The dilemma European Security Policy and Privacy

Ilias Chantzos
Government Relations EMEA

Terena Conference, May 2006

AGENDA

I. Managing risk and the threat landscape

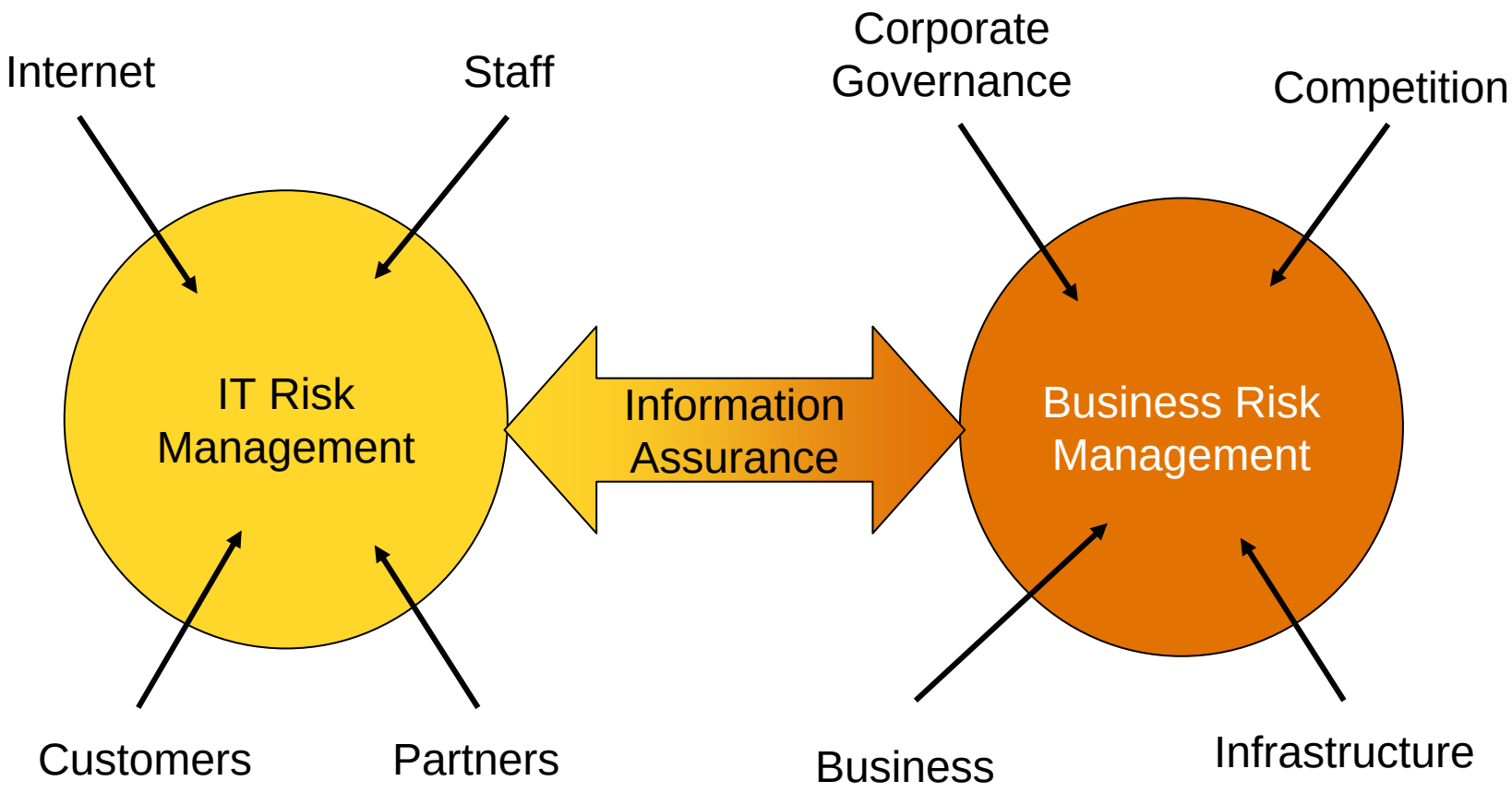
II. Regulation

III. Conclusions

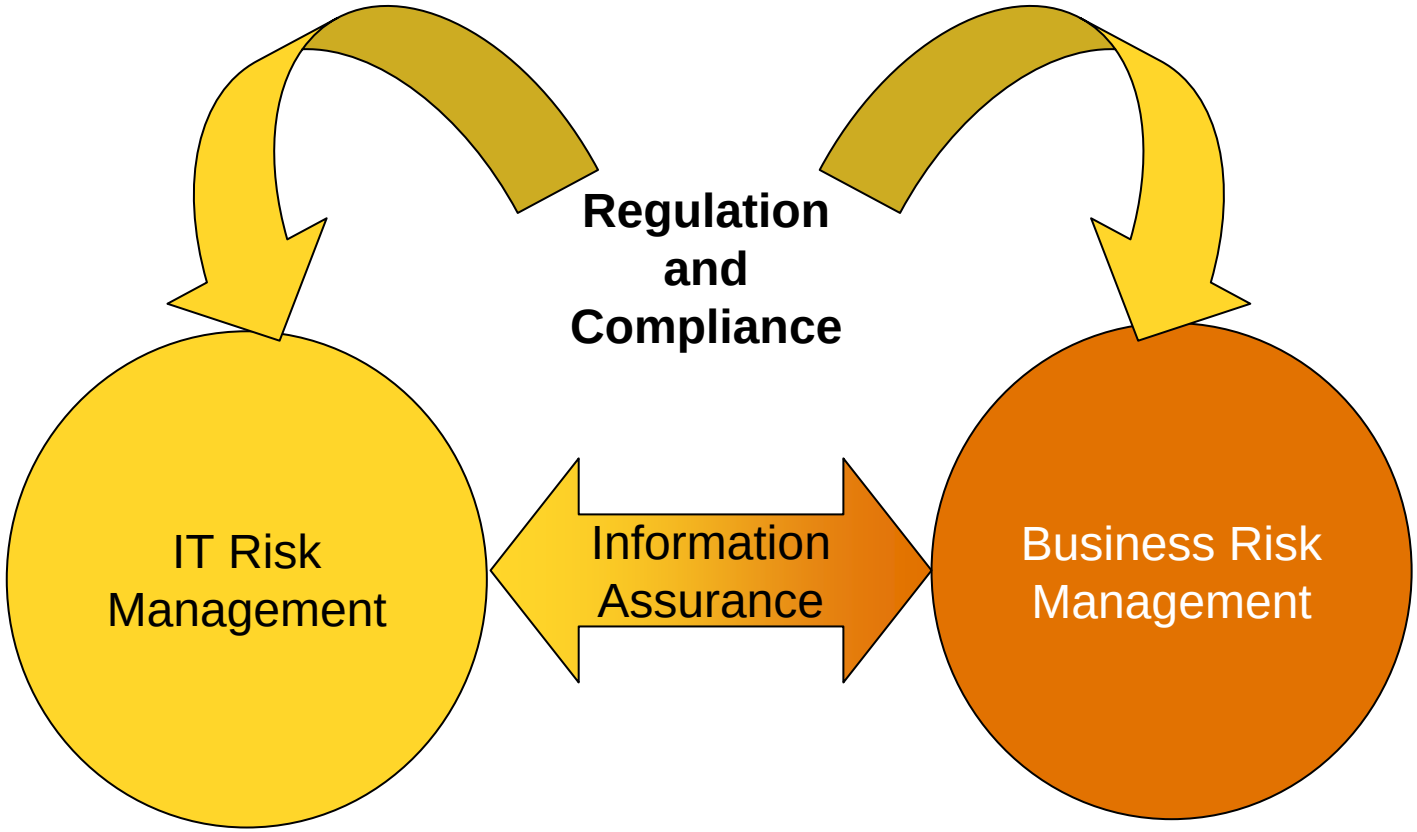
Managing the risk is a daily challenge

Key Issues:
- ✓Cost
- ✓Complexity
- ✓Compliance

Information assurance is about managing risk



A key element is regulatory compliance

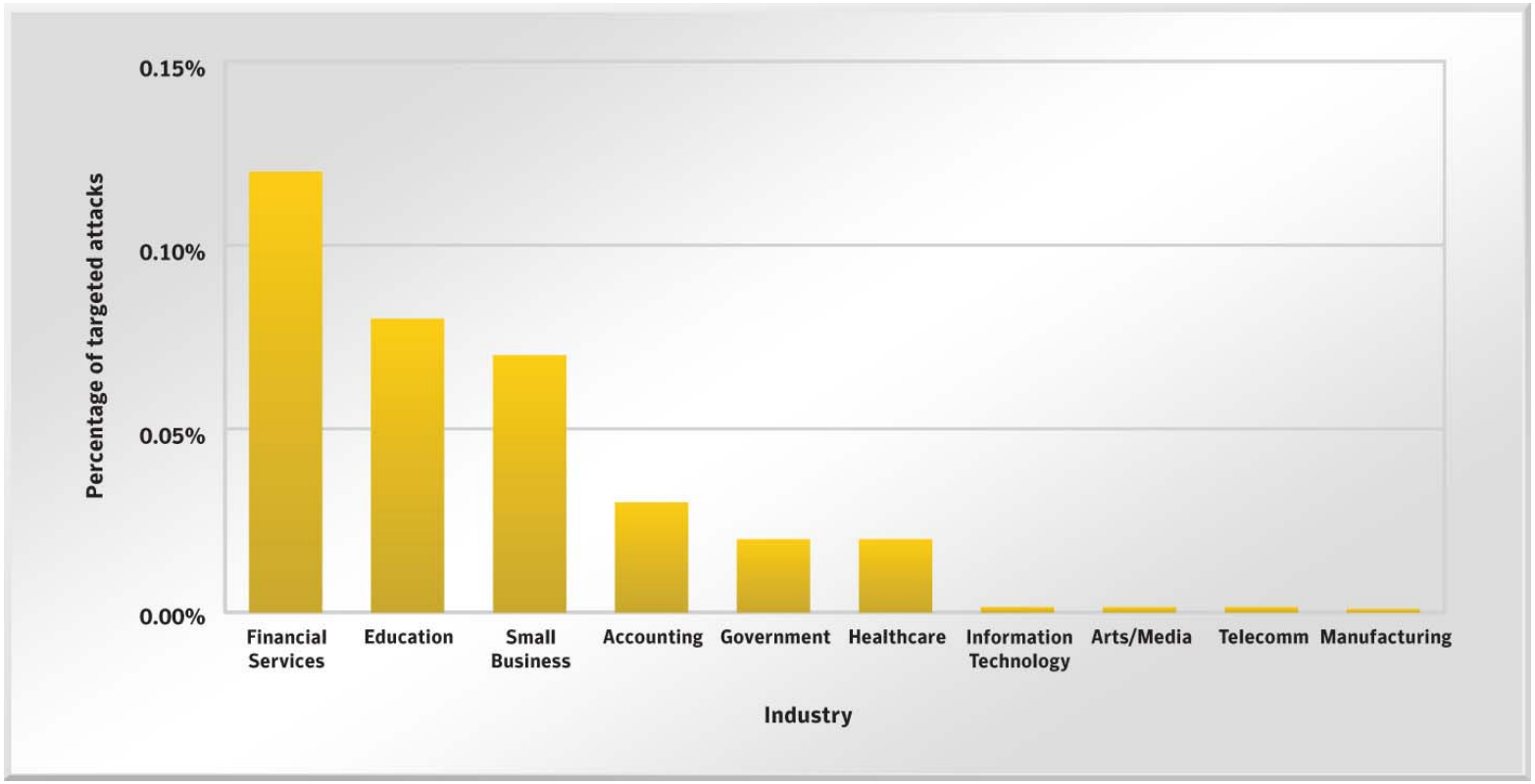


Today's Threat Landscape

- Cybercrimes such as online fraud and the theft of confidential information are dominating the public's consciousness .
- Bots, bot networks and customizable or 'modular' malicious code are the preferred methods of attack.
- Web applications and web browsers increasingly becoming the focal point of attacks.
- Continued decline in noisy Category 3 & 4 threats and a corresponding increase in quieter, stealthier Category 1 and 2 threats.
- You have to go looking for the threats……

