IBM SECURITY TRENDS SEMINAR 2012

FORTIFY YOUR COMPANY
AGAINST INTERNAL AND EXTERNAL THREATS

Recent Trends in Information Security Management and ISO 27001

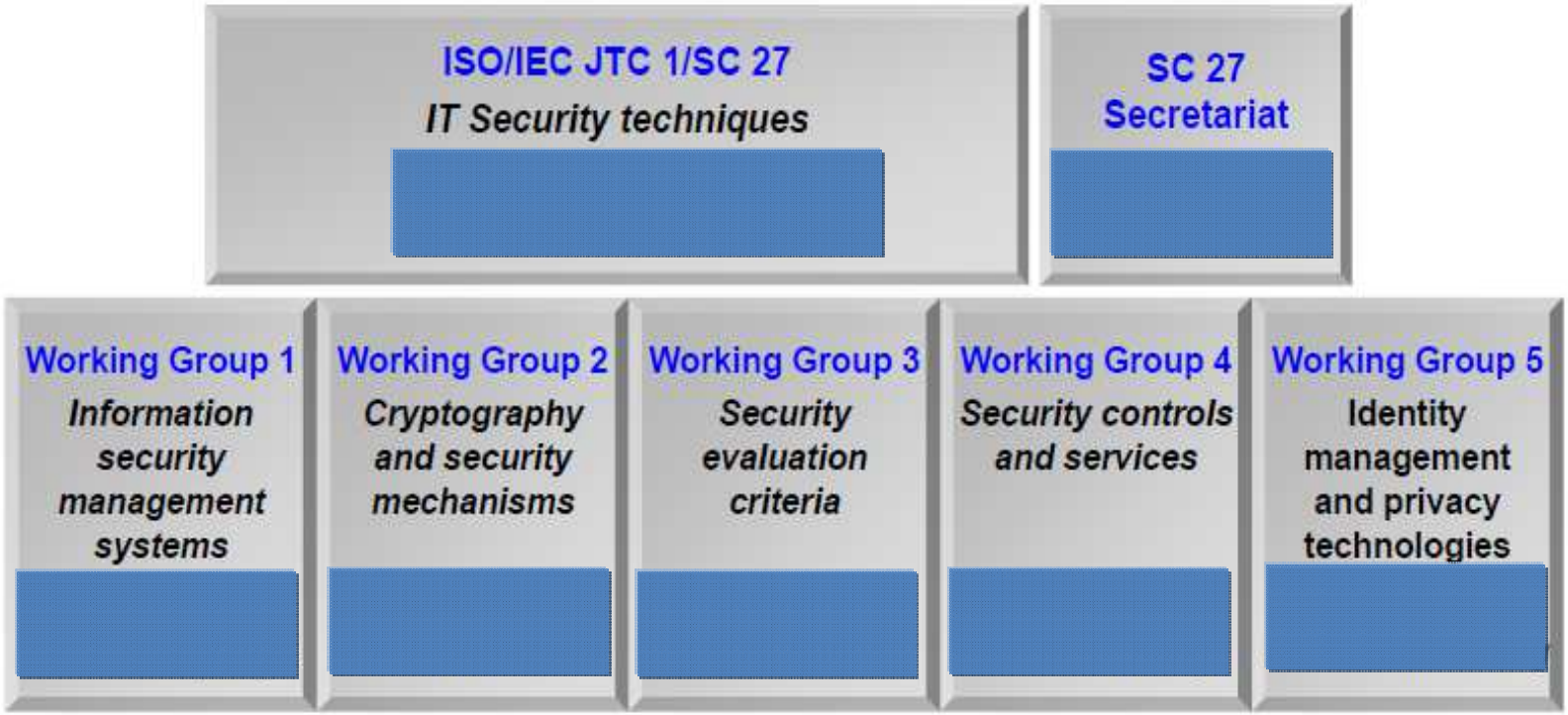
Dale Johnstone
Vice-Convenor ISO/IEC JTC 1 SC 27 WG 1

IBM SECURITY SOLUTIONS
RISK MITIGATION. PROTECTION. COMPLIANCE.

