



Confidence in a connected world.



Network security policy issues

Ilias Chantzou, Director EMEA & APJ

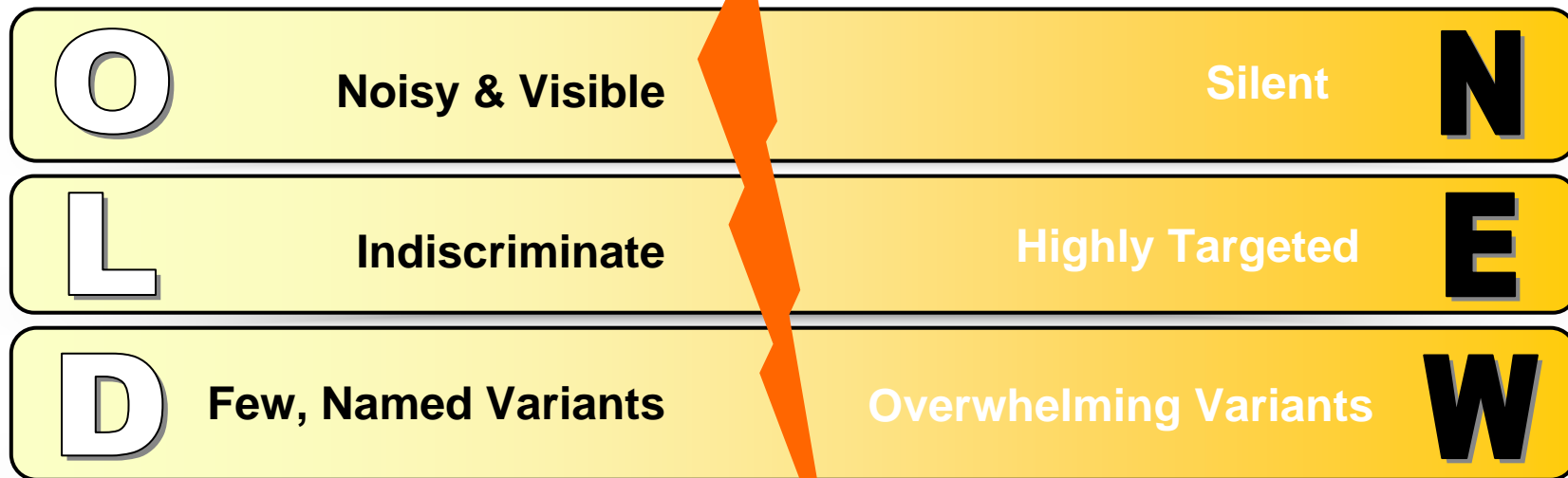
NIS Summer School 2008, Crete, Greece

Sample Agenda Slide



