The future direction of information security good practice

Presentation to the JNSA

27 January 2010

Bill Caughie ISF Chief Operating Officer

Agenda

1. Introduction to the Information Security Forum
2. What is good practice?
3. A look into the future
4. How good practice should evolve
5. Conclusion

Information
Security
Forum

An introduction to the Information Security Forum

The Information Security Forum

Is a not-for-profit Membership organisation

Has just under 300 Members who are large corporates or governments

Operates in many regions of the world

Delivers:

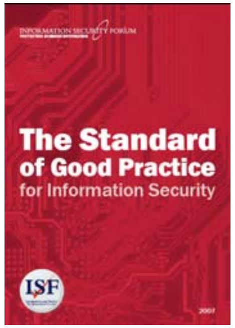
- Research on Member's security issues
- Benchmarking services
- Risk software and tools
- Publishes a standard

What is good practice?

Good practice

The ISF publishes a standard defining good practice every two years, based on its research with leading organisations across the world in order to:

- respond to the needs of leading international organisations
- refine areas of best practice for information security
- reflect the most up-to-date thinking in information security
- remain aligned with other information security-related standards, such as ISO 27002 (17799) and COBIT v4.1
- include information on the latest ‘hot topics’.



INFORMATION SECURITY FORUM

The Standard of Good Practice for Information Security

ISF

2007

The benefits of adopting good practice

Organisations adopting good practice can:

- Improve their information security policies, standards and procedures
- Measure the effectiveness of information security across the organisation
- Raise awareness of information security enterprise-wide
- Develop or improve information security controls
- Comply with internal and external information security requirements
- Undertake information risk analysis of important applications and systems.

INFORMATION SECURITY FORUM

The Standard of Good Practice for Information Security

ISF

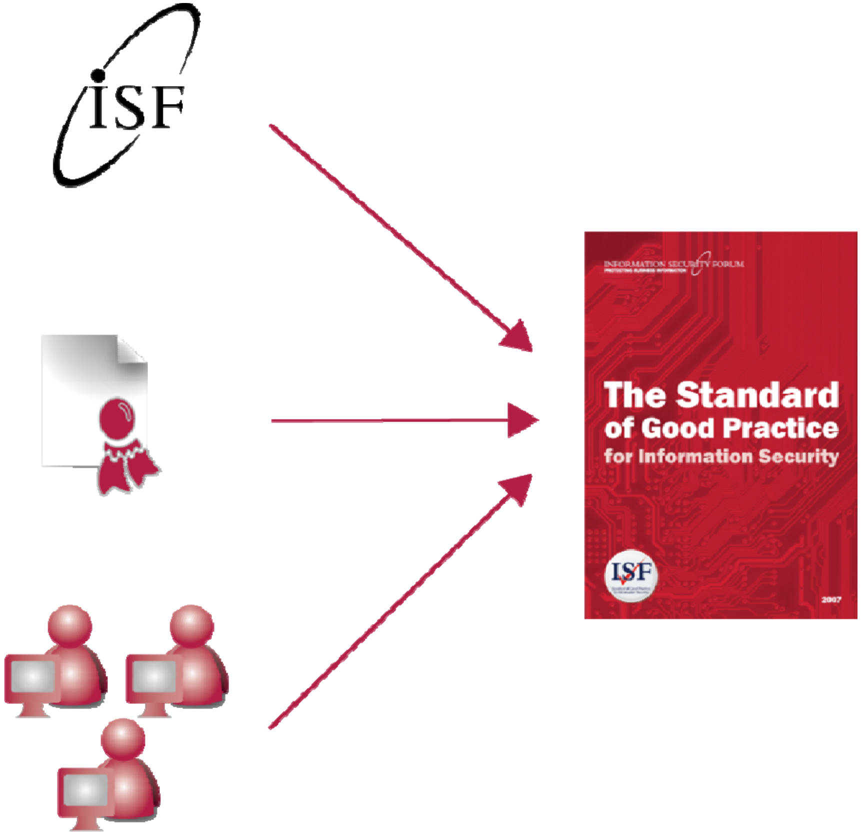
2007

How the standard is put together

An extensive work programme involving the expertise of a full-time ISF Management Team, that performs comprehensive research into hot topics in information security, produces reports, tools and methodologies, and maintains strategic projects such as the ISF's Information Risk Analysis Methodology (IRAM).

Analysis and integration of information security-related standards (eg ISO 27002 and COBIT v4.1), and legal and regulatory requirements (eg Sarbanes-Oxley Act 2002, Payment Card Industry (PCI) Data Security Standard, Basel II 1998, and the EU Directive on Data Protection).

The involvement of ISF Members, using techniques such as workshops, face-to-face meetings and interviews, and the results of the ISF's Information Security Status Survey.


ISF
INFORMATION SECURITY FORUM
The Standard of Good Practice for Information Security
ISF
2007

A look into the future

Why look into the future?

In order to understand how good practice should change in the future we need to understand what threats that we will face in the future and how we should respond to them.

The ISF call this the

Threat Horizon

What is the threat horizon?

