What the Agency wants to get across

Some main issues and what does ENISA do about them?

How does ENISA collaborate with stakeholders?

How useful is ENISA’s work?

What’s next?
How big is the problem?
Security incidents are hard to quantify

- Reluctance to report (brand image)
- Difficult to report incidents
- Statistics don’t add up (different types of incidents/areas)
- Reports made by organisations with possible bias
How feasible is EU-wide data collection?

Feasibility study (COM request 2007) aiming to create EU-wide partnership for establishing a data collection framework

One partnership for data collection (“one-size-fits-all”) is not feasible

It will be necessary to create new (or promote existing) partnerships of different kinds and on different levels

An additional co-ordinating partnership could tie together specific existing or new partnerships
Please be advised ...

We have to accept living with uncertainty about the size of the problem, but should be aware of the nature of risks and vulnerabilities and trends thereof.
ENISA helps providing better insight

Three-year programme to create trust and confidence with decision makers through better insight in emerging risks

By 2010, at least 30 stakeholder (organisations) from at least 15 Member States refer to ENISA as point of reference

TOPICS
• Online Social Networking
• Botnets
• Web2.0
Massive Cyber attacks

What is it?
Overwhelming of networks, systems and/or services

How is it done?
DDoS, targeted attacks, etc.
Attacking much cheaper than mitigation

Why is it done?
Economical gain, extortion political motives

What is the impact?
Disruption of daily business and peoples daily lives
Massive attacks cannot be prevented

Source: Elion AS (Largest Estonian ISP)
ENISA helps counter massive Cyber attacks
Improving eResilience

Three-year programme to collectively evaluate and improve resilience of Europe’s public e-Communication networks and services

Stock taking
- Regulation
- Market/operators
- Technology

Gap analysis

Develop
- Best practices
- Guidelines

Promote
- Best practices
- Recommendations

2008 2009 2010

By 2010, the Commission and > 50% of the Member States have made use of ENISA recommendations in their policy making process
Challenges in improving eResilience

Complex regulatory frameworks
Overlapping/conflicting regulations and measures in MS

Lack of transparency (of Internet)
Who is responsible for what?

Difference in sectors
Diversity of requirements
Variety of expectations

Emerging topic
Only a few pan-European specialised professional bodies
Existing stakeholder groups just started developing capabilities
Standards and technologies in progress
ENISA helps counter massive Cyber attacks
CERTs as “digital fire squads”
How ENISA supports the CERT community
Promote best practice

2005: Stocktaking

2006: Setting up & Cooperation

2007: Support operation Quality assurance

2008: Good practice on CERT exercises

2009: Pilot good practice on CERT exercises

[...]
About online Social Networking
Tools for organising my personal data
About online Social Networking
Access control to personal data based on credentials
About online Social Networking
Tools for managing access control based on credentials

Privacy

Profile
Control who can see your profile and personal information.

Search
Control who can search for you, and how you can be contacted.

News Feed and Mini-feed
Control what stories about you get published to your profile and to your friends’ News Feeds.

Applications
Control what information is available to applications you use on Facebook.

Block People
If you block someone, they will not be able to search for you, see your profile, or contact you on Facebook. Any ties you currently have with a person you block will be broken (friendship connections, relationships, etc.).
About online Social Networking
Tools for finding out who has accessed personal data
Privacy issues with online Social Networking
Access control based on credentials?

Account & Settings

Account Options

<table>
<thead>
<tr>
<th>Select an Account Type:</th>
<th>Pro</th>
<th>Recruiting • HR Research • Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost per month</td>
<td>$200 per month</td>
<td>The only thing more powerful than your network is a well coordinated team connecting multiple networks.</td>
</tr>
<tr>
<td>Receive Requests for Introductions</td>
<td>40 at a time</td>
<td>Learn more...</td>
</tr>
<tr>
<td>Send InMails™</td>
<td>50 per month</td>
<td></td>
</tr>
<tr>
<td>Network results</td>
<td>200 per search</td>
<td></td>
</tr>
</tbody>
</table>

“It's ok because only my friends can see my profile data”
Privacy issues with online Social Networking
Inappropriate (and often irreversible) disclosure

“Digital cocktail party: digital hangover?”

People are not aware of their audience
Privacy issues with online Social Networking

Inappropriate (and often irreversible) disclosure
Privacy issues with online Social Networking
Low friending threshold (poor authentication)

Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves

Research highlights dangers of irresponsible behavior on social networking sites

Sophos, a world leader in IT security and control, is warning social networking users of the dangers of allowing strangers to gain access to their online profiles, following new research into the risks of identity theft occurring through global phenomenon Facebook.

Compiled from a random snapshot of Facebook users, Sophos' research shows that 41% of users, more than two in five, will divulge personal information — such as email address, date of birth and phone number — to a complete stranger, greatly increasing their susceptibility to ID theft.

To coincide with the research, Sophos has also published a best practice user guide for behaving securely on Facebook, which reportedly signs up 100,000 new users every day.

The Sophos Facebook ID Probe involved creating a fabricated Facebook profile before sending out friend requests to individuals chosen at random from across the globe. To conduct the experiment, Sophos set up a profile page for Fredal Shair (an anagram of "ID thief"), a slim green plastic frog who divulged minimal personal information about himself. Sophos then sent out 200 friend requests to observe how many people would respond, and how much personal information could be gleaned from the respondents.