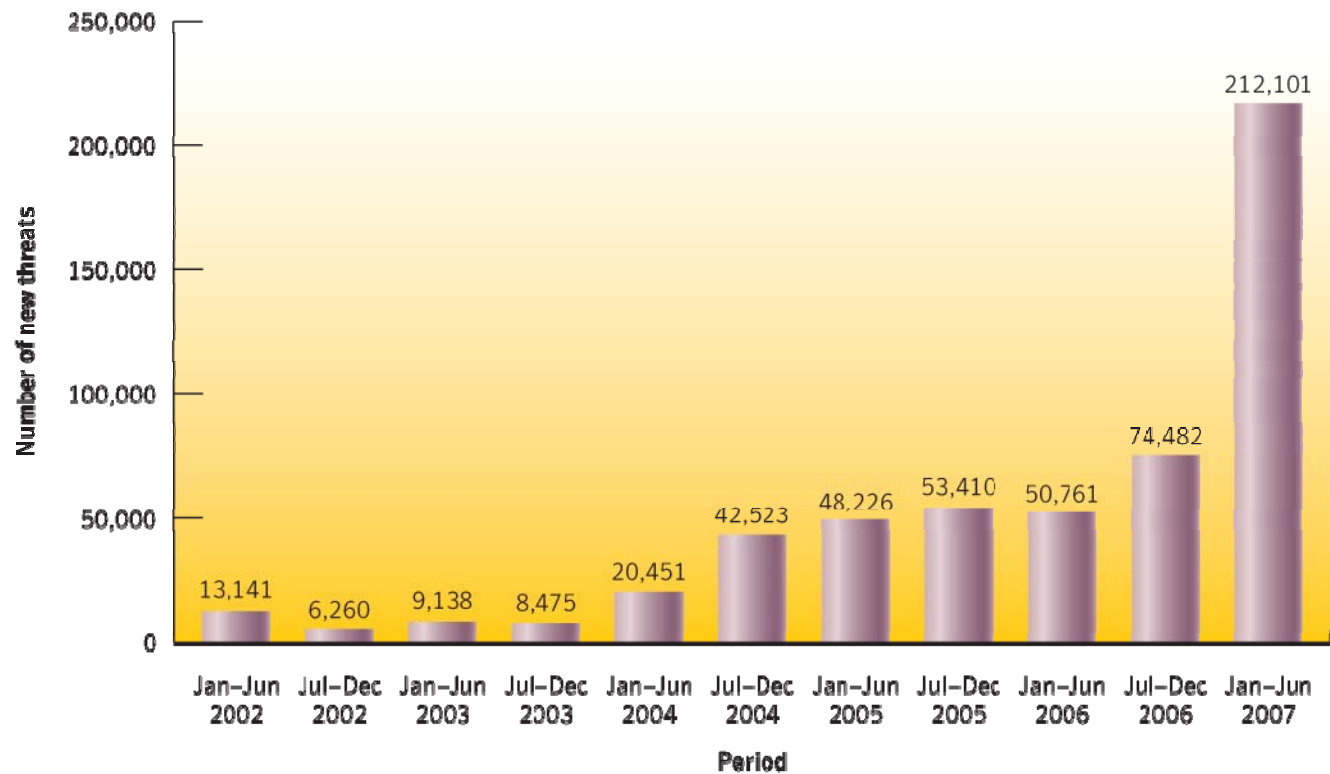
- 1 The current threat landscape
- 2 IT security and policy leadership
- 3 The EU model data protection-centric
- 4 Cybercrime
- 5 From cyber security to CIIP
- 6 Some thoughts about the future