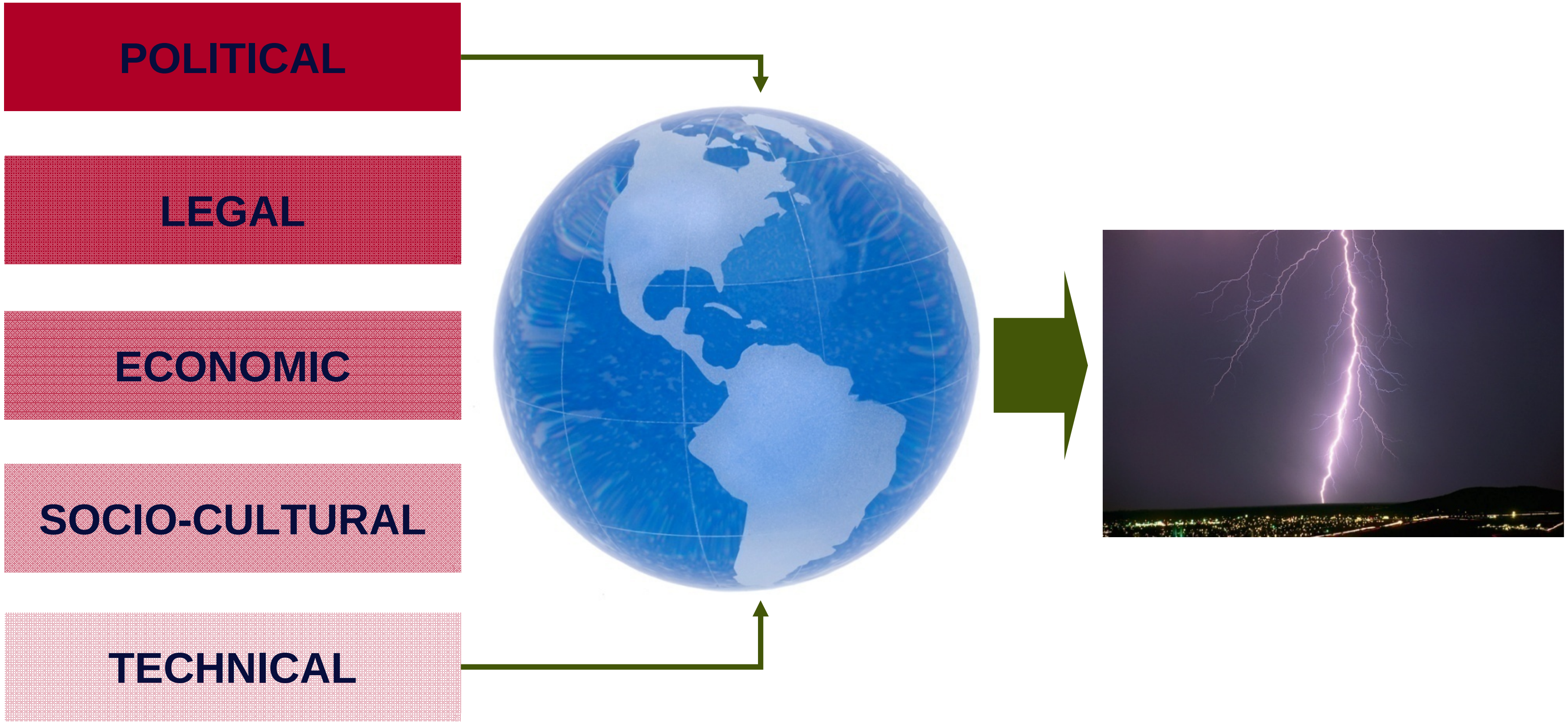
A report that...

- identifies new and changing threats that are likely to impact information security over the next 24 months
- is written for both information security **and** business audiences
- informs information security strategy.

Threat Horizon Supplement
Threat Horizon 2010
Threat Horizon 2011
2006
2008
2009

Threat horizon methodology

Consider the world of the future and how this may give rise to information security threats