International Standards Organization – SC 27

- The development of standards for the protection of information and ICT. This includes **generic methods, techniques and guidelines** to address both **security** and **privacy** aspects, such as
  - Information Security Management Systems (ISMS), security controls and services;
  - Cryptographic mechanisms;
  - Security aspects of identity management, biometrics and privacy;
  - Conformance assessment, accreditation and auditing requirements in the area of information security;
  - Security evaluation criteria and methodology.

International Standards Organization



ISMS FAMILY OF STANDARDS (WG1)

27001: 2005 ISMS Requirements		
27000: 2009 ISMS Overview and Vocabulary	27006: 2011 Accreditation Requirements	27010 ISMS for inter-sector and inter-organisational communications
27002: 2005 (pka 17799) Code of Practice	27007: 2011 ISMS Auditing Guidelines	27011: 2008 | ITU-T X.1051 Telecom Sector ISMS Requirements
27003: 2010 ISMS Implementation Guidance	TR 27008: 2011 ISMS Guide for auditors on ISMS controls	27014 | ITU-T X.1054 Governance of information security
27004: 2009 Information Security Mgt Measurement		TR 27015 Information security mgt guidelines for financial services
27005: 2011 Information Security Risk Management		TR 27016 Information security mgt - Organizational economics
Supporting Guidelines	*Accreditation Requirements and Auditing Guidelines*	*Sector Specific Requirements and Guidelines*

Security Controls (WG4)

- ICT Readiness for Business Continuity (27031)
- Cybersecurity (27032)

Unknown or Emerging Security Issues

- Network Security (27033 – parts)
- Application Security (27034 - parts)
- Security of Information Objects (15816)
- Security of Outsourcing (27036)
- TTP Services Security (14516)
- Time Stamping Services (29149)

Known Security Issues

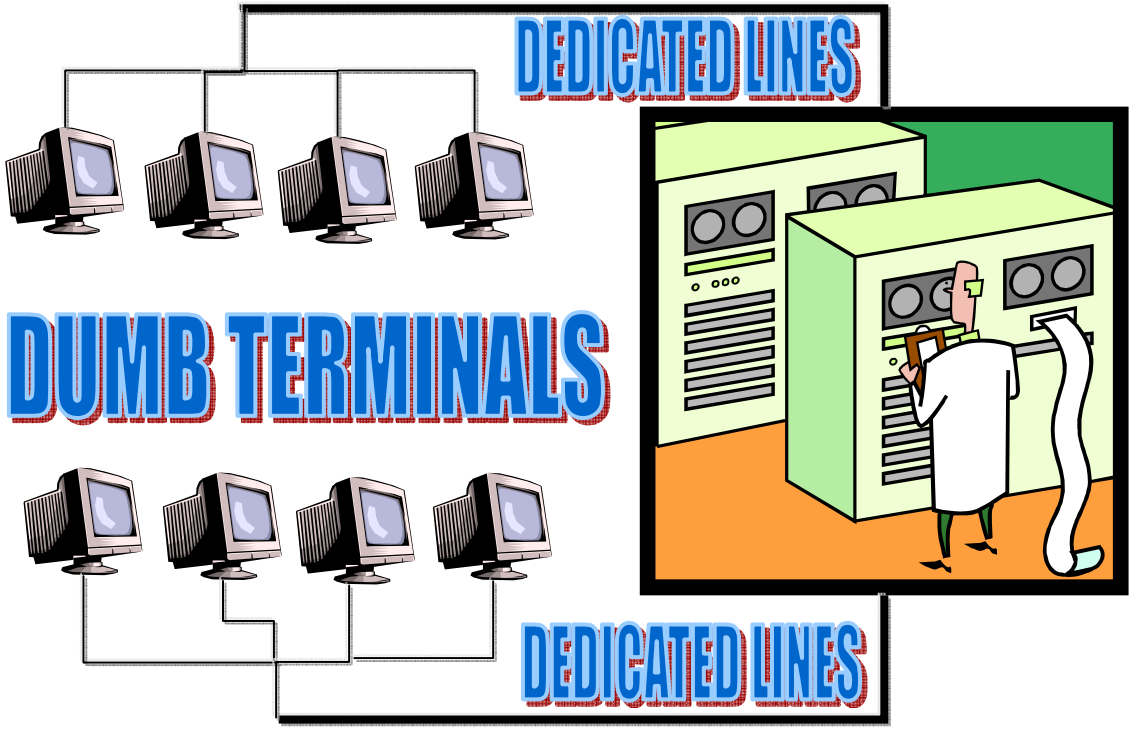
- Information security Incident Management (27035)
- ICT Disaster Recovery Services (24762)
- ID, Collection, Acquisition, Preservation of Digital Evidence (27037)