From Hackers & Spies... To Thieves

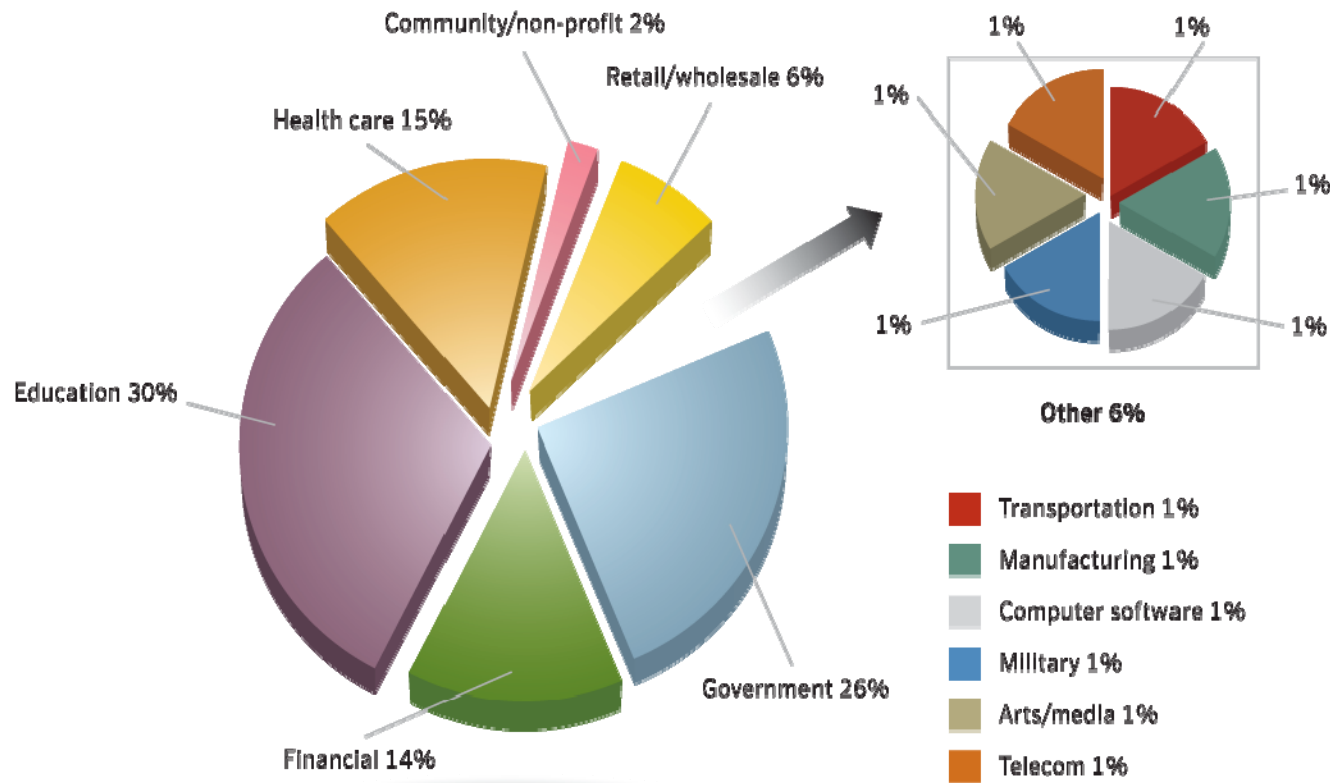


Moving from Disrupting Operations To Damaging Trust and Reputations

Figure 25. New malicious code threats



Gov't - Data breaches that could lead to identity theft by sector



EMEA - Bot-infected computers by country



Regional Rank	Previous Regional Rank	Country	Percentage of Regional Bots	Previous Percentage of Regional Bots	Percentage of Worldwide Bots	Average Lifespan (days)	Command-and-Control
1	2	Germany	23%	16%	9%	1	25%
2	3	Spain	15%	14%	6%	2	2%
3	1	France	11%	16%	5%	2	5%
4	6	Italy	9%	6%	4%	3	6%
5	4	United Kingdom	9%	11%	4%	3	11%
6	7	Israel	6%	5%	3%	3	2%
7	5	Poland	6%	8%	3%	3	2%
8	9	Portugal	2%	2%	1%	4	0%
9	8	Turkey	2%	3%	1%	2	5%
10	10	India	2%	2%	1%	4	3%

EMEA - Top countries targeted by DoS attacks



Regional Rank	Previous Regional Rank	Country	Percentage of Regional Attacks	Previous Percentage of Regional Attacks	Percentage of Worldwide Attacks
1	1	United Kingdom	46%	49%	12%
2	2	Germany	10%	11%	2%
3	4	Netherlands	7%	6%	2%
4	3	France	7%	8%	2%
5	5	Italy	4%	4%	1%
6	6	Spain	3%	4%	1%
7	7	Sweden	2%	2%	1%
8	11	Russia	2%	1%	1%
9	9	Ireland	2%	1%	0%
10	14	Poland	2%	1%	0%

The Changing Security Policy Leadership



- The US and the EU are now competing for information security thought leadership
- Connected nations are realizing the importance of good information security policy
- Legislators and regulators are beginning to think of IT security horizontally.
- Protection of the data itself is driving legislation
- Strong regulatory environment in Europe driving both good and less good policy initiatives