POLITICAL

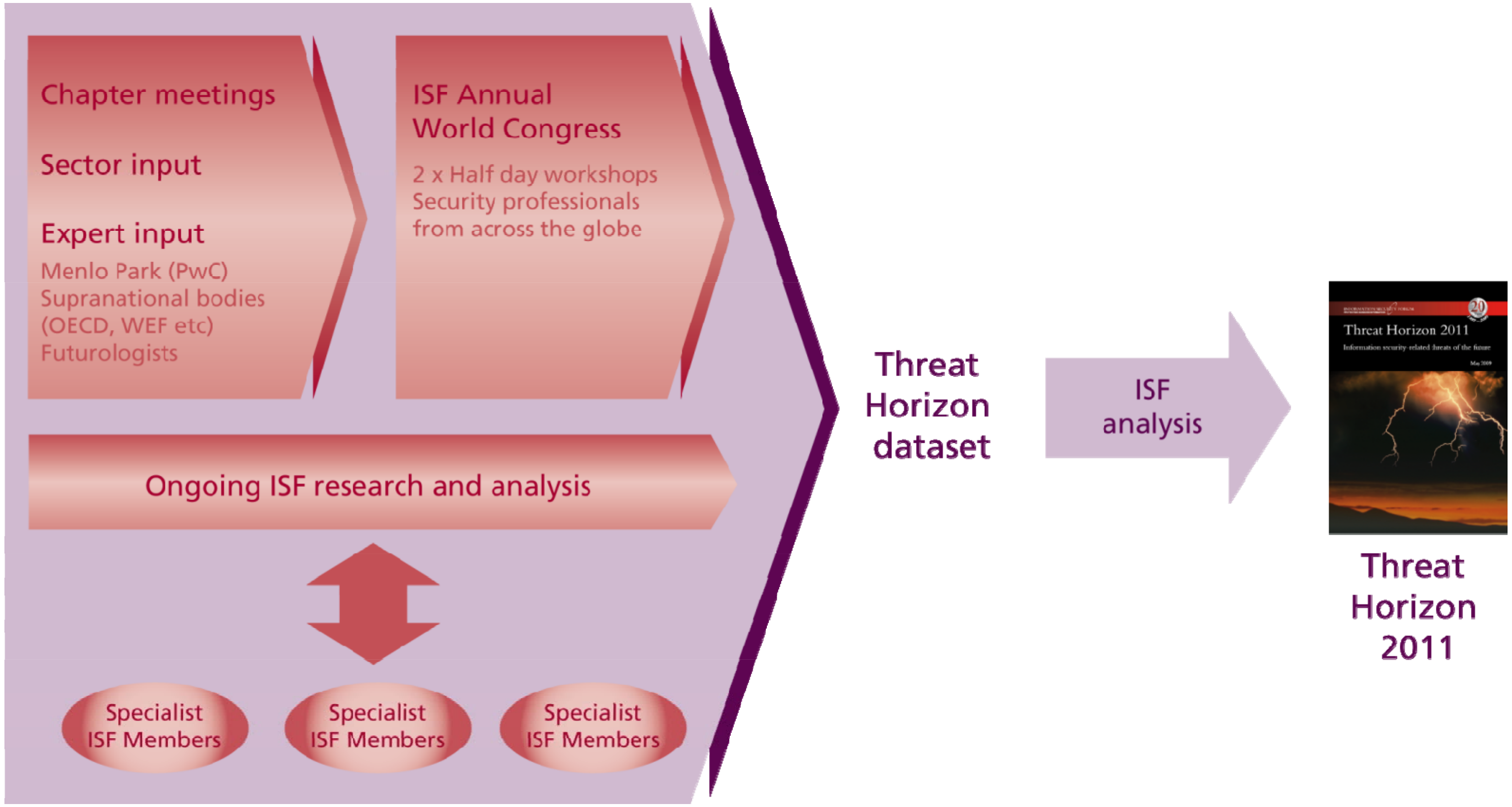
LEGAL

ECONOMIC

SOCIO-CULTURAL

TECHNICAL

Threat horizon framework



Chapter meetings

Sector input

Expert input

Menlo Park (PwC)
Supranational bodies
(OECD, WEF etc)
Futurologists

ISF Annual World Congress

2 x Half day workshops
Security professionals
from across the globe

Ongoing ISF research and analysis

Specialist ISF Members

Specialist ISF Members

Specialist ISF Members

Threat Horizon dataset

ISF analysis

Threat Horizon 2011

2006 headlines

Unintentional actions will have the biggest business impacts

It’s not outside… it’s inside as well

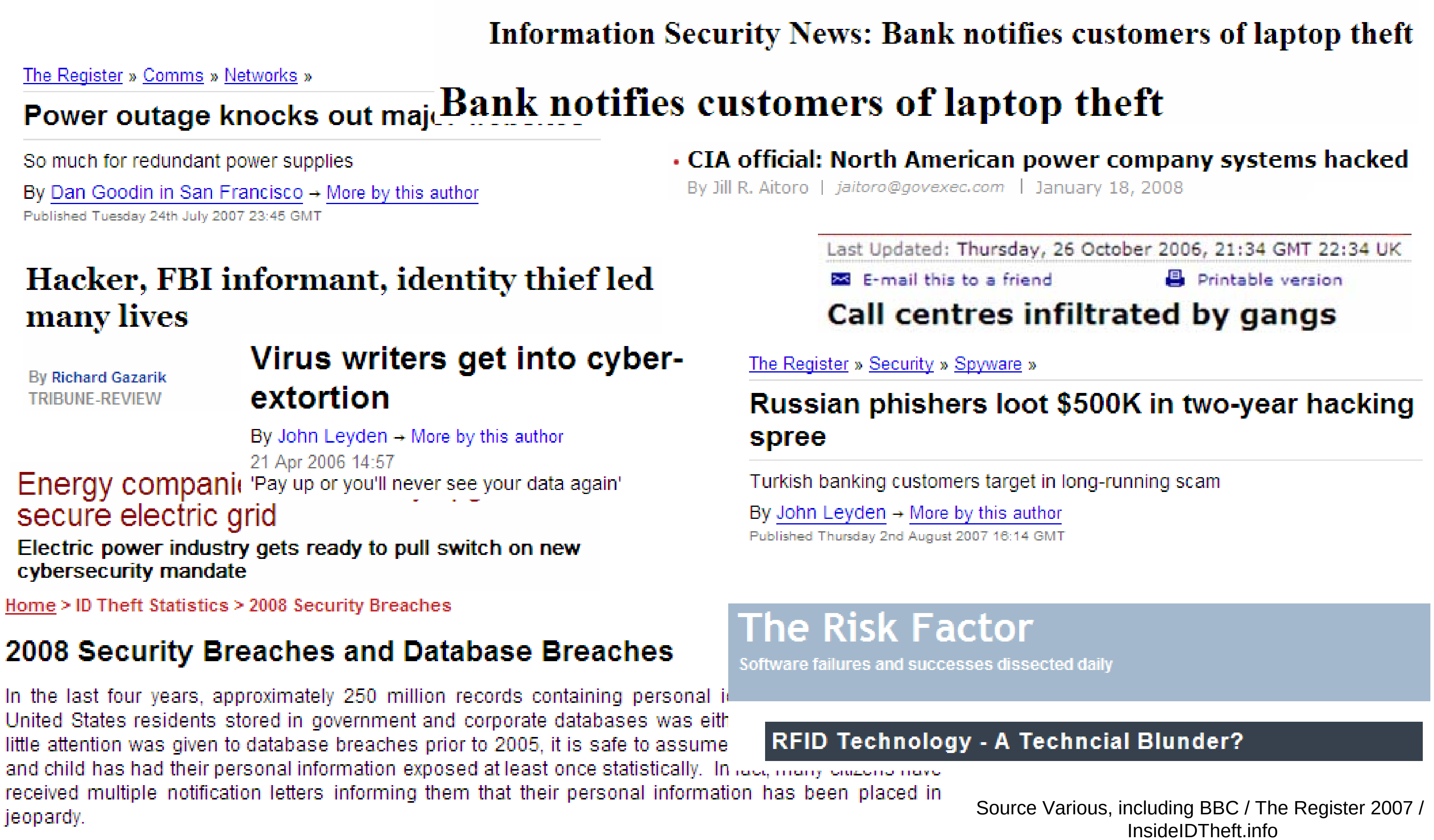
More malware

Organised crime muscles in

Threats aren’t single anymore… they’re clustered

Look both ways – inside and out to the near horizon

And here's the proof….



