

Cybercrime reporting systems (CRS)

Why? (aims pursued)

Fundamental aims:

- **objective:** as part of an overall strategy in the fight against cybercrime, to contribute to a safe, open and stable information society
- **subjective:** by demonstrating that offline regulation also applies online, to address what is perceived as a continuously increase in cybercrime

Applied aims:

- **action:** to get a centralised reporting tool in order to improve the action of public authorities, especially law enforcement agencies (LEA)
- **prevention:** to raise awareness towards citizens and organisations and provide educational tools in order to improve prevention of cybercrime

What for? (benefits expected)

Core benefits:

- to collect of an **actionable intelligence** from victims and witnesses, which can be the basis for investigations and prosecutions (if possible in a centralised database), after a first analysis (or investigation if LEA-managed CRS) of relevance, scope and localisation
- to provide, as a single point of contact (PoC), a **passive coordination** between LEA (no duplicates, no feed back), by transfert of actionable reports to the relevant authorities according to a pre-established dispatching plan
- to produce **national statistics**, which enables to understand and measure trends, to identify new threats on citizens and organisations, to adapt law enforcement capacities (legal, organisation, training, equipment) and to better target the response
- to share information/advices with **domestic and foreign authorities**
- to establish a channel of communication with **citizens and organisations**, especially for creating awareness about threats and CRS itself
- to foster a culture of **public/private cooperation** (information sharing and pratical collaboration)

What for? (benefits expected)

Potential benefits:

- to organise a **mandatory reporting** for domestic Internet access/service providers
- to collect and process **complaints** from victims in a full dematerialized way
- to provide an **active coordination** (animation, feed back) between LEA
- to supply **black lists** of websites hosting illegal contents, which can be used by a blocking or dereferencing system
- to develop a **CSIRT/CERT** for citizens and non-sensitive organisations

Which one? (scope and model)

Cybercrime or cybersecurity?

- CRS or all-users CSIRT?
- step by step?

General or special?

- processing all threats or focussing on main ones?
- step by step?

Public or private?

- whose initiative, whose funding?
- partnership?

CRS or all-users CSIRT?

<i>Model</i>	<i>Advantages</i>	<i>Drawbacks</i>
Cybercrime reporting system (CRS)	technically easier perception of penal response	less direct response possible mistrust less efficient awareness
All-users computer security response team (CSIRT)	more direct response mutual trust/understanding more efficient awareness	technically more ambitious no perception of penal response

Processing all threats or focussing on main ones?

The features of cybercrime:

- **Definition:** any crime mainly committed against or through digital system
- **Characteristics:** versatile, international, dematerialized, growing, durable, unmeasured
- **Motivations:** money, ideology, sex, ego
- **Perpetrators:** swindler/trafficker, extremist/terrorist, abuser, hacker ...
- **Victims:** see table below

<i>Target</i>	National security	Industries/Business	Individuals
<i>Subject</i>	sensitive data	valuable data money/goods economical damage	identity/bank data money/goods psych./phys. damage
<i>Means</i>	hacking, attacks social engineering	hacking, attacks social engineering	spamming, phishing social engineering
<i>Reporting</i>	low impact confidentiality intelligence interest	real impact deep understanding mutual trust	high impact

Processing all threats or focussing on main ones?

The choice of a strategy:

<i>Model</i>	<i>Advantages</i>	<i>Drawbacks</i>
General	large scope processing: - intelligence and coordination - statistics and threat assessment	huge processing: - numerous staff - various skills
Special	more light processing easier partnerships more visibility/credibility	narrow scope processing but extensible

Whose initiative, whose funding?

<i>Initiative/Funding</i>	Public	Private
Public	established, run and funded by public sector with some level of cooperation with the private sector Example: Internet Signalement, France	established by private sector not sustainable without funding from the public sector Example: INHOPE, European Union
Private	established by private sector sustainable without funding from the public sector but requires input from it Example: Signal Spam, France	established by private sector with some level of cooperation with the public sector Example: Anti-Phishing Working Group, USA

Whose initiative, whose funding?

A public reporting mechanism: Internet Signalement, France:

- **law enforcement** initiative, initially against **child pornography** online (2000)
- **mandatory reporting** for access/service providers regarding certain contents (2004)
- single PoC (2005) extended to **all cybercrimes** with a brand new website (2009)
- 10 **LEA staff** (gendarmerie/police), numerous public-private **partnerships**
- a similar developement for e-Cops Belgium (from special to general threat)
- a different choice than Mauritian National CSIRT (CERT-MU)

A public-private reporting mechanism: INHOPE, European Union:

- EU-funded international **association of 49 Internet hotlines** (public, NGO, private) from 43 countries, against illegal contents, especially **child pornography** online
- hotlines accessing the reports from public according to their national legislation, tracing the apparent locations of contents, passing the report to either their national **LEA** for further investigation, **ISP** for take-down or **other INHOPE hotlines**, sharing of knowledge, information and best practices

Whose initiative, whose funding?