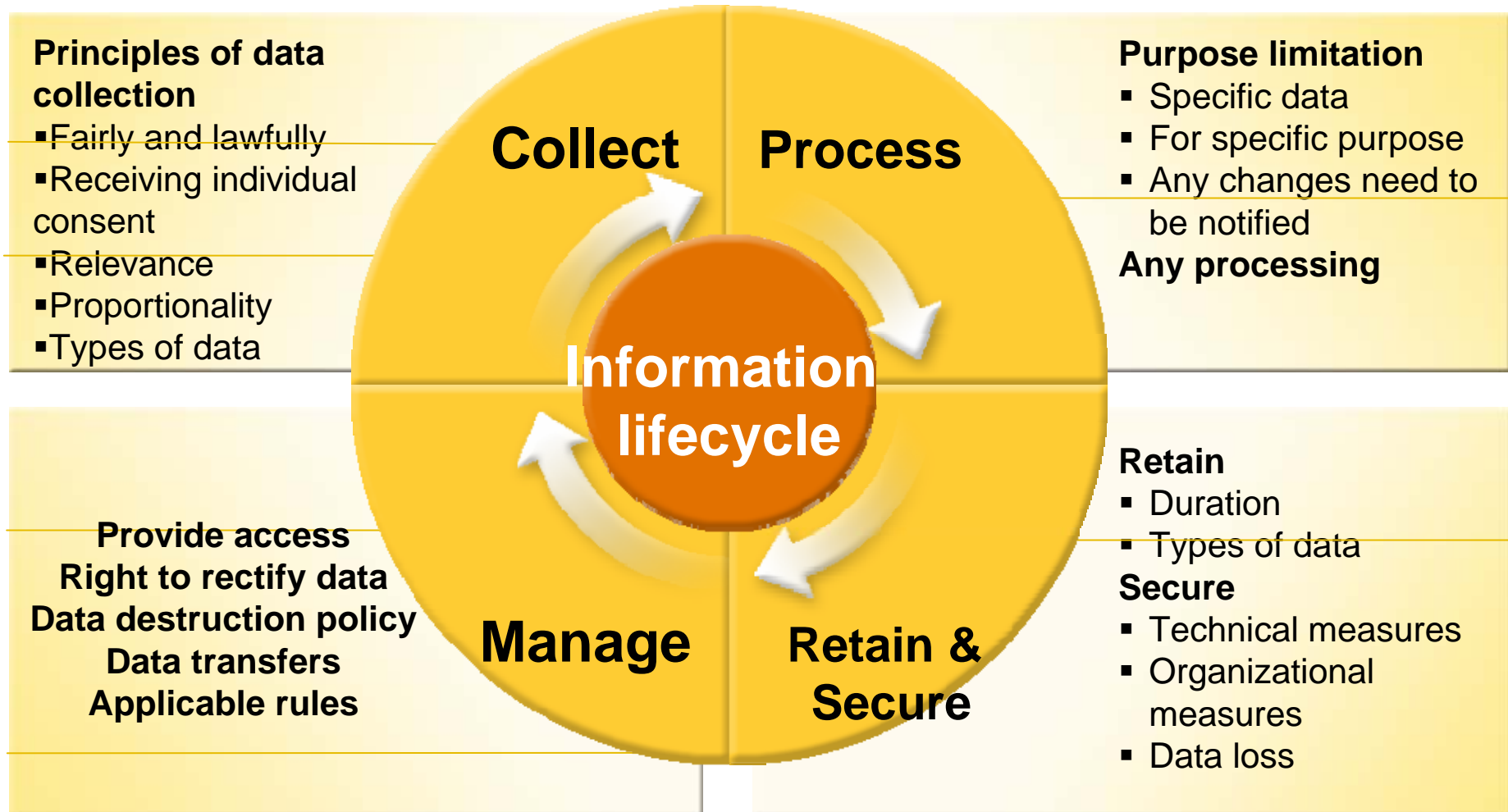
The European approach to privacy



- Cybersecurity legislation primarily through privacy laws in Europe
- EU has attempted to take a leadership role on privacy internationally by exporting its regime
- Privacy a fundamental human right since ECHR 1950
- Several countries outside the EU follow the EU model of law as it is seen as more “comprehensive”
- Principle-based
- Across all sectors
- EU FP7 research money funds privacy enhancing technologies