Information Security News: Bank notifies customers of laptop theft

The Register » Comms » Networks »

Power outage knocks out maj

So much for redundant power supplies

By Dan Goodin in San Francisco → More by this author

Published Tuesday 24th July 2007 23:45 GMT

Bank notifies customers of laptop theft

- CIA official: North American power company systems hacked

By Jill R. Aitoro | jaitoro@govexec.com | January 18, 2008

Last Updated: Thursday, 26 October 2006, 21:34 GMT 22:34 UK

E-mail this to a friend Printable version

Call centres infiltrated by gangs

Hacker, FBI informant, identity thief led many lives

By Richard Gazarik
TRIBUNE-REVIEW

Virus writers get into cyber-extortion

By John Leyden → More by this author

21 Apr 2006 14:57

'Pay up or you'll never see your data again'

Energy compani
secure electric grid

Electric power industry gets ready to pull switch on new cybersecurity mandate

The Register » Security » Spyware »

Russian phishers loot $500K in two-year hacking spree

Turkish banking customers target in long-running scam

By John Leyden → More by this author

Published Thursday 2nd August 2007 16:14 GMT

Home > ID Theft Statistics > 2008 Security Breaches

2008 Security Breaches and Database Breaches

In the last four years, approximately 250 million records containing personal i United States residents stored in government and corporate databases was eith little attention was given to database breaches prior to 2005, it is safe to assume and child has had their personal information exposed at least once statistically. In received multiple notification letters informing them that their personal information has been placed in jeopardy.

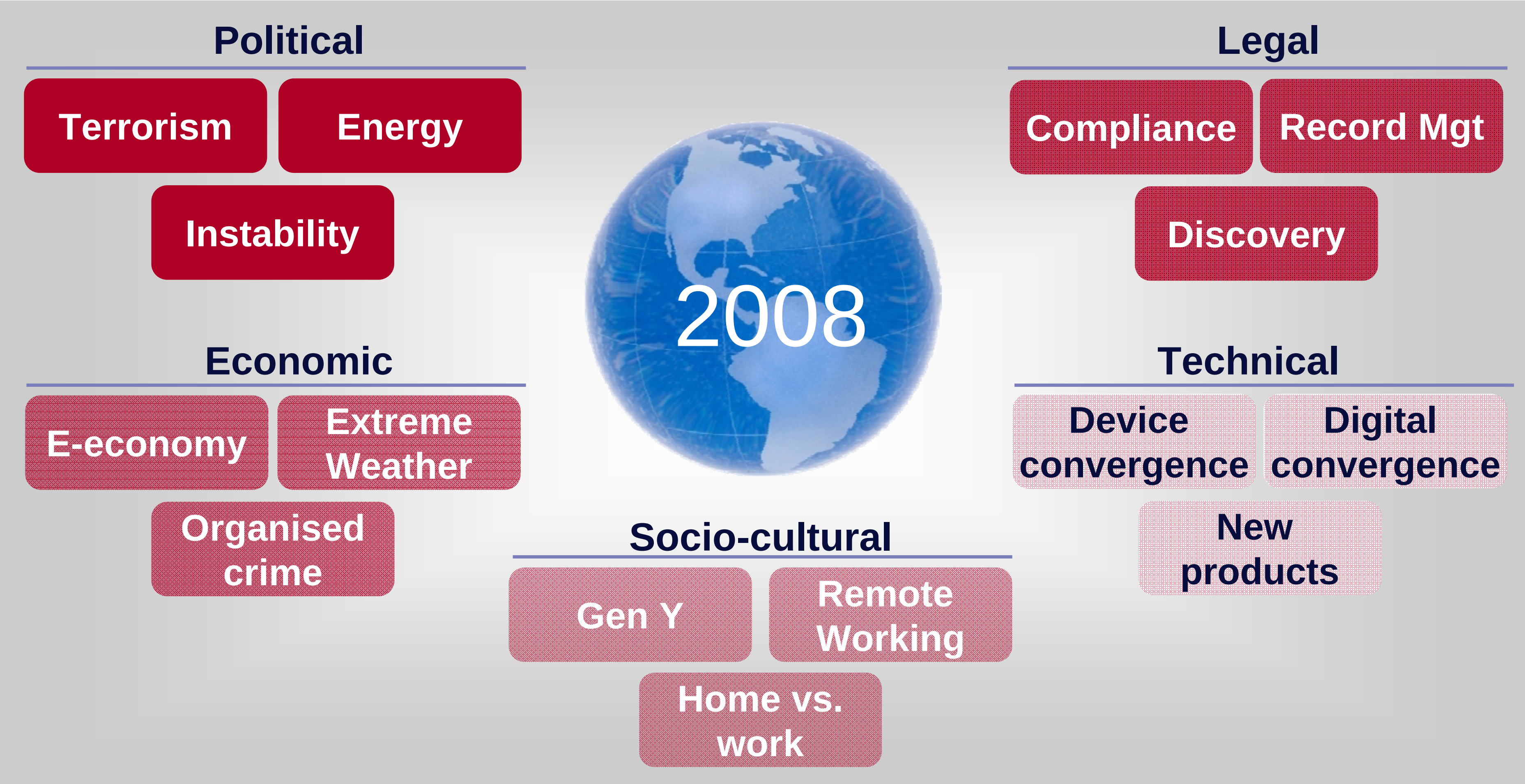
The Risk Factor

Software failures and successes dissected daily

RFID Technology - A Techncial Blunder?