A private-public reporting mechanism: Signal Spam, France:

- **non-profit organisation** against spam, enabling reports of unsolicited/abusive emails
- members: **public authorities** (data protection, LEA), **email stakeholders** (e-marketing senders, email boxes providers, security vendors)
- a co-managed private-funded system, but **initially a public-private initiative** with public management/funding designed to support the French data protection authority
- **reports** collected and redistributed to the best positioned members for further action (including LEA investigations), **educational tools**, **data sharing** with relevant Internet actors, best practices empowering (mandatory code of ethics for members)

A private reporting mechanism: APWG, USA

- **worldwide coalition** of more than 2.000 institutions (industry, government, LEA), established as a clearinghouse for organisations victims of phishing attacks
- phishing websites reported for **blocking** to browser developers and antivirus companies; reports also used to understand **trends**, create **statistics**, enable **urgent notifications** to clean corrupted nodes and suspend criminal domain names
- **advises** international institutions (EU, CoE, OSCE, OAS, UN) or governance bodies (ICANN), national governments, global or regional companies

How? (launching and operating)

Dealing with requirements and costs

- Common requirements for all CRS
- Widely variable costs

Creating awareness

- During the launch phase
- Afterwards

Seeking assistance

- e.g. INHOPE Foundation

Dealing with requirements and costs

Common requirements to all CRS:

- **political/top management support:** to ensure the initiative is perceived as relevant and to secure the budget and staff required for its launch and operation
- **ICT project team** supported for designing by both digital investigators and Internet users
- **ICT infrastructure:** website or call centre
- **dedicated staff**, including some cybercrime specialists (analysts or investigators)
- standardized **cybercrime nomenclature**
- **support of LEA and the Judiciary** (mandatory for agreeing a nomenclature and handling reports/complaints)
- capacity to measure **return on investment** (especially private-funding CRS)

Dealing with requirements and costs

Costs widely varying on:

- the **scope** of the CRS (general/special)
- the method to collect the **reports** (manual/automated)
- the implementation and maintenance of a **database**
- how technically **LEA** are connected to the CRS to retrieve and process information
- the **partnerships** involved
- the size of the **population** of the country

Creating awareness

During the launch phase:

- awareness **campaign** (e.g. Internet Signalement, 2009) involving in particular national media (press articles, TV spots, posters ...)
- **SMS** campaigning
- **leaflets** attached to phone bills
- **social media** campaigning

Afterwards:

- **referencing** on Internet service providers, e-commerce or other websites homepages (e.g. Internet Signalement, e-Cops)
- regular publications of **reports** (e.g. Internet Signalement)
- communication through **social media**
- regular articles in the **press**
- periodic public service **announcements**
- attendance of national and international **conferences and meetings** on cybercrime

Seeking assistance (e.g. INHOPE Foundation)

INHOPE Foundation supports **start-up activities of new hotlines outside EU**, mainly in countries where:

- **child pornography** is facilitated/produced/distributed
- there is an **identified need but limited funding, awareness or support for a CRS** to identify, report, remove and/or investigate child pornography

INHOPE Foundation identifies and enters into **partnerships** with national organisations (mainly NGO, private companies) meeting the Foundation's **criteria** and can provide:

- initial start-up **support and training on best practices** to the staff
- a **guided oversight** during the initial start-up phase, including instruction on best practices for staffing requirements, equipment needs, location security, data safeguarding, and internal and external policy development
- a **limited financial support** (no response to requests for funding)

2014-2015: focus on Latin America, South East Asia and Africa

So? (recommendations/conclusions)

Recommendations:

- to prefer a CRS than a CSIRT initially, a **CRS empowering an enforcement action and enabling a continuous improvement of the criminal justice**
- to involve government, LEA & Justice (for further investigation/prosecution), Internet industry (for further removal/blocking), NGO (e.g. child protection) and to seek **partnerships public/private, assistance from international CSR** (e.g. INHOPE)
- to focus initially on the **main threats and later on expand** to all threats
- to choose the **right interface**, with regard to national organisation, budget or skills availability
- to begin with a **small staff and budget and later on expand** the capacity, especially through partnerships
- to define **how the information collected will be distributed among agencies and authorities**, without duplication of efforts

So? (recommandations/conclusions)

Conclusions:

- **step by step !**
- **according to the country specificities and needs (no worldwide model)!**