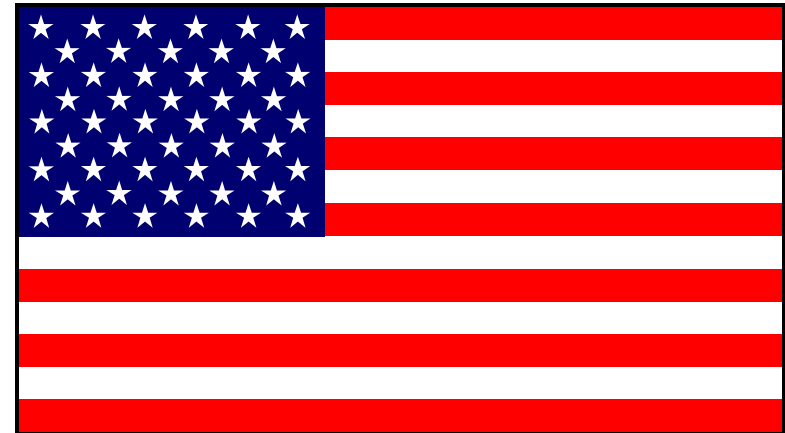
The information lifecycle and EU law



The US Approach to Privacy



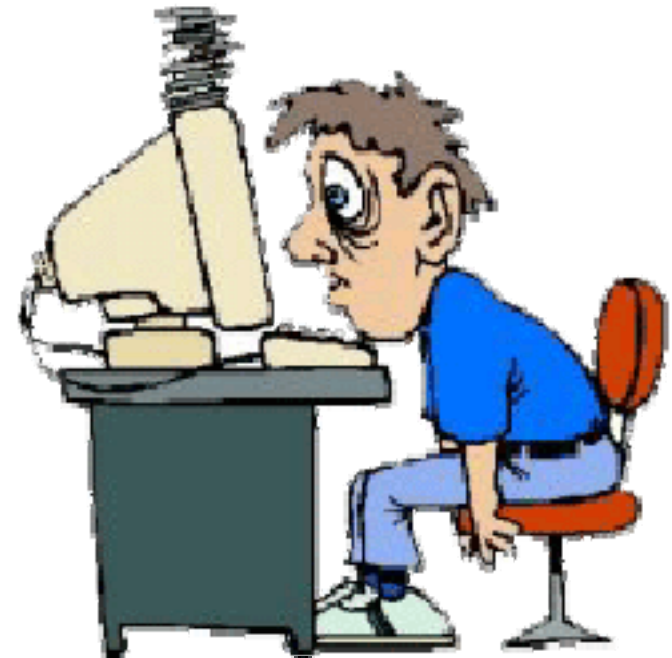
- National approach to privacy is ad hoc
- Focused on sensitive personal information areas
 - Finance and Banking (Gramm, Leach, Bliley)
 - Healthcare (HIPAA)
 - Children (CIPA, COPA)
- Compliance with varied global privacy laws becoming difficult
- Rise of identity theft and data breaches are raising the prospect for a broader approach to privacy regulation in the US
- Some in technology industry starting to push towards a legislative solution – Consumer Privacy Legislative Forum (CPLF)



What are the problems in Europe?



- Data protection is a very confrontational issue
 - Either good or bad guy
- Seen as adding another layer of compliance
 - With all the liabilities that carries
- Causes problems in doing business
 - Cross border transfers of data
- Seen as a obstacle in law enforcement cooperation
 - Data retention Directive
 - Lack of applicability on third pillar
- The discussion is often polarized and seen as dominated by extreme views
- Uncertainty about the legality of business practices that would be elsewhere legitimate
- Diverging views of the national authorities



At the heart of the problem



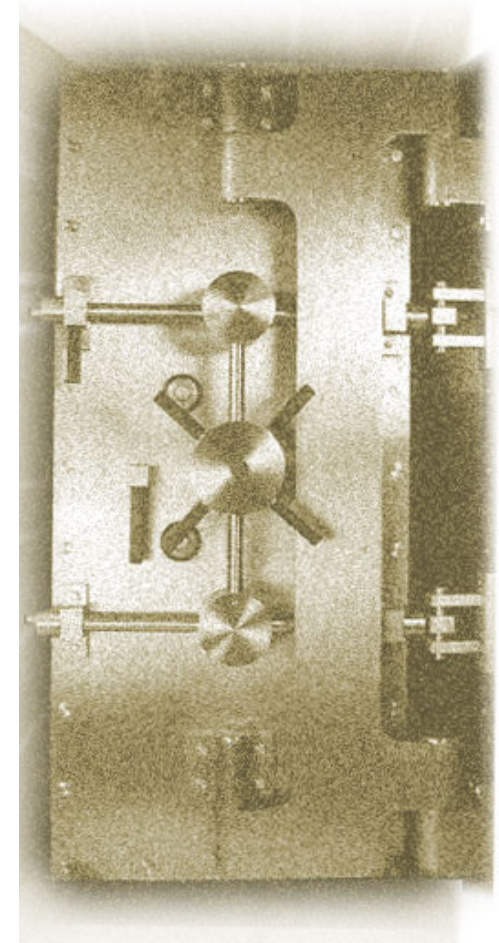
- What is personal data?
 - Broad definition
 - Relates to an individual
 - Identifies or makes the individual identifiable
- Are IP addresses personal data?
 - Old discussion
 - Initiated at the time of the data retention directive
 - Google-DoubleClick merger brought it to the forefront
 - Has taken an explosive dimension
- Conflicting interests
 - Marketing
 - IPR enforcement
 - Law enforcement
 - Search engines
 - eCommerce
 - Security
- Lack of clarity
- Is there a need for a third category of data?



