where electronic evidence is involved

Agenda

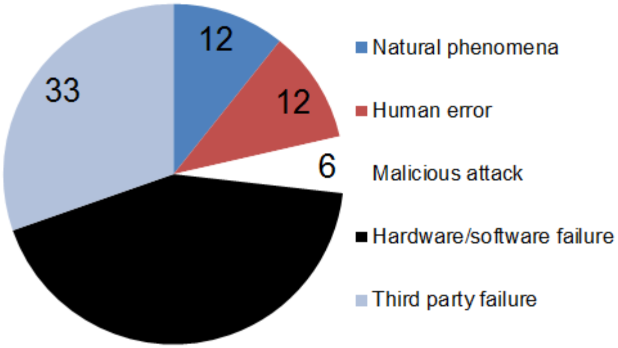
- About ENISA
- The EU Cyber Security Strategy
- Protecting Critical Information Infrastructure
- Input to EU & MS Cyber Security Strategies
- Assisting Operational Communities
- Security & Data Breach Notification
- Data Protection

Security & Data Breach Notification

- Supporting MS in implementing Article 13a of the Telecommunications Framework Directive
  - Supported NRA's in implementing the provisions under article 13a
  - Developed and implemented the process for collecting annual national reports of security breaches
  - Developed minimum security requirements and propose associated metrics and thresholds
- Supporting COM and MS in defining technical implementation measures for Article 4 of the ePrivacy Directive.
  - Recommendations for the implementation of Article 4.
  - Collaboration with Art.29 TS in producing a severity methodology for the assessment of breaches by DPAs

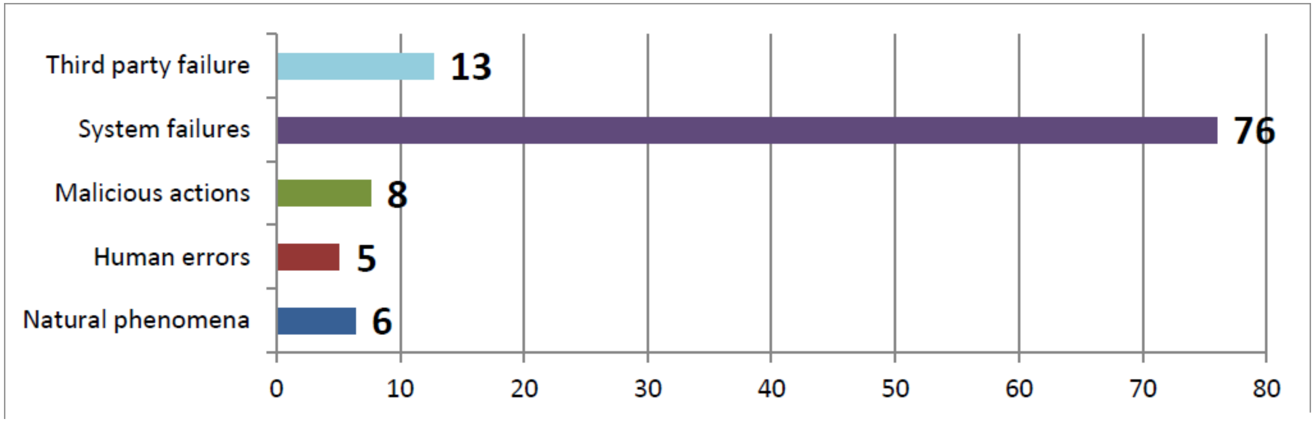
Article 13a - Incidents 2011

- 51 incidents from 11 countries, 9 countries without significant incidents, 9 countries with incomplete implementation
- Most incidents
  - Affect mobile comms (60%)
  - Are caused by
    - hardware/software failures (47%)
    - third party failures (33%),
    - natural disasters (12%)
  - Many involve power cuts (20%)
  - Natural disasters (storm, floods, et cetera)
    - often cause power cuts, which cause outages



Article 13a - Incidents 2012

- 79 incidents from 18 countries, 9 countries without significant incidents, 1 country with incomplete implementation
- Most incidents
  - Are caused by
    - System failures (76%) , third party failures (13%), Malicious actions (8%)
    - natural disasters (6%)



Questions?

Follow ENISA: