Cybercrime reporting mechanisms – Good practice study

Agenda : Introduction to the draft study

Activity under Result 6 of GLACY : ***"Information sharing: increased public/private and interagency information sharing in line with data protection standards"***

Consultants :

- Jean-Christophe Le Toquin, cybercrime and information governance
- Fabrice Bulian, cybersecurity and fraud
- Maelle LeLardic, internet policy

Timeframe : completion in June 2014

Expected results

- **Strengthen country capacity to measure threats, understand trends and build a response :**

  - Provide the necessary information to up to 10 countries to set up public cybercrime reporting mechanisms

  - Make available information sharing policies and data protection requirements for setting up online reporting mechanisms

  - Law enforcement/ISP cooperation agreements adopted in up to 10 countries

Approach

- **Who can benefit from this study?**

  - Any country not equipped with cybercrime reporting mechanism,
  - which are looking at ways to get started

- **3 elements to be considered :**

  - Impact : on individuals, industry, national security
  - Initiative : public and/or private
  - Funding : public and/or private

Expected benefits

- **At strategic level :**

  - get a **centralised** reporting tool, and **coordinate** actions across law enforcement agencies or public authorities in a given country,

  - demonstrate that regulation which applies offline also applies online,

  - raise **awareness** towards consumer and businesses and provide educational tools,

  - Develop **public/private cooperation**

Expected benefits

- **At operational level :**

- **Measure** cybercrime at country level and develop enforcement capacity,

- produce **statistics** on trends and threats,

- develop **intelligence** from these statistics and better target law enforcement actions,

- share **expertise** with other national or international law enforcement authorities through publications, reports, symposiums…

1st impact of cybercrime : on individuals

- **Threats**
  - Identity theft, personal data theft, e-reputation, sexual abuse online, incitement to racial hatred…

- **Pros and cons of a cybercrime reporting mechanisms**
  - Potentially large volume of reports to be expected
  - Requires large scale awareness campaigns
  - Enforcement response is challenging

2nd impact of cybercrime : on industry

- **Threats**
  - Loss of confidential or protected information, reputational damages, intellectual property infringements, direct or indirect financial losses, denial of service…

- **Pros and cons of a cybercrime reporting mechanisms**
  - Smaller volume of reports to be expected
  - Requires developing public/private trust
  - Enforcement response requires deeper technical expertise

3rd impact of cybercrime : on national infrastructure

- **Threats**
  - Government, law enforcement agencies, public authorities, critical infrastructure can be the target of politically motivated offenders seeking to cause disruption

- **Pros and cons of cybercrime reporting mechanisms**
  - Not an adequate response…
  - But cybercrime reporting mechanisms may provide useful information on threats against national infrastructure

4 governance models identified

- **Public :** established, run and funded by public sector, with some level of cooperation with the private sector
- **Public/private :** established by the private sector, not sustainable without funding from public sector
- **Private/public :** established by the private sector, sustainable without funding from public sector, but requires input from the public sector
- **Private :** established by the private sector with some level of cooperation with the public sector.

11 reporting mechanisms surveyed

Public	• Action Fraud, UK • Consumer Sentinel Network (CSN), USA • e-Cops, Belgium • European Cybercrime Center (EC3), EU • Internet Signalement, France
Public/Private	• National Cybersecurity Center (NCSC), Netherlands • Internet Crime Complaint Centre (IC3), USA • INHOPE, EU • BotFrei, Germany
Private/Public	• Signal Spam, France
Private	• Anti-Phishing Working Group, USA

A variety of operational models

Country	Population	Scope	Public	Public-Private	Private-public
U.K.	63 millions	Fraud	**Action Fraud**: 229,018 frauds from March 2012 to March 2013		
Belgium	11 millions	Cybercrime	**e-Cops** : 24,220 complaints received in 2011		
France	66 millions	Pharos: cybercrime Signal Spam : spam	**Pharos** : 123,987 complaints received in 2013		**Signal Spam**: 2,454,369 complaints received in 2012
U.S.A.	314 millions	FTC: fraud IC3 US: cybercrime	**Consumer Sentinel Network**: 2,101,780 complaints received in 2013	**IC3**: 303,809 complaints received in 2010	

Budget & staff requirements

- **Budget requirement:**
  - Information challenging to obtain
  - U.S. Federal Trade Commission's Consumer Sentinel requires an entire building and purchase all the IT equipment for several millions $.
  - Private sector initiatives annual budget :
    - Signal Spam : € 200.000
    - APWG : € 400.000

- **Dedicated staff requirement**
  - From 2 to more than 30 persons
  - Larger initiatives (FTC, IC3 US, Action Fraud UK, Pharos France) require an initial staff of minimum 10 members

Recommendations for public reporting mechanisms

- **Political/top management support**

- **Experienced personnel:**
  - ICT project manager to set up the ICT environment,
  - Police manager that liaise with senior management in order to solve any occurring problems during the establishment and the operational phase of the reporting mechanisms,
  - Digital investigators to help define the working structure of the reporting mechanism,
  - Digital investigators to handle complaints assisted by administrative employees that can do a first selection of the complaints,
  - Involvement of the judiciary

Recommendations for private reporting mechanisms

- **Measuring return on investment is critical**
  - "Monetising" data reported to private-public and private reporting mechanisms is not only an operational necessity, it helps define a good governance of the organisation

- **Involvement of public authorities has many benefits :**
  - Contributes to public trust
  - Learning exercise for both public and private parties, based on operational data

Conclusions

Questions ?

Jean-Christophe Le Toquin
jcletoquin@socogi.fr