Source Various, including BBC / The Register 2007 / InsideIDTheft.info

2006 predictions for 2008



Political

Terrorism

Energy

Instability

Legal

Compliance

Record Mgt

Discovery

2008

Economic

E-economy

Extreme Weather

Organised crime

Technical

Device convergence

Digital convergence

New products

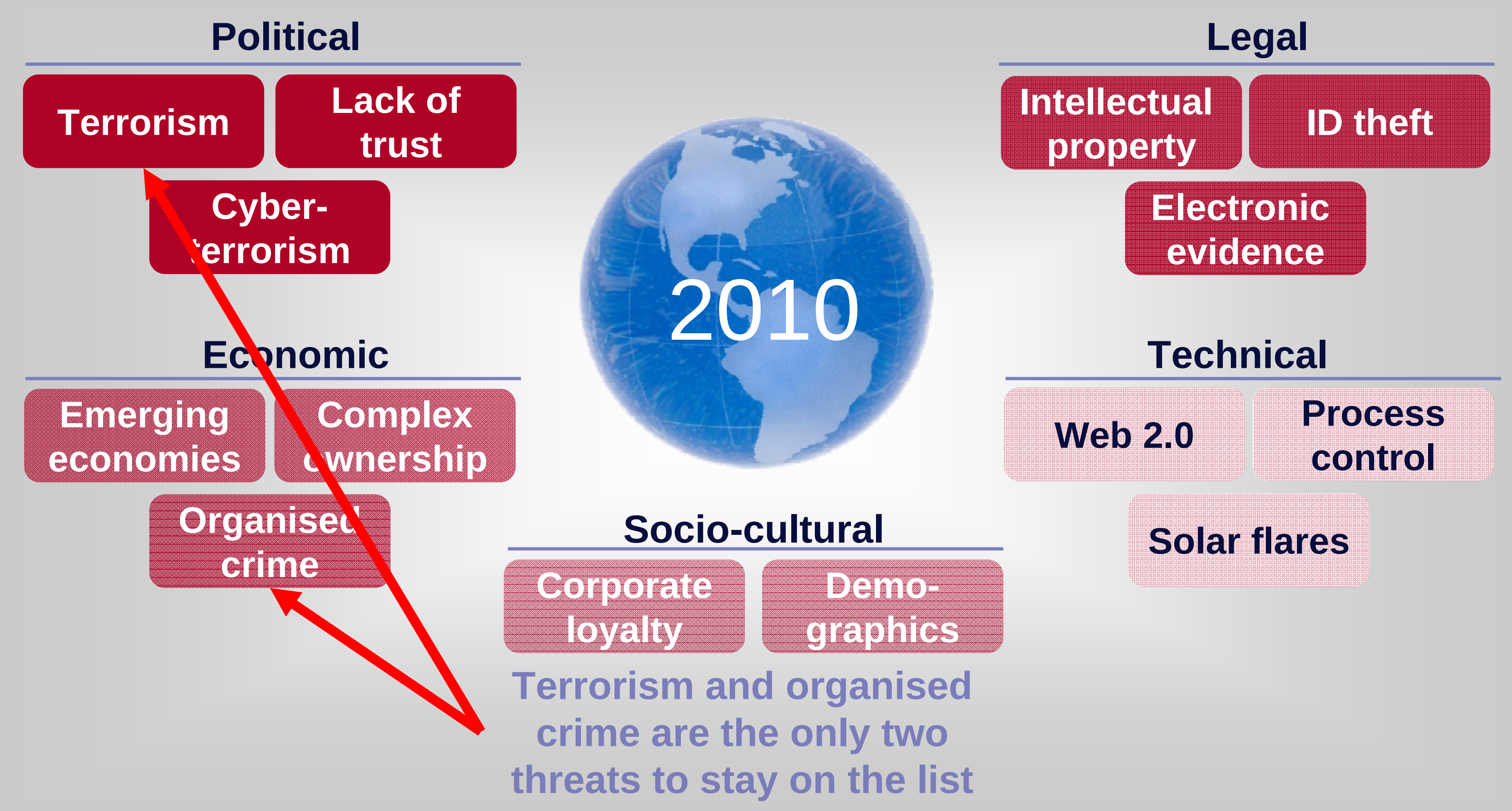
Socio-cultural

Gen Y

Remote Working

Home vs. work

2008 for 2010… What changed?



