Data Collection of Security Incidents and Consumer Confidence

- Is a partnership feasible? -

Carsten Casper
Senior Expert at ENISA

FIRST Conference, Sevilla 2007

Request to ENISA

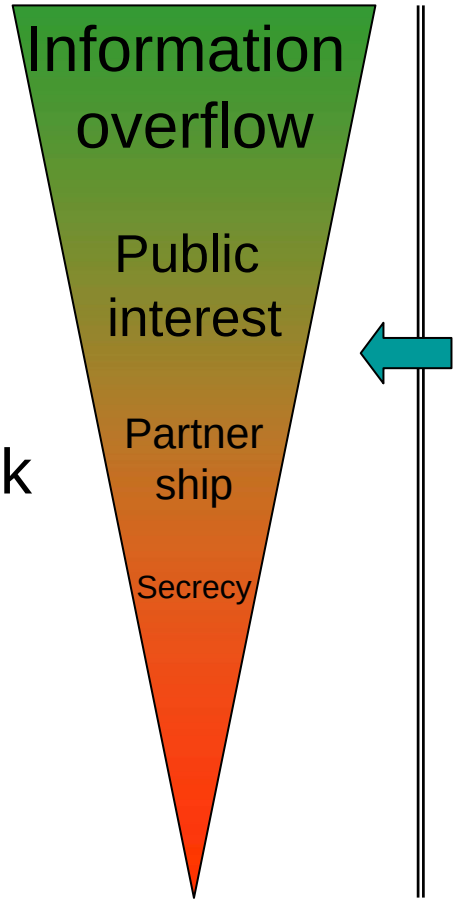
COM(2006) 251

"Develop a trusted partnership with Member States and stakeholders to develop an appropriate data collection framework, including the procedures and mechanisms to collect and analyse EU-wide data on security incidents and consumer confidence"

- Based on the Communication "A strategy for a Secure Information Society – Dialogue, partnership and empowerment"
- Request from the EU Commission in Oct 2006
- „Data Collection on volumes and trends of security incidents and consumer confidence"
- Or: „Better data – better decisions"

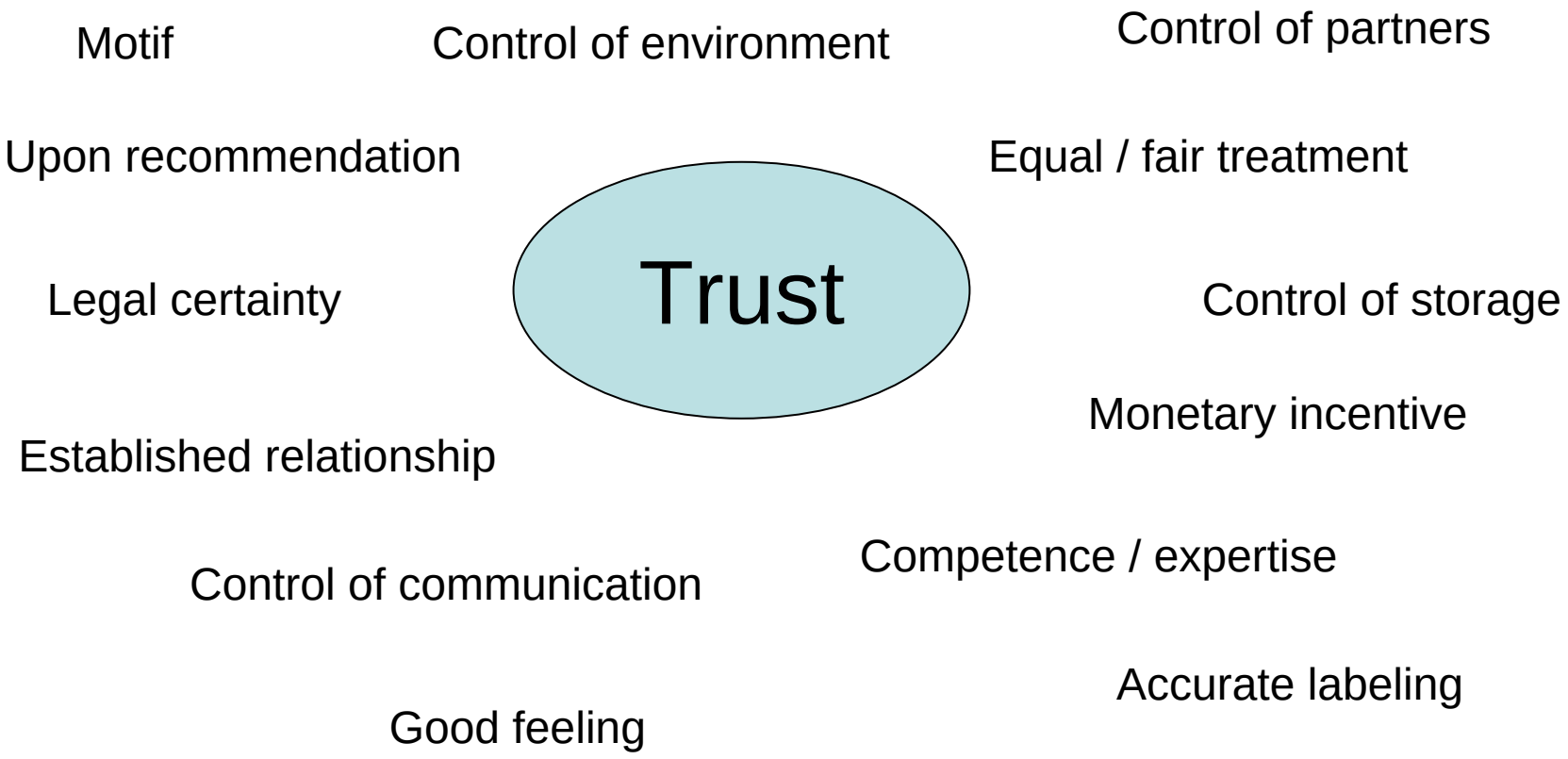
What data *could* we share?