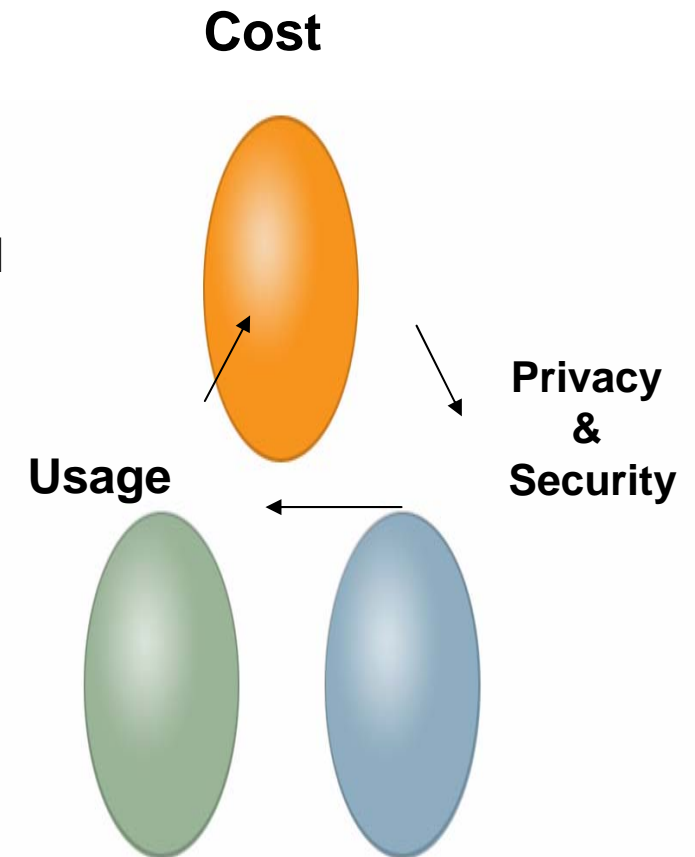
Data Retention and data protection



- The result of a conflict
 - The requirement to minimize data to protect individual privacy
 - The need to maintain data accessible to law enforcement
- Communication service providers retain data on everyone as a result of the 2006 Directive.
- That data becomes valuable as means to potentially:
 - Generate income
 - Avoid/lead to a conviction
 - Send a political message



- Cost
 - Who will pay for data retention?
 - The service provider, the EU, who?
- Privacy & Security
 - Not only storing subscriber data about you and me BUT destination of our communication e.g
 - URL web site address = content detail
 - Privacy advocates hotly contesting this!
 - Security and integrity of data stores
- Usability
 - Searching the data will be an immense challenge
 - Accuracy and integrity of the data



The risks



- Cost of digital storage becomes less of an issue, but this may not be the case for physical.
- Volume of information and duration are key factors
- Redesigning of some systems may be required
- Overwhelming amount of information will put the usefulness of the system in question
- **Security will become the primary concern**
- Searching the information in a meaningful manner a challenge

- The danger of abuse
- Information security and integrity
 - Data needs to be available
 - Data needs to be secure
 - Data needs to be collected, stored, transmitted & maintained in a forensically “clean” manner so as to stand in court
 - **Data vaults will become potential target of terrorist, organised criminal, hactivist etc.**
 - Lack of adequate security will be used as a defence