Political

Terrorism

Lack of trust

Cyber-terrorism

Economic

Emerging economies

Complex ownership

Organised crime

Legal

Intellectual property

ID theft

Electronic evidence

Technical

Web 2.0

Process control

Solar flares

Socio-cultural

Corporate loyalty

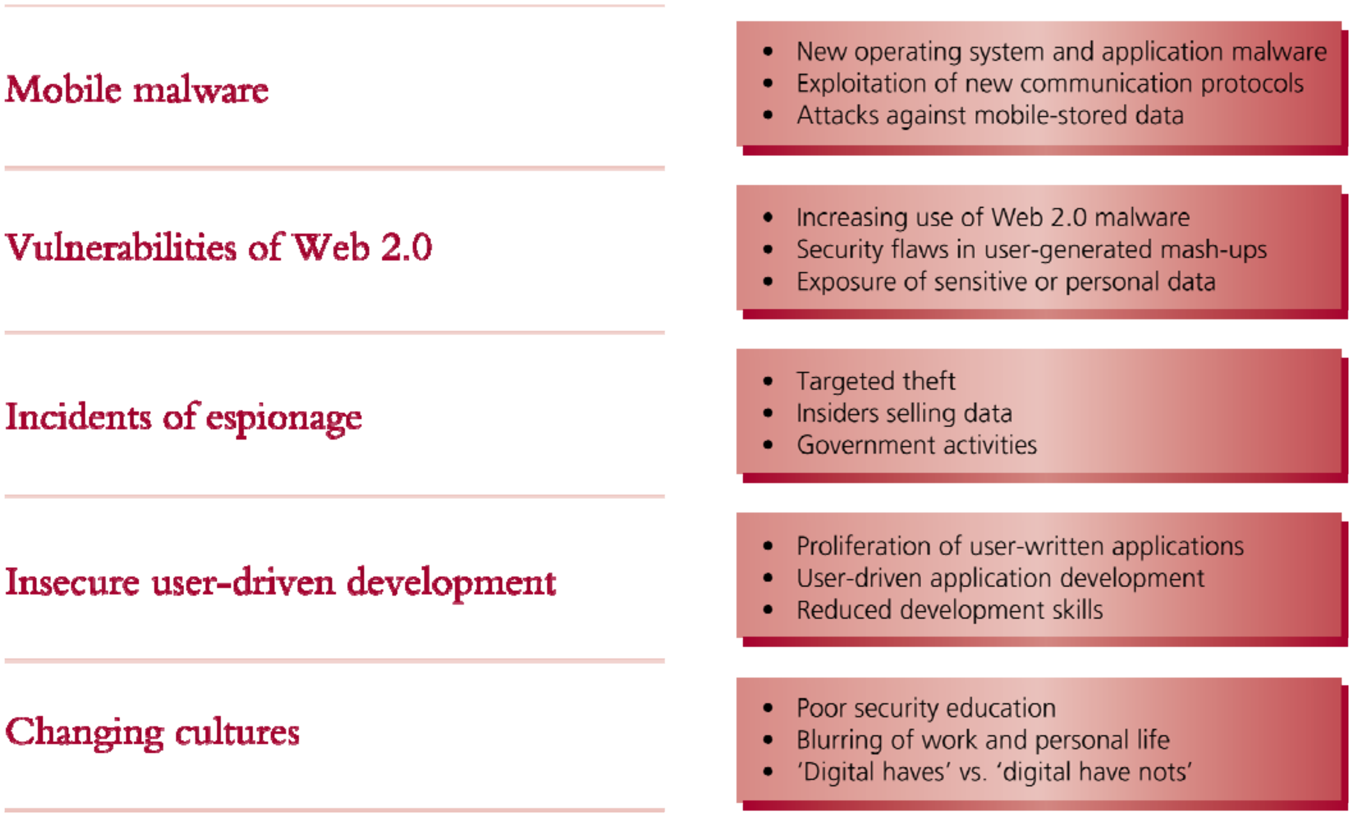
Demo-graphics

Terrorism and organised crime are the only two threats to stay on the list

The threats of 2010

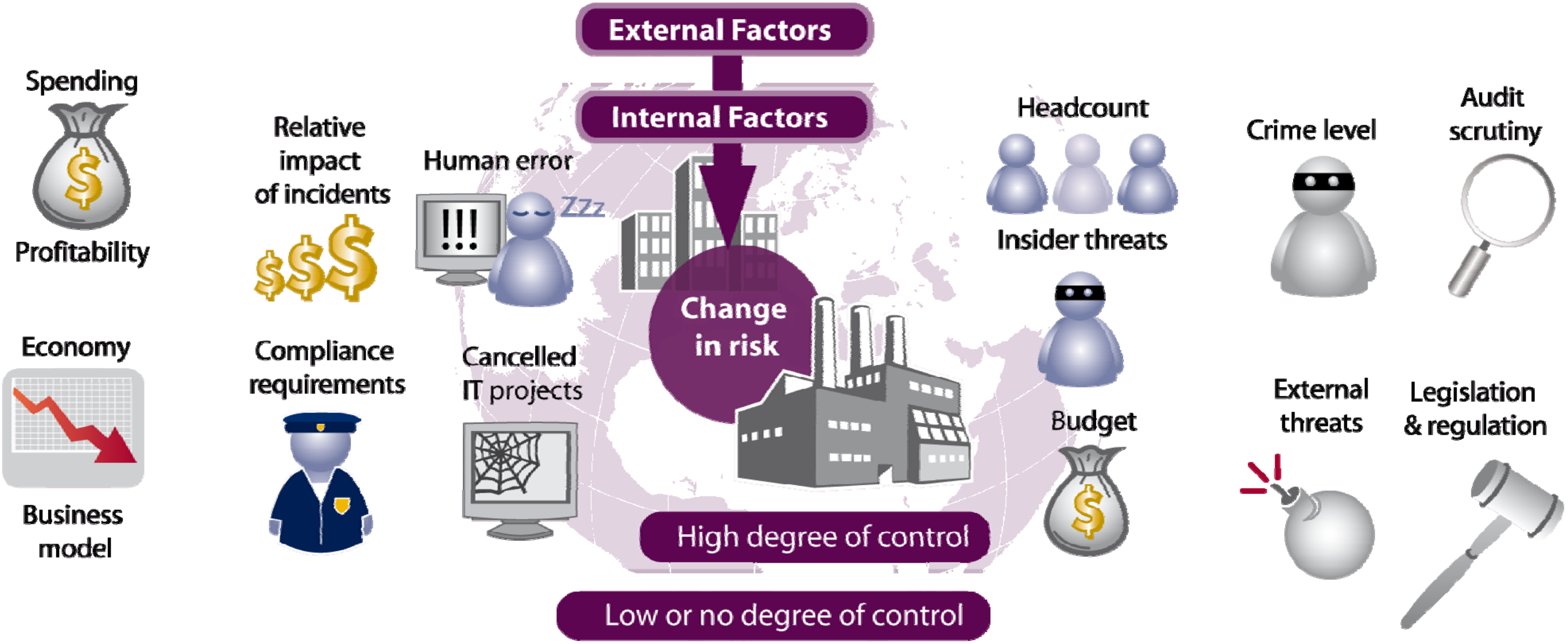
Criminal attacks	• Crimeware as a service • Attacks by disgruntled employees • Infiltration of organisations
Weaknesses in infrastructure	• Reduced investment • *Complexity and integration* • Increase in zero-day attacks • Reliance on third parties for upgrades
Tougher statutory environment	• Greater emphasis on privacy • Incompatible laws • Stronger regulation and punishment
Pressures on offshoring / outsourcing	• Drive to outsource business operations *and information security* • Difficulties meeting compliance requirements • Instability of providers
Eroding network boundaries	• Adoption of cloud computing • Proliferation of connections • Bypass of defences by malware