Security Breaches and Compromises

Japan	4004	Hong Kong	32	Vietnam	14	Morocco	4	Armenia	1
UK	536	Greece	31	Iceland	13	South Africa	4	Bangladesh	1
India	527	Australia	29	Indonesia	13	Belgium	3	Belarus	1
China	507	Singapore	29	Colombia	11	Chile	3	Denmark	1
Taiwan	456	Mexico	27	Kuwait	11	Gibraltar	3	Ecuador	1
Germany	202	France	26	Norway	10	Macau	3	Jersey	1
Korea	106	Slovakia	26	Portugal	10	Qatar	3	Kyrgyzstan	1
Czech Republic	110	Turkey	26	Sweden	10	Albania	2	Lebanon	1
USA	104	Brazil	24	Canada	9	Argentina	2	Moldova	1
Italy	81	UAE	20	Russian Federation	9	Bosnia Herzegovina	2	New Zealand	1
Spain	75	Netherlands	22	Switzerland	9	Cyprus	2	Sudan	1
Hungary	70	Croatia	21	Bahrain	8	Isle of Man	2	Uruguay	1
Poland	62	Slovenia	20	Egypt	5	Kazakhstan	2	Yemen	1
Malaysia	58	Bulgaria	18	Oman	5	Luxembourg	2		
Thailand	48	Iran	18	Peru	5	Macedonia	2		
Austria	44	Philippines	15	Sri Lanka	5	Malta	2		
Ireland	44	Pakistan	14	Dominican Republic	4	Ukraine	2		
Romania	35	Saudi Arabia	14	Lithuania	4	Mauritius	2	**Total**	**7686**

ISO 27001 Certifications

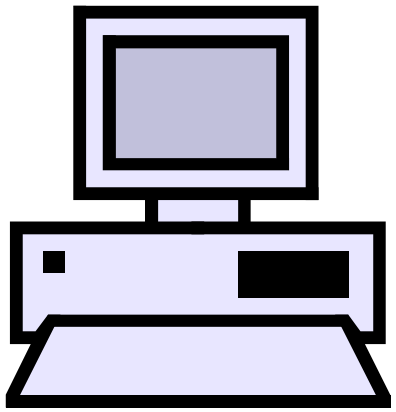
In the Beginning – 30+ Years Ago



HOME USERS
STAND-ALONE

In the Beginning – 30+ Years Ago

July 1980, IBM representatives met with Microsoft's Bill Gates to talk about writing an operating system for IBM's new hush-hush "personal" computer.



12 August 1981, IBM released their new computer, re-named the IBM PC. The "PC" stood for "personal computer" making IBM responsible for popularizing the term "PC".

Ran on 4.77 MHz Intel 8088 microprocessor, 16 kilobytes of memory, expandable to 256k