The privacy regulatory agenda in EU



- 2002/58/EC is under review
- There are a number of proposals on the table
 - Breach notice
 - Limited only to Electronic Communication providers
 - Spyware
 - Include them in the current framework
 - Spam
 - Align and cooperate better internationally
- Numerous high-profile breaches have re-enforced calls in Europe for data breach requirements across all sectors
 - Advocacy in Europe as in the US asks for safe harbour and significant breaches to be notified
 - Success depends on the whole success of this package
- 95/46/EC to be reviewed likely in 2 years time
 - More fundamental questions to be raised
- Data retention Directive under implementation but challenged at the ECJ



- Council of Europe Convention
 - By far the most comprehensive legal instrument
 - Covers substantial and procedural law
 - Adopted by a number of countries including US, Canada, Japan and South Africa
- EU Framework Decision on Attacks against information systems
 - Substantive criminal law
 - Hacking, viruses, DoS
 - What about phishing, spam, botnets?
- Currently Cybercrime legislation under implementation review
- DG JLS pushing for public-private partnerships
- Data protection remains an issue
- Enforcement remains an issue



An Active Underground Economy



- ▶ Trading in credit cards, identities, online payment services, bank accounts, bots, fraud tools, etc. are ranked according to goods most frequently offered for sale on underground economy servers.



CIP and a number of high-profile incidents



- A number of high profile incidents lead to quotes about “cyberwar”
- Too early to tell at this point what we will see coming or who is responsible for it
- Military and intelligence across the world is interested in CIIP capabilities



Some data on Estonia



- **128 Unique DDoS Attacks:**

- 115 – ICMP Floods
- 4 – TCP SYN Floods
- 9 – Generic Traffic Floods

Source = ArborSert

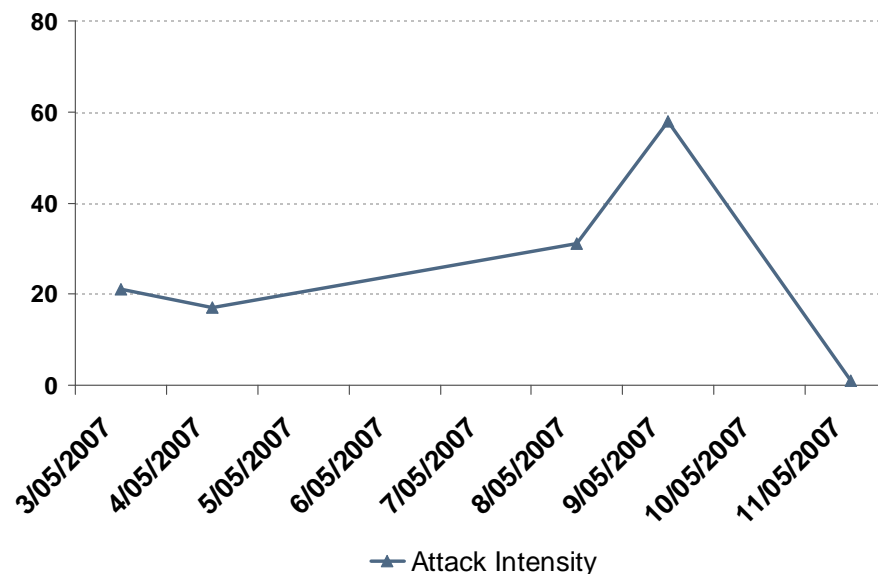
- **Daily Attack Rate:**

- 03/05/2007 = 21
- 04/05/2007 = 17
- 08/05/2007 = 31
- 09/05/2007 = 58
- 11/05/2007 = 1

Source = ArborSert

- **Attack Duration:**

- 17 attacks – Less than 1 minute
- 78 attacks – 1 minute ~ 1 hour
- 16 attacks – 1 hour ~ 5 hours
- 8 attacks – 5 hours ~ 9 hours
- 7 attacks – 10 hours or more



- Peak saw traffic equivalent of 5000 clicks per second

- Attacks stopped at Midnight

- Tactics shifted as weaknesses emerged

- Swamped web sites associated with Government Ministries, Banks, Newspapers & Broadcasters