The threats of 2010

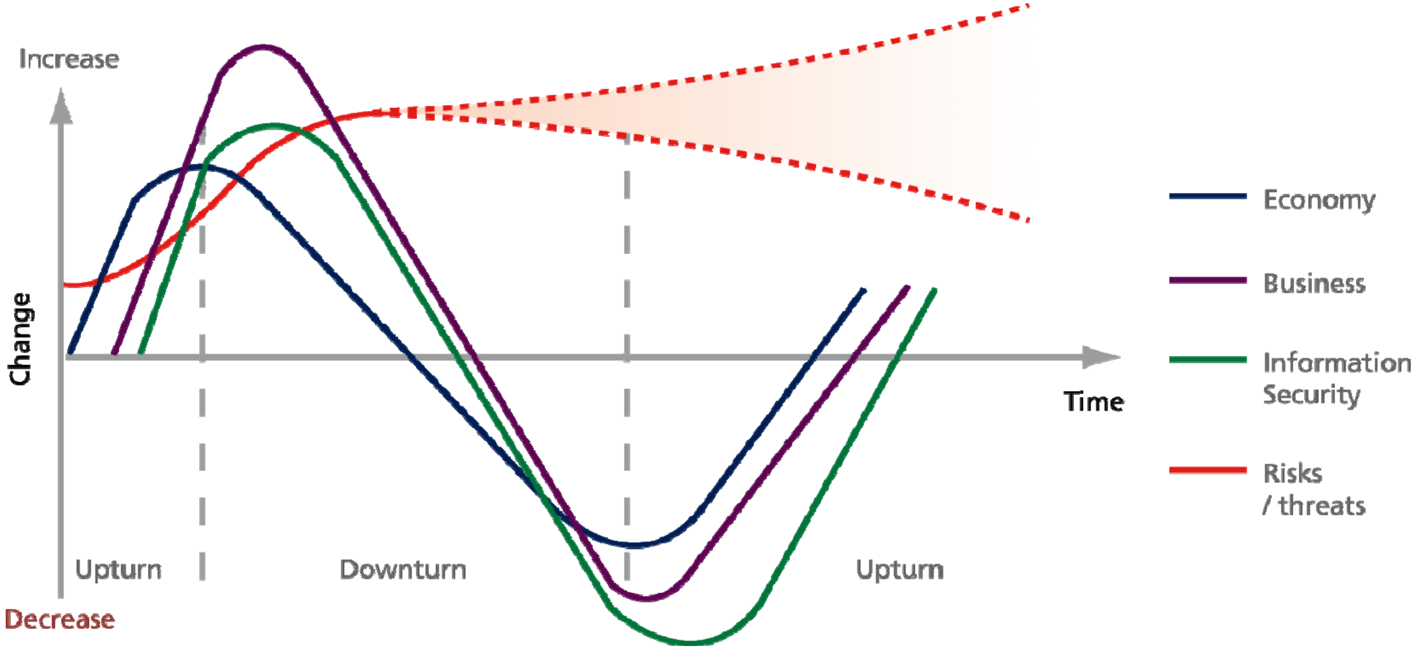


Mobile malware	- New operating system and application malware - Exploitation of new communication protocols - Attacks against mobile-stored data
Vulnerabilities of Web 2.0	- Increasing use of Web 2.0 malware - Security flaws in user-generated mash-ups - Exposure of sensitive or personal data
Incidents of espionage	- Targeted theft - Insiders selling data - Government activities
Insecure user-driven development	- Proliferation of user-written applications - User-driven application development - Reduced development skills
Changing cultures	- Poor security education - Blurring of work and personal life - ‘Digital haves’ vs. ‘digital have nots’

The impact of the credit crunch



Succeeding in the new world order...



How good practice should evolve

Responding to the threat horizon

Information security controls that defend against threats are:

Often part of a wide infrastructure project (eg firewall, network segregation)

Sometimes difficult to justify to the business

AND

Sometime can take years to plan and deliver

THEREFORE

We need to start to plan controls for future threats NOW!

What do I do now? – at a strategic level

Re-assess the risks to your organisation and its information

- Inside and outside…

Change your thinking about threats

- Don’t rely on trends or historical data

Revise your information security arrangements

- Question ‘security as usual’

Focus on the basics

- That includes people, not just technology!

Prepare for the future

- Be ready to support initiatives such as cloud computing

What do I do now? – at a practical level

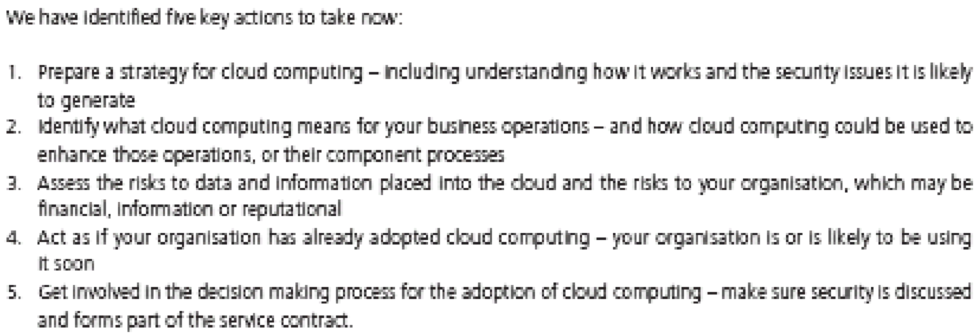
The ISF has produced recent research reports on these topics:

- Cloud computing
- Social networking
- Third party security
- Risk convergence
- Privacy
- Encryption
- Risk reporting
- Security audits