- Share even with those who do not want to know
- Share with interested parties
- Share within an established framework with clear rules
- Share only with very few, well-known, trusted actors on a case-by-case basis



- Marketing
- Surveys
- Industry collaborations
- Within organisations

Conditions for sharing data

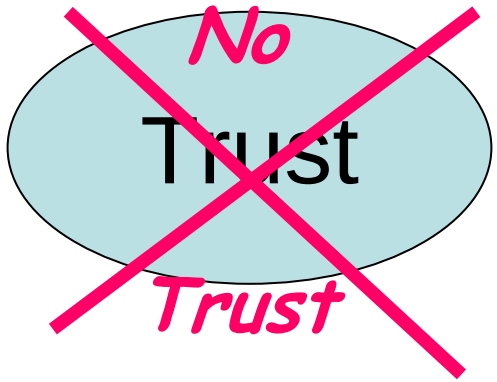


Conditions for not sharing data

Motif for abuse

Any suspicions

Violation of law



Violation of corporate rules

Absence of incentives

Unclear or inconsistent partners

No time for evaluation

Trust not transitive

Lack of budget

Benefits < risks

Sensitive data not separable

Timing of sharing too difficult

Motivations for partnership

- Governments need reliable and up-to-date statistical and economic data for effective policy making
- Progress of policies and their enforcement can be measured over time
- Not about benchmarking of different countries
- Link data from different countries to get a bigger picture
- Private organizations could tune their technical countermeasures
- Competitors receive guaranteed benefits (information) without risks (loss of information)
- Industry benefits from sector-specific benchmarking
- Specialized observers harmonize their approaches with others

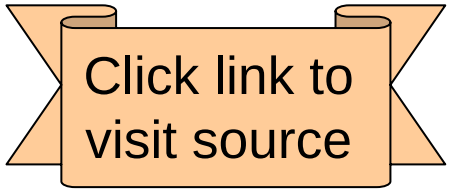
It takes time to create trust between partners. Once achieved, an established partnership can bring benefits continously.