- Emergency Services Number disabled for at least 1 hour

- Access was cut to sites outside of Estonia in order to keep local access available

Modern War fighters are dependant on achieving
“Information Dominance”

Network Enabled Capability (UK)
Network Centric Warfare (US)

They require the following:

- Intelligence collection

- Flexible dynamic networks

- Ability to share information between networks

- Ability to deploy new technologies quickly and painlessly

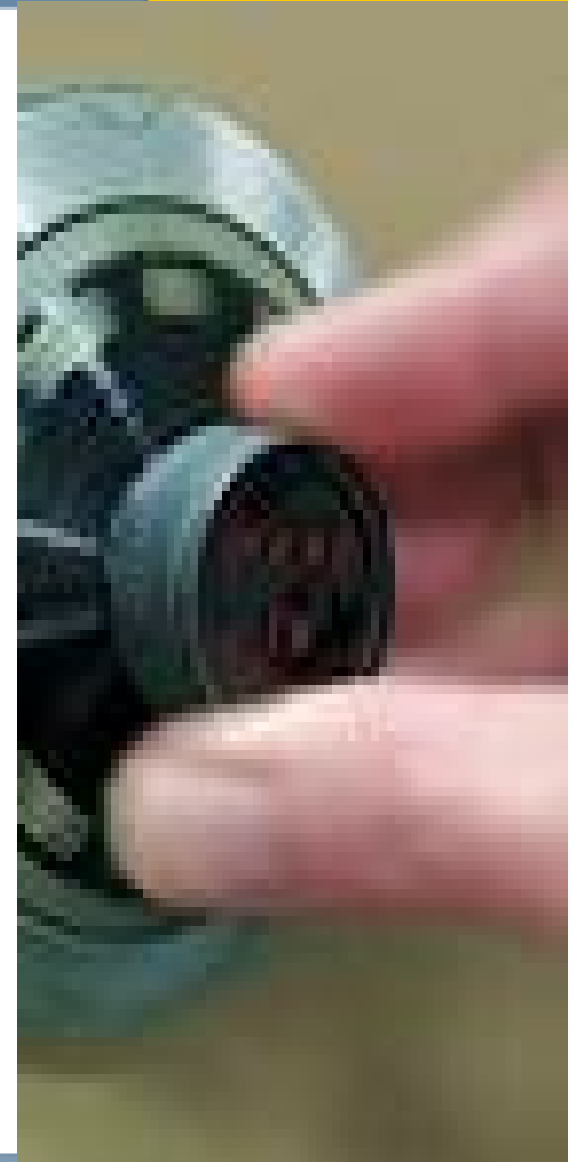
- A high level of resilience and security***

- Risk Management...not risk avoidance***

CIIP and Brussels



- No clear EU competence on these issues
- EU Proposals for Critical Infrastructure Protection
- Will apply to all EU Member States
 - A number of sectors determined as “Critical”,
 - Requirement to designate CIP operators and facilities of cross-European importance
 - Requirement to develop plans to deal with all hazards with a terrorist priority
 - Requirement to submit the plans to the national authority and audit them
- ICT is now out but CIIP communication expected this year
- EU Projects on CIIP
- Potentially a role for ENISA
- NATO active in this area with its own projects



Concluding remarks



- Threats are there and will continue
- Approach to ensure security through data protection is the right way provided data protection is properly applied
- The debate will continue until more legal clarity is achieved
- Cybercrime legislation is OK as long as it is updated and properly enforced
- The CIIP element is on the rise and the EU will get a stronger role
- The military and intelligence component will necessarily become involved
- Security is driven by competition and diversity
- This is just the beginning!!





Confidence in a connected world.

Thank You!

Ilias Chantzos

Ilias_chantzos@symantec.com

+3225311176

© 2007 Symantec Corporation. All rights reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND IS NOT INTENDED AS ADVERTISING. ALL WARRANTIES RELATING TO THE INFORMATION IN THIS DOCUMENT, EITHER EXPRESS OR IMPLIED, ARE DISCLAIMED TO THE MAXIMUM EXTENT ALLOWED BY LAW. THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE.