Information Security Forum

Information security and risk management: key challenges for security professionals in 2011

Steve Durbin

ISF Global Vice President

Tokyo, 25 January 2011

Agenda

1. Introduction to the ISF
2. Key challenges in 2010 (and beyond):
    1. Managing external suppliers
    2. The Cloud
    3. Social Media
3. A look into the future – Threat Horizon
4. Conclusion

An introduction to the ISF

What is the ISF?

An international association of some 300 leading global organisations, which...

- addresses key issues in information risk management through research and collaboration
- develops practical tools and guidance
- is fully independent, not-for-profit organisation and driven by its Members
- promotes networking within its membership

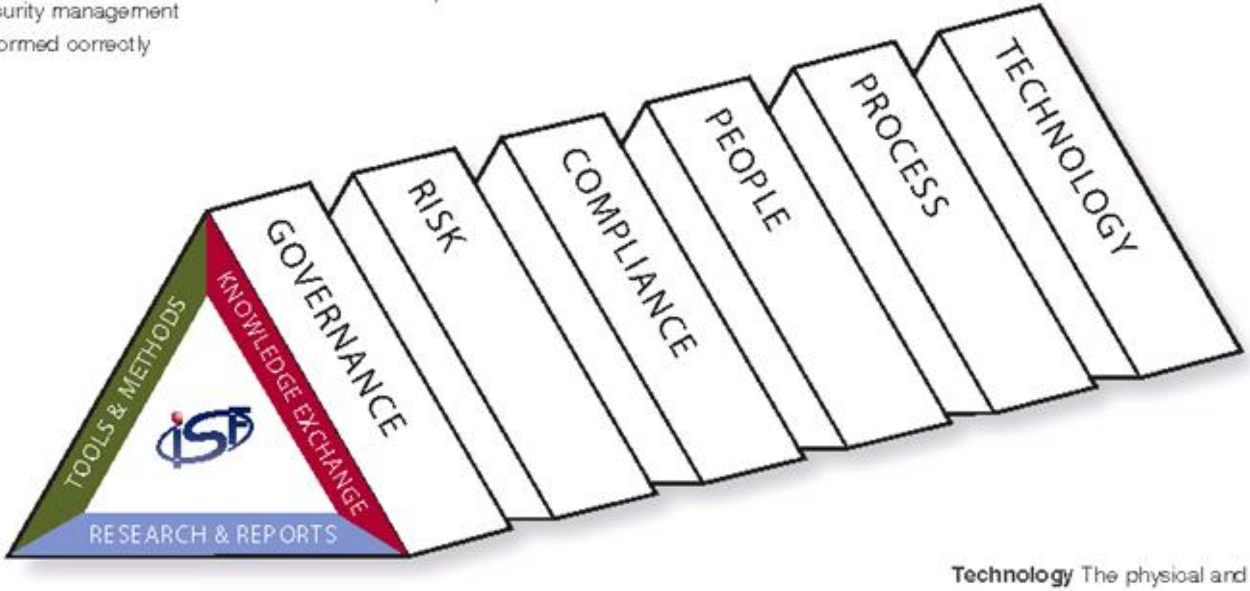
The leading, global authority on information security and information risk management

The ISF Security Model

Governance The framework by which policy and direction is set, providing senior management with assurance that security management activities are being performed correctly and consistently.

Risk The potential business impact and likelihood of particular threats materialising – and the application of control to mitigate risk to acceptable levels.

Compliance The policy, statutory and contractual obligations relevant to information security which must be met to operate in today's business world to avoid civil or criminal penalties and mitigate risk.