ENISA Questionnaire
- General Comments -

- ENISA should look at all potential international partners, not only on those who cover only European citizens
- ENISA should focus on “security incidents”, less on “consumer confidence”
- Presented list of data sources is comprehensive

Regular Reports

- Arbor Worldwide Infrastructure Report
- CSI/FBI Computer Crime and Security Survey
- CSO Online E-Crime Watch
- DTI/PwC Information Security Breaches Survey
- E&Y Global Information Security Survey
- European Information Technology Observatory
- Facetime Annual Impact Report
- FH Gelsenkirchen - Email Reliability (in German)
- Internet Crime Complaint Center Annual Reports
- kes Sicherheitsstudie (in German)
- MAAWG Email Metrics Report
- Message Labs Intelligence Reports
- Postini Message Management & Threat Report
- Sophos Security Threats Report
- Symantec Internet Threat Report



One-time Reports

- AOL/NCSA Online Safety Study
- APWG Phishing Activity Trends Report
- ARECI - Availability and Robustness of Electronic Communication Infrastructures – Report 2007
- Benchmark Study of European and U.S. Corporate Privacy Practices
- White & Case - Benchmarking Security and Trust in the Information Society in Europe & the US
- Privacy Rights - Chronology of Data Breaches 2006
- ETH Zürich - Information Security in Swiss Companies
- McAfee - Mapping the Mal Web
- Microsoft - Security Intelligence Report
- PITAC – Report Cyber Security: A Crisis of Prioritization
- Internet Defence - The Phishery
- Kapersky: Internal IT Threats in Europe 2006
- E-Communications Household Survey
- Central and Eastern Europe Information Society Benchmarks 2004
- The IT Security Situation in Germany in 2005
- (N)Onliner-Atlas 2006 (in German)

Other Reports

- Reports without statistical data
  - Federal Plan for Cyber Security and Information Assurance Research and Development
  - MELANI – Semi-Annual Reports
  - Emerging Risks-related information collection and dissemination: A study for ENISA
- Statistical data without report
  - CAIDA - Cooperative Association for Internet Data Analysis
  - ITU Survey on Trust and Cybersecurity 2006
  - Secunia Advisory Statistics

Potential Partners

- Managed Security Service Providers (MSSP)
- Computer Emergency Response Teams (CERT)
- National security organisations
- National / EU statistics offices
- IT security vendors
- Electronic communication service providers (e.g. ISPs, telcos)
- Universities
- National Research Networks
- Insurance Companies
- Enterprises (i.e. users of statistics)

Potential Partners

Alcatel-Lucent APWG British Telecom (BT) Cybertrust Datamonitor Deutsche Telekom (DT) eco/SpotSpam ECSC EITO CERT Network Ernst & Young ETH Zurich (CSS) ETNO ETIS EuroISPA European Commission Eurostat Ferris Research FH Gelsenkirchen (Ifis) FIRST Forrester FORTH France Telecom (FT) Frost & Sullivan F-Secure Gartner Global Information Inc. IBM/ISS IDC Infonetics In-Stat ISF KES JRC IPSC Leurrecom LOBSTER MAAWG McAfee Message Labs MITRE (CVE/CME) MOME NISCC/CPNI NoAH OECD Panda Soft Radicati Royal Holloway (ISG) SignalSpam Sophos Spamhaus SpotSpam Symantec Telecom Italia Terena The Honeynet Project University of London Viruslist.com White & Case

Ways of collaboration

- Face-to-face meetings at workshops or a conference are crucial to create trust
- Joint editing and storage are also important
- Mailing list can be open or closed, depending on topics
- Hardly anybody wants phone or video conferences

- Workshop(s) with contributions from various partners
- Face-to-face meeting(s) with ENISA to discuss this topic in private
- Open mailing list (i.e. every interested party can join)
- Closed mailing list (i.e. existing members can veto the entrance of new members)
- Regular phone conferences
- Wiki to jointly draft documents
- CIRCA (EU online collaboration portal) to store information
- Video conferences
- European-wide, multi-day conference

“Initially time efforts in participation will probably be a critical success factor – there should be calculable time frames for fostering that framework project, which is not the case for "ongoing efforts" as in mailing lists or wikis – on the other hand, once established – those means are probably necessary to keep things evolving...”