"Freddal may look like a happy green frog that just wants to be friendly, but actually he's happy because he's just encouraged 82 users to hand over their personal details on a plate," said Graham Cluley, senior technology consultant at Sophos. "While accepting friend requests is unlikely to result directly in theft, it is an embarr[ing] gating od[er]nals [that] the building blocks they need to spoof identities, to gain access to online user accounts, or potentially to deflate their employees' computer networks."

**Sophos Facebook ID Probe findings:**
- 87 of the 200 Facebook users contacted responded to Fredal, with 82 leaking personal information (41% of those approached)
- 72% of respondents divulged one or more email address
- 94% of respondents listed their full date of birth
- 87% of respondents provided details about their education or workplace
- 70% of respondents listed their current address or location
- 23% of respondents listed their current phone numbers
- 26% of respondents provided their instant messaging screenname
- 12% of respondents included a photo of family and friends

41% of people agreed to become Facebook friends with Fredal Shair, leaking personal details
Privacy issues with online Social Networking

Data mining tools

MyFaceID automatically processes your photos, find all faces, help you tag them and let you search for similar people.
Privacy issues with online Social Networking
Data mining tools

Which fortunately doesn’t always work that well
Locked-in by Social Networking sites
The hotel California effect

“Social Networking is like the Hotel California. You can check out, but you can never leave.”

Nipon Das to the New York Times

Root cause: value of the network (e.g., $15 billion and counting) due to its personal data, ability to profile people for advertising and ability to spread information virally
ENISA helps counter online Social Networking risks
By developing position paper and reach out

ENISA’s position
Consider online Social Networking as eIdentity Management system
SN sites should provide privacy and anonymity tools and sophisticated reputation systems – use the social network to authenticate people

Make social networks portable (checking out of the Hotel California with secure briefcase and going to another one) enabled by portable access control and security

Education on the risks. In-context videos and quizzes.

Media impact after publication
Der Spiegel, Le Monde, Harald Tribune, Computer Weekly, ...

Paper promoted for EP LIBE Committee (February 2008)
Public hearing on "Data Protection and Search Engines on Internet"
Study on economics of NIS: Analysis of barriers and incentives for NIS in Internal Market for e-Communication

Identify existing barriers
Assess impact of barriers in Internal Market
Identify and analyse incentives
Provide recommendations

Request for comments on report open until end of May
Some recommendations open for comments

Responsible disclosure and fast patching

Should the EU adopt a combination of early responsible vulnerability disclosure and vendor liability for not providing software patches timely?

Would responsible vulnerability disclosure be more efficient in the long run as it creates a constructive relationship among stakeholders?
Some recommendations open for comments
Secure by default

Should the EU re-allocate slices of liability in response to specific market failures?

Should the EU develop and enforce standards for network-connected equipment to be secure by default?

Should vendors be required to (self-)certify that their products are secure by default?
Some recommendations open for comments
Security breach notification

Does the EU need a comprehensive security-breach notification law?

Are there lessons to be learned from experiences in some US states?
Imbalance in Member States’ capabilities
Some more “equipped” than others?

Limited number of MS already work together to exchange experiences in order to develop their NIS capabilities

All MS should support each other by sharing information and lessons learned on good practices on a structural basis
ENISA acts as broker between MS

The ENISA team at your service

The PSG members are willing to share

Member States working together

Online Platform as supporting tool
ENISA Brokerage in action

Some cases

Hungary supporting Bulgaria in setting up governmental CERT

Finland willing to support Slovenia in organising awareness raising activities

Netherlands and Hungary envisage cooperation in structured cyber crime-related information exchange, to be expanded to other countries
How to address SMEs?
Small firms as real giants of EU economy

99% of businesses in the European Union are SMEs and they provide two-thirds of all private sector jobs

Many SMEs aware of security problems but do not know how to solve them have lack of resources to invest

SMEs should actively be offered ready-to-use tools and solutions

An EU-wide network to deliver such tools and solutions should be (further) developed

Source: European Commission
ENISA helping to address SMEs

Preparatory Action to investigate the feasibility for developing an MTP on micro enterprises

Ad-hoc Working Group

Pilots
ENISA helping to address SMEs
Is an EU-wide info sharing & alert system (EISAS) feasible?

Feasibility study (COM request 2007)
Focussed on home users and SMEs

Most feasible scenario builds on existing national ISASs

EU as facilitator of good practice for national ISASs (no operational role for EU)
Clearing house for new ISAS
Support new ISAS
Facilitate dialogue between existing ISAS
Analyse and review methods of ISAS

Follow-up by DG JLS
Call for proposals April 2008
How does ENISA engage stakeholders?
Bringing them together: “NIS is people”

ENISA Bodies
Management Board
Permanent Stakeholders’ Group
National Liaison Officers network

Expert groups
Ad-hoc Working Groups
Virtual Expert Groups
Consultation workshops

EU Institutions
European Parliament, Council, COM

Multiplier organisations
Road show to industry, users/consumers

Communication and outreach
Website
ENISA Quarterly Magazine
Conferences and Joint Events
Dissemination workshops
How useful is ENISA’s work?
Study on the practical use of deliverables

Eager beaver ...?

... scope for improvement?
ENISA’s work is of high quality
Outreach has not reached its full potential

- Awareness:
  - 50% people unaware
  - 50% people aware
    - 28% of people have read

- Attitude:
  - 7 out of 10 marking for attitude
  - 87% of people see support or strong support of objectives

- Acceptance:
  - ‘remainder’
    - 69% of people already took action or Intend to

- Action:
  - 18% action

Awareness Attitude Acceptance Action
What’s next?