Social engineering
Solving the data privacy puzzle
Achieving compliance
Security Implications of Cloud Computing
Risk Convergence
Outsourcing and Third Party Risk Management – ISF deliverables

What do I do now? – at a practical level

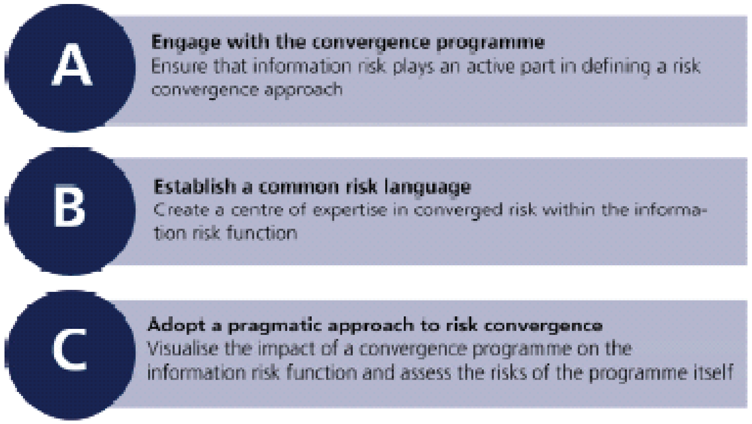
With recommendations such as:



We have identified five key actions to take now:

1. Prepare a strategy for cloud computing – including understanding how it works and the security issues it is likely to generate
2. Identify what cloud computing means for your business operations – and how cloud computing could be used to enhance those operations, or their component processes
3. Assess the risks to data and information placed into the cloud and the risks to your organisation, which may be financial, information or reputational
4. Act as if your organisation has already adopted cloud computing – your organisation is or is likely to be using it soon
5. Get involved in the decision making process for the adoption of cloud computing – make sure security is discussed and forms part of the service contract.

Figure 6: Summary of steps towards convergence



A

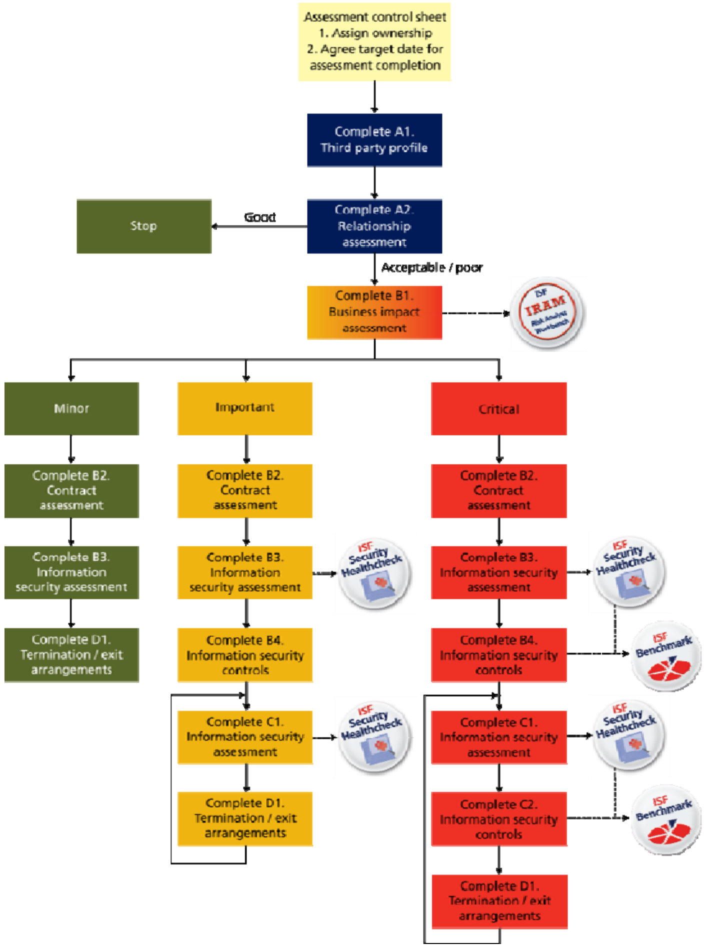
Engage with the convergence programme
Ensure that information risk plays an active part in defining a risk convergence approach

B

Establish a common risk language
Create a centre of expertise in converged risk within the information risk function

C

Adopt a pragmatic approach to risk convergence
Visualise the impact of a convergence programme on the information risk function and assess the risks of the programme itself



Assessment control sheet
1. Assign ownership
2. Agree target date for assessment completion

Complete A1. Third party profile

Complete A2. Relationship assessment

Good

Stop

Acceptable / poor

Complete B1. Business impact assessment

Minor

Complete B2. Contract assessment

Complete B3. Information security assessment

Complete D1. Termination / exit arrangements

Important

Complete B2. Contract assessment

Complete B3. Information security assessment

Complete B4. Information security controls

Complete C1. Information security assessment

Complete D1. Termination / exit arrangements

Critical

Complete B2. Contract assessment

Complete B3. Information security assessment

Complete B4. Information security controls

Complete C1. Information security assessment

Complete C2. Information security controls

Complete D1. Termination / exit arrangements

What do I do now? – at a practical level

Which will be incorporated into the next version of

INFORMATION SECURITY FORUM

The Standard of Good Practice for Information Security

ISF

2007

Conclusion

Conclusion

Threats change quickly and in sophisticated and unexpected ways.

To compromise an organisation's information security an attacker needs to find only one way to get around organisational defences.

Information security professionals however, need to think of ALL the ways that this could happen

Good practice in information security includes adopting known good practice, but also predicting future good practice in order to stay ahead of threats

Thank you for your attention

Bill Caughie

Chief Operating Office
E-mail: Bill.Caughie@securityforum.org
Web: www.securityforum.org