Possible motivations

- Everything can be a motivation
- Everything can be a „non-motivation“
- The more motivations, the better
- Access to raw data is slightly less in demand

- Earn money
- Gain competitive advantage
- Lobby political decision makers
- Get easy access to aggregated data from others
- Get access to raw data from others
- Achieve better publicity for related own projects
- Benchmark success of security controls
- Improve own statistics

Possible contributions

- Reports
- Raw data
- Aggregated data
- Anonymized data
- Standardisation/ harmonization expertise
- Leadership, Management
- Endorsement (i.e. marketing, branding)
- Sponsorship (i.e. money, long-term funding)
- Administration (e.g. event logistics)
- IT resources (e.g. hosting, hardware, software)

- People expect more than they are willing to contribute
- Earning money is a motivation, but sponsorship is never an option
- Reports and aggregated data are shared more easily
- Little interest in sharing raw data

Ideas for sharing

• Volume of threats per quarter, per year • Volume of threats per megabyte of traffic, per session • Percentage of malicious content versus whole valuable payload
• Viruses, worms, DoS etc. or other destructive payload as defined collectively • Breaches, incidents or reconnaissance activity • Spam, spim, spit, and other nuisances • Installed bot-nets, rootkits, trojans, spyware
• Geographic and industry sector distribution
• Cases of online vandalism • Cases of identity fraud and identity theft (including phishing and pharming)
• Business transactions processed or failed • Purchases completed or cancelled • Size of the ICT security product, services and hosting market • User perception
• Countermeasures
• Network packet traces which contain attacks

Ideas for alignment

- Definition of countries
- Country codes (e.g. TLDs)
- Study time frame (e.g. cover at least quarters, published not later than 3 months later)
- Definition of company sizes (especially for SMEs)
- Minimum statistical sample
- Publication rights (e.g. at least available after free registration)
- Definition of well-known threats (e.g. spam, virus)
- Country where to count a threat (e.g. legal location of attacker, location of launching computer, location of victim)
- Definition of severity levels

Possible Scenarios

1. Pooling of reports
2. Commenting / Meta search
3. Common understanding
4. Cross references and synergy
5. Exchange of non-published data
6. Exchange of anonymized data
7. Exchange of raw data

Scenario 1
Pooling of reports

- All reports on security incidents and consumer confidence in Europe are available from a central location.
- They are presented with a standard description of their scope (e.g. timeframe, geography, topics)

Scenario 2
Commenting / Meta search

- All reports are tagged consistently …
- … and readers can search across a (sub)-set of reports for specific information (e.g. a country, the time of an outbreak).

Scenario 3
Common understanding

- Reports that follow an agreed
  - terminology,
  - data format
  - or structure
- … present a specific seal, e.g. “Registered European Information Security Report”

Scenario 4
Cross references and synergy

- Reports within this framework refer to other published reports.
- A yearly summary report summarizes all contributed reports during the last year,
  - e.g. as a condensed information for decision makers.

Scenario 5
Exchange of non-public data

- Partners exchange data that is not meant to be published, but of value for similar initiatives,
  - e.g. draft reports,
  - details behind published data,
  - methods of data collection.

Scenario 6
Exchange of anonymized data

- Partners exchange data which has been
  - anonymized or
  - psydonomized
- in order to protect the identity of the data source

