ecrime
The Economic Impacts of Cyber Crime

Industry interviews

Rain Ottis
Tallinn University of Technology

SEVENTH FRAMEWORK PROGRAMME

Background

ecrime
The Economic Impacts of Cyber Crime

- Part of WP4 – Framework for Economic Impact and Analysis
- Conducted by: TRI, GCSEC, TUD, WARWICK, TUT and UIBK
- The countries covered by industry interviews were Estonia, Germany, Italy, the Netherlands, the UK, and Poland
- 37 interviews conducted in total
- Timeframe: July 2015 to October 2015

Background

- Mostly in-person, some by telephone or e-mail
- Interview guide
- Semi-structured interview summaries
- Analysis by TUT – sectorial analysis, + insights from LEAs and DPAs
- Answers anonymised
- Interviewees:
  - Primarily from E-CRIME stakeholder foorum, some additional contacts
  - Respondents covered all non-ICT sectors as ID-d for the E-CRIME project (energy, financial services, health, retail, and transport)
  - Respondents also from LEAs and DPAs

Overview of interview spread

ecrime
The Economic Impacts of Cyber Crime

Country	Financial services	Retail	Trans-port	Energy	Health-care	Interviews per country	Other interviews
DE	1		1		1	3	1
NL	1			2	1	4	0
UK	2	2	2	1	2	9	5
PL	1					1	1
SI						0	1
LT						0	1
IT	1	1	1	1		4	1
EE	1	1	1	1	1	5	1
Total	7	4	5	5	5	26	11

General comments – healthcare

- **Healthcare** sector is mostly worried about data protection issues (privacy, data integrity), but differences emerge in the attitude towards digitized healthcare solutions
- General IT security vs protecting patient data
- Need more collaboration and information sharing in the sector
- Smaller actors may need government support

General comments – energy

- **Energy** sector is mostly worried about disruption of operations
- No significant cyber attacks reported by interviewees
- Human factor seen as weakest link in security
- Respondents use international standards and best practices
- Differing national regulations hinder standardizing the security controls and policies across companies that operate in multiple jurisdictions

General comments – financial

ecrime
The Economic Impacts of Cyber Crime

- **Financial** sector is mostly worried about cyber crimes that go after the assets of customers or companies
- More apt to report cyber crimes, better cooperation with LEAs
- International standards implemented
- Human factor seen as the bigger threat (compared to technology)
- Attackers after financial gain
- Need for citizen awareness programs
- International cooperation of LEAs needs to be improved
- Need scalable monitoring and threat intelligence
- More government focus on un-targeted low value crimes needed

General comments – retail

- **Retail** sector is mostly worried about online fraud
- More security awareness needed at management level (especially smaller companies)
- Centralized reporting and sharing of cyber incident data needed
- Insurance sector still emerging, different focus depending on country

General comments – transport

- **Transport** sector is mostly worried about service interruption and data theft
- Information sharing is weak
- Cloud services
- User friendliness vs security

General comments – LEA&DPA

ecrime
The Economic Impacts of Cyber Crime

- Deceptive financially oriented crimes are most prevalent
  - Phishing, ransomware, etc.
- LEA focus is on corporate, while DPA focus is on personal data

Thank you for your attention

ecrime
The Economic Impacts of Cyber Crime

Any questions?