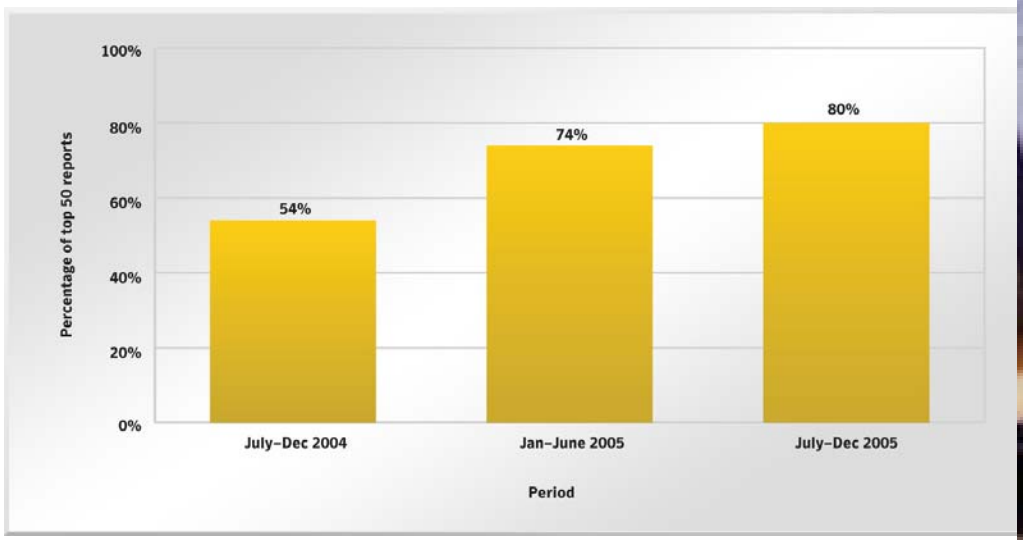
Attack Trends – Top Targeted Industries

- As predicted, the rise in online fraud and the shift towards financial motivation has moved Financial services to the top of targeted industries in the last half of 2005.



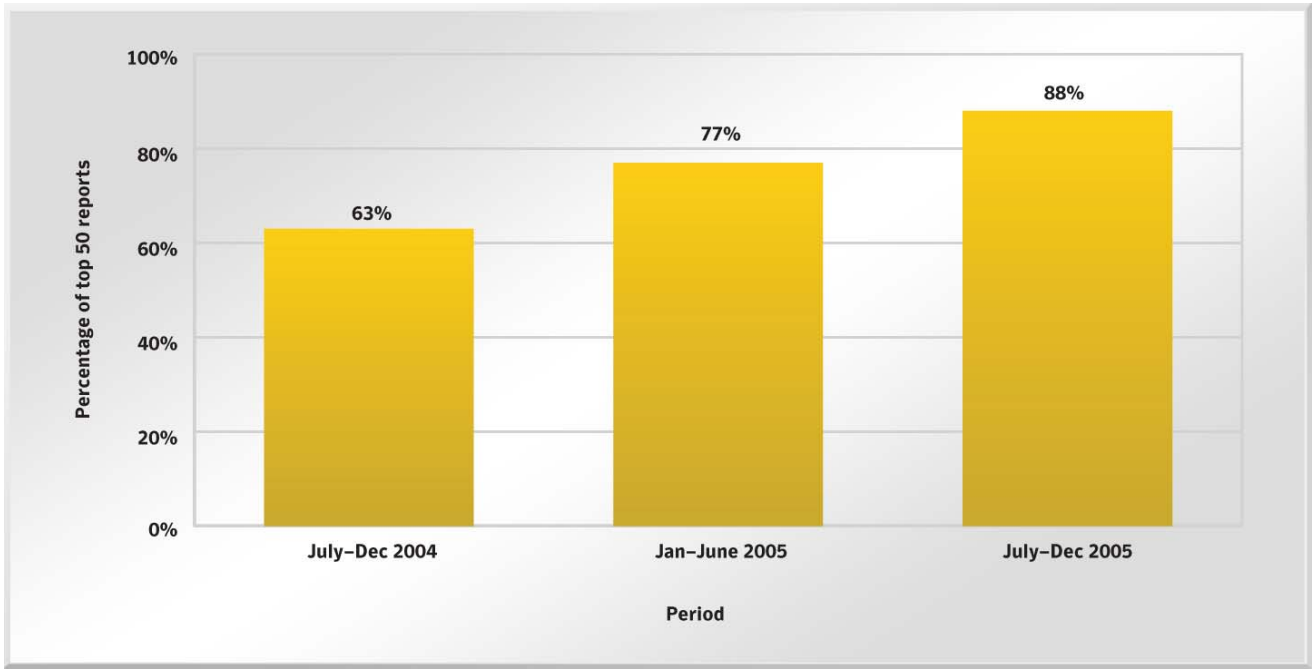
Malicious Code Trends – Threats to Confidential Information

- Threats to confidential information continue to increase over the past three reporting periods with 80% of the Top 50 reported malicious code in this period, having the potential to expose confidential information.