PC came with one or two 160k floppy disk drives and optional color monitor

http://inventors.about.com/od/computersandinternet/a/Ibm-Pc.htm

IBM SECURITY TR

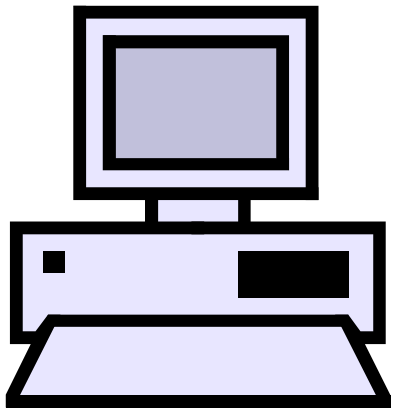
FORTIFY YOUR COMPANY AG

IBM

In the … go

July 1980 – Star…

12 August 1981 …



1… …n the wild

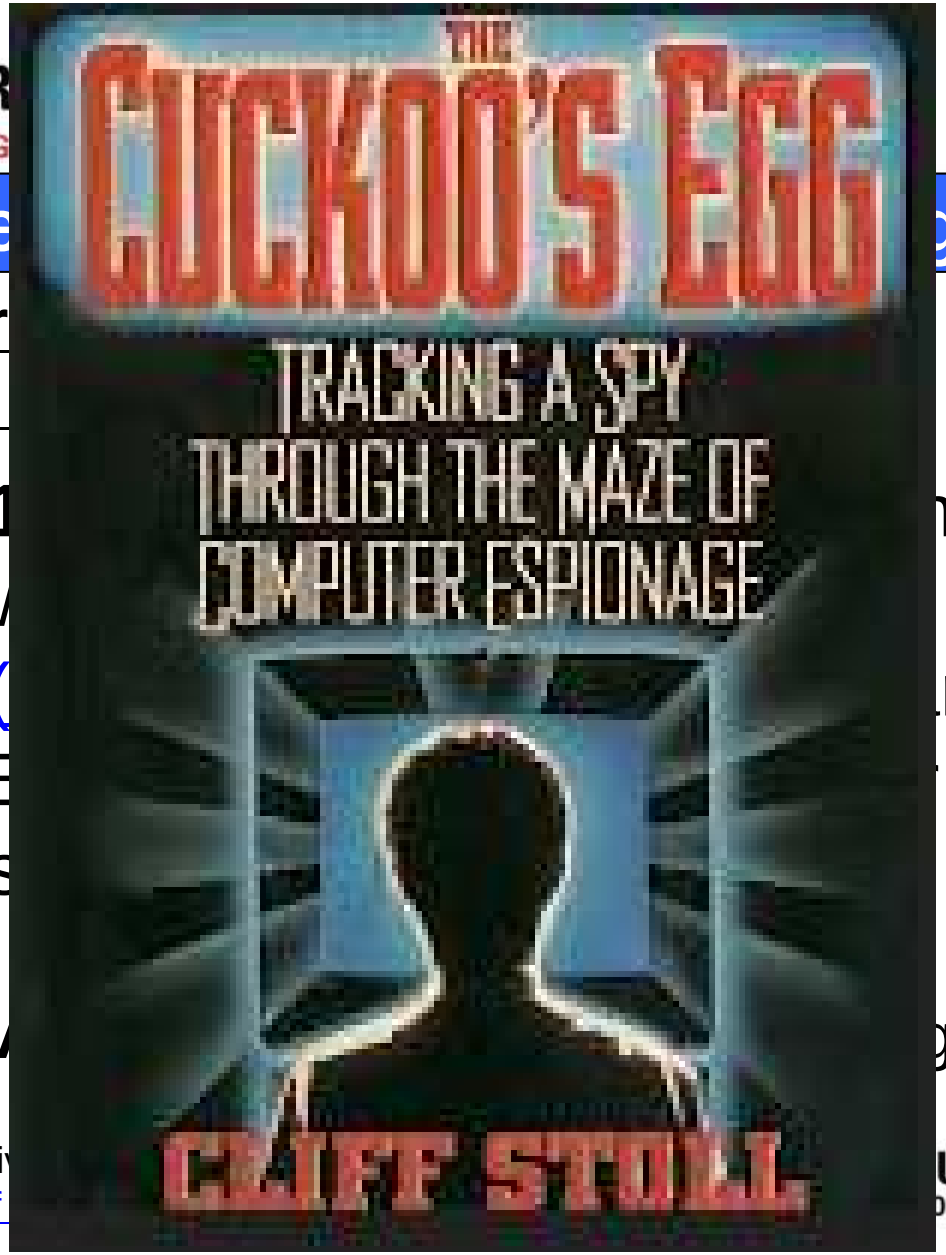
v… dubbed

(… …rooq Alvi

E… piracy of

s…

A… …g (1989), Stoll



"Boot sector virus repair". Anti…

Amjad Farooq Alvi Inventor of …

…URITY SOLUTIONS

…ON. PROTECTION. COMPLIANCE.