Scenario 7
Exchange of raw data

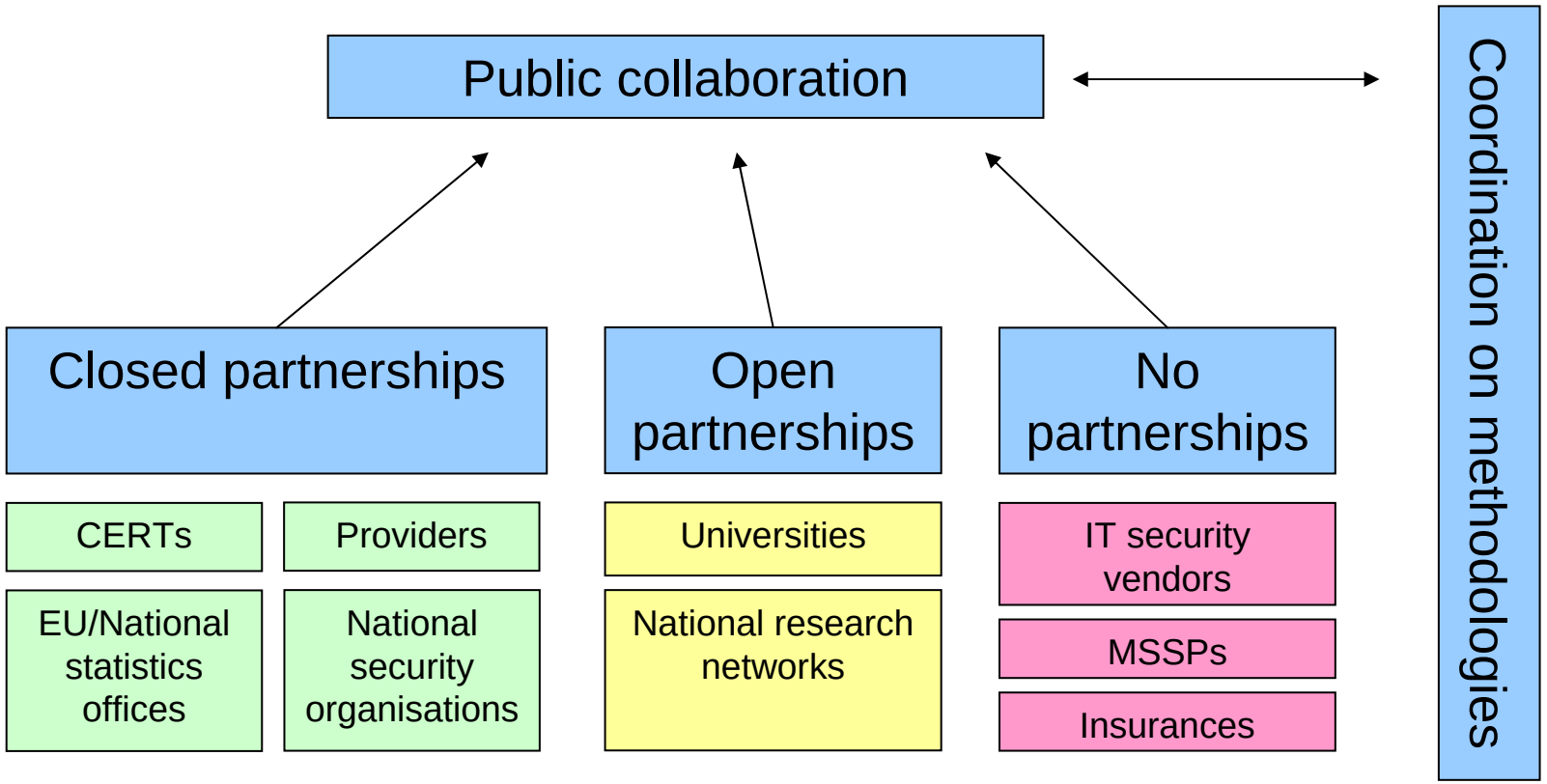
- Partners make detailed data directly available to other partners.

- Of course this requires strong security measures and a deep trust relationship between named partners.

Scenarios – realistic?

- Probably most potential partners would not mind
  - pooling data,
  - developing a common understanding and
  - maybe even accept comments / meta search
- Vendors and providers are seen as least likely to share data
- Sharing not-published data is a problem for most potential partners

Layered partnership(s)



Vision for Data Sharing

1. All actors must have compatible motives
2. It takes time
3. It depends on individuals
4. It must have a clearly described scope
5. It will happen in phases
6. It will happen on different levels
7. It needs a supporting framework

Contact Details

Questionnaire still available at
http://www.enisa.europa.eu/pages/data_collection

ENISA (European Network and Information Security Agency)
Carsten CASPER
Senior Expert - Information Security Policies, Tools & Architectures
Technical Department
+30.2810.39.1280
carsten.casper@enisa.europa.eu