Malicious Code Trends – Modular Malicious Code

- Modular malicious code is malicious code that initially possesses limited functionality, but that, once installed on a target host can download other pieces (or modules) of code with different, usually malicious, functionalities.
- 88% of all malware code had this functionality



Attack Trends – Time To Compromise - Servers

- Server operating systems in a web sever role

Configuration	Median Average (h:m:s)	Max (h:m:s)	Min (h:m:s)
Microsoft Windows 2000 Server – No Patches	1:16:55	18:27:47	0:01:14
Microsoft Windows 2000 Server – Service Pack 4	1:32:08	17:12:54	0:00:41
Microsoft Windows 2003 Web Edition – No Patches	4:36:55	23:00:13	0:02:08
RedHat Enterprise Linux 3 Web – Unpatched	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows 2000 Server – Fully Patched	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows 2003 Web Edition – Fully Patched	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows 2003 Web Edition – Service Pack 1	Not Compromised	Not Compromised	Not Compromised

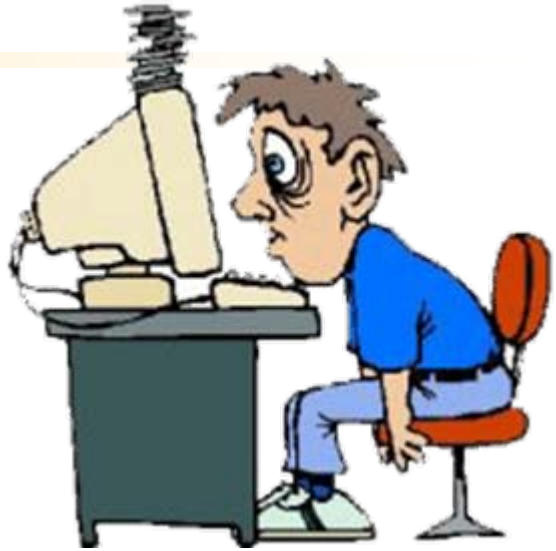
Attack Trends – Time To Compromise - Desktops

- Desktop systems NOT behind a firewall.

Configuration	Median Average (h:m:s)	Max (h:m:s)	Min (h:m:s)
Microsoft Windows XP Professional – No Patches	1:00:12	22:13:18	0:00:37
Microsoft Windows 2000 Professional – No Patches	1:03:18	20:18:03	0:01:19
Microsoft Windows 2000 Professional – Service Pack 4	1:14:20	21:02:48	0:00:39
SuSE Linux 9 Desktop	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows 2000 Professional – Full Patch	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows XP Professional – Full Patch	Not Compromised	Not Compromised	Not Compromised
Microsoft Windows XP Professional – Service Pack 2	Not Compromised	Not Compromised	Not Compromised

The Regulatory Challenges

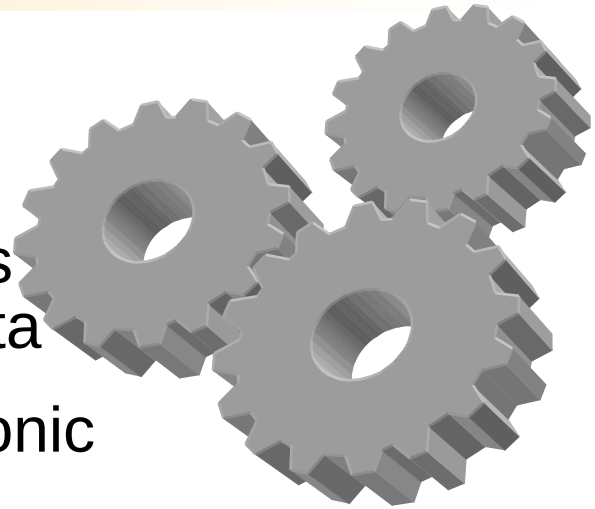
Examples of European Regulation



- Protecting YOUR data
  - 95/46/EC Generic Data Protection
  - 2002/58/EC Specific Data Protection
  - Data Retention
- Protecting against damaging data
  - Framework Decision on attacks against info-systems
  - Council of Europe Convention on Cybercrime
- Protecting the data of specific industries
  - Basel II
  - Use of public sector information