Information Technology

Information Technology Is Crucial

BREACH TRENDS

…385 breaches of protected **HEALTH** information affecting over **19 million** records reported since August 2009

…breach notification regulation issued …

Health Information Technology for Economic and Clinical Health (HITECH) Act

Redspin Breach Report 2011 - Protected Health Information, February 2012

BREACH TRENDS

PHI Data Breach by Source/ Device, Oct 2009 - Nov 2011

Laptop and other portable device		151	39.2%
Paper		92	23.9%
Computer		56	14.5%
Server		38	9.9%
Other		18	4.7%
Email		7	2%
Electronic Health Record		6	1.6%
X-Ray		5	1.3%
Back-up Tapes		4	1%
Drives		3	0.8%
Mail, Postcards		3	0.8%
CD		2	0.5%
	Total	385	100%

Study on Patient Privacy and Data Security, Ponemon Institute, December 2011

BREACH TRENDS – Q4 2011 Highlights

101 billion
Average daily **spam/phishing** emails sent

Pharmacy ads
Most popular spam topic (31.2% of spam)

209,000 **Zombies**
Daily turnover

India
Country with the most **zombies** (23.5%)

Streaming media/ Downloads
Most popular blog topic on user-generated content sites

Parked Domains
Website category most likely to be contain **malware**

ComTech, Internet Threats Trend Report, January 2012

BREACH TRENDS – 2012 Predictions

Industrial Threats

The Threat Within: Embedded Hardware

Hacktivism

Virtual Currency

Cyberwar

DNSSEC

Spam Goes "Legit"

Mobile Threats

Botnets + Rootkits = low-level trouble

Mobile Banking Attacks

Rogue Certificates

Advances in Operating Systems

McAfee, 2012 Threats Predictions

11 MASSIVE SECURITY BREACHES

They make the news on a regular basis: incidents in which a company or government agency's security is breached, leading to a loss of information, personal records, or other data...

Some (breaches) result in the loss of millions of data records, some affect millions of people, and some wind up costing the affected businesses a lot of money. Not to mention, the questions if you calculate the value of personal medical information vs. credit card numbers

http://www.informationweek.com/news/galleries/security/attacks/229300675

11 MASSIVE SECURITY BREACHES

April 2009

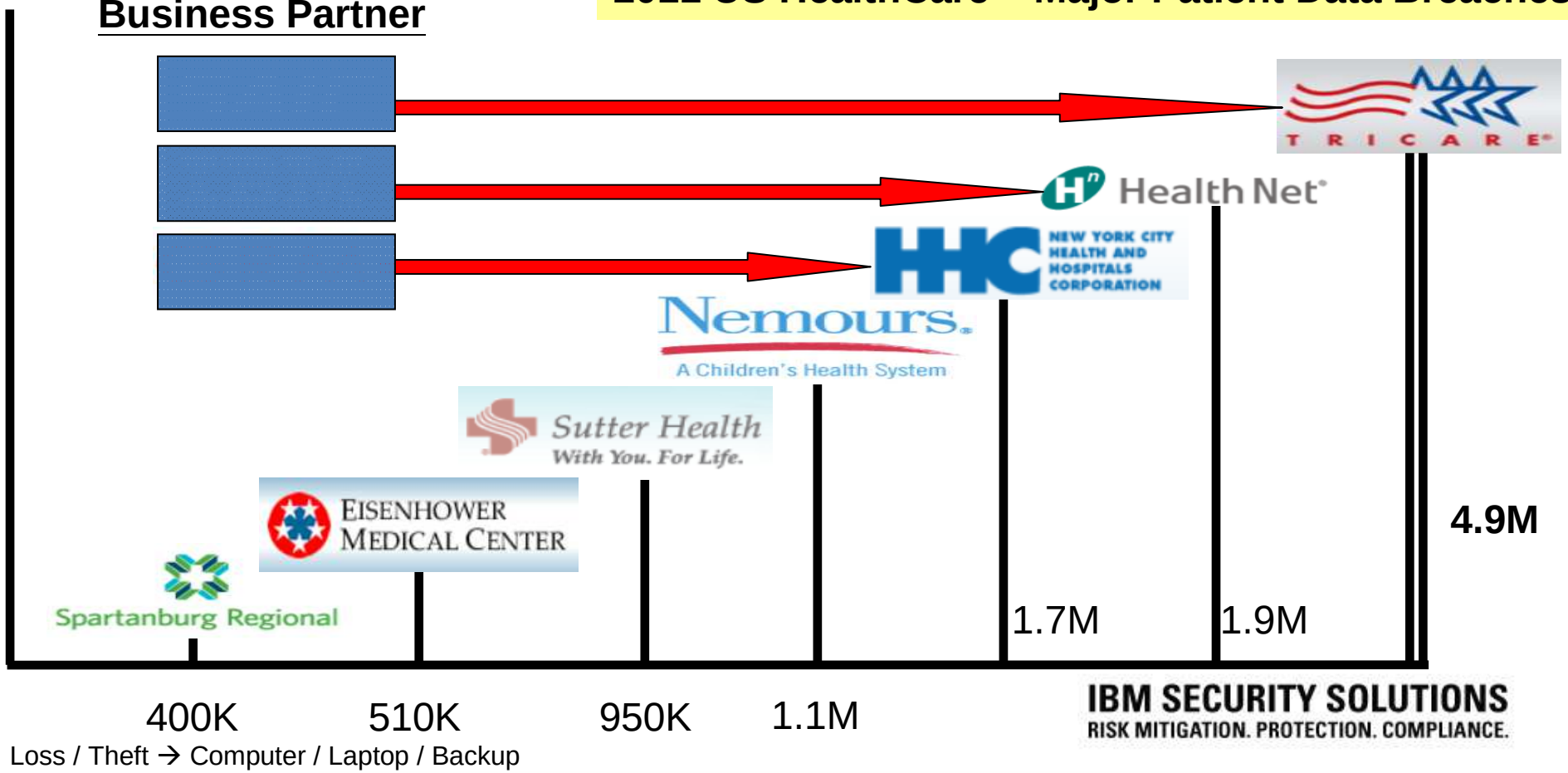
Spyware Emailed 1000+ Screenshots of 62 Patients

1.5 million customers

http://www.informationweek.com/news/galleries/security/attacks/229300675

BREACH TRENDS

2011 US HealthCare – Major Patient Data Breaches



IBM SECURITY TRENDS SEMINAR 2012

FORTIFY YOUR COMPANY AGAINST INTERNAL AND EXTERNAL THREATS

YOU WANT MORE – 2011 BREACHES

WORDPRESS.COM

IBM SECURITY SOLUTIONS

RISK MITIGATION. PROTECTION. COMPLIANCE.

EUROPEAN COMMISSION – Data Protection Laws

25 January 2012

EUROPEAN COMMISSION PROPOSES A COMPREHENSIVE REFORM OF DATA PROTECTION RULES TO INCREASE USERS' CONTROL OF THEIR DATA AND TO CUT COSTS FOR BUSINESSES

EU'S DATA PROTECTION LAW INTRODUCE A SINGLE SET OF RULES ON DATA PROTECTION, VALID ACROSS EU

Not Yet Approved

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=EN&guiLanguage=en

EUROPEAN COMMISSION – Data Protection Laws

Protecting people
Company **responsibility and accountability** – notify clients of any theft or accidental release of PII

Consent explicitly required before a company reuses personal data – people also access their own private data and to transfer it to another service provider

'right to be forgotten' – people able to have their PII deleted if a Company has no legitimate reason for keeping it

Apply EU rules when PII is **processed outside Europe** – people able to involve national data protection authority in their country, even when their data is processed by a company based outside the EU

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=EN&guiLanguage=en

CONCLUSION

Threats are Real

Risks are Increasing

Data is Becoming More Mobile & Duplicated

Staff ARE IT Empowered Beyond Organisation Control

IF YOU THINK YOUR ORGANISATION IS IMMUNE FROM THE RISK OF COMPROMISE THINK AGAIN !!!

Questions

Dale Johnstone
Vice-Convenor ISO/IEC JTC 1 SC 27 WG 1