Data protection

- Directives 95/46/EC (generic) and 2002/58/EC (specific)
- Generic Directive covers all activities related to processing of personal data
- Specific Directive covers only electronic communications
- Create independent authorities responsible for supervision and enforcement
- Very interesting from a security standpoint

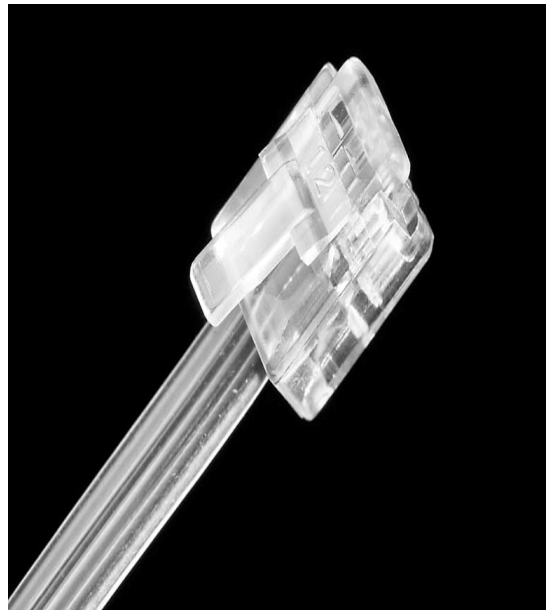


The Generic Directive

- Defines data categories
- Requires information collection fairly and lawfully subject to consent
- Requires information security and availability for the storage of data
- Requires access to data subject and rectification of the data
- Forbids cross-border transfer of personal data
- Determines jurisdiction

Specific Directive

- Defines traffic data
- Requires network security
- Obliges eCommunication providers to notify users of the services for eminent threats
- Obliges the destruction of traffic data if no excluded specific business is applicable
- Forbids spam distribution
- Leaves the door open for data retention



Data retention

- Routinely retaining traffic data by eCommunication service providers for law enforcement purposes
  - What data?
  - How much?
  - How long?
- Not preservation
- Not interception

The data……

- Personal Data
  - My name
  - My ID number
  - Anything that identifies me
- Sensitive Data
  - Race
  - Religious beliefs
  - Etc
- Traffic data
  - IP addresses
  - URLs
- Data
  - Any data covered by the Data Retention Directive

Some challenges with current privacy rules

Looking at 2002/58/EC

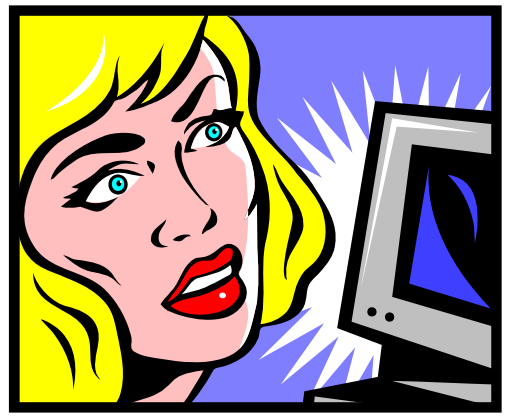
- What is personal data in eCommunications environment?
- IP addresses are personal data?
  - How do we log them
  - Do we ask permission
- Staying ahead of the threats
  - Spam is covered by the Directive but what about?
    - Spyware
    - Addware
    - Phishing
- How we collect the data and how do we use them?
  - No obligation to notify in case of breach
- What is the role of the service provide?
  - To provide an appropriate level of security

So does Internet kill regulation?

- Internet is probably one of the most regulated environments in the world
  - Everybody's laws seem to apply
- The issue is better/smarter regulation as opposed to no regulation
- Do not become a hostage of fortune
- Do not over-protect
- Technology and self-regulation
- Finding the right balance…..

Security vs Privacy vs Regulation

- Technology does not mean less privacy
  - Privacy enhancing technologies everywhere around us
- Security is not against privacy
  - Security is a privacy pre-condition
- Regulation is not against technology
  - Needs to be regularly updated/reviewed
  - Needs to be technology neutral
  - Needs to set framework conditions
  - Should not be over-extended
  - Should be prepared in consultation
  - Current review of 2002/58/EC



Thank You!

Ilias_chantzos@symantec.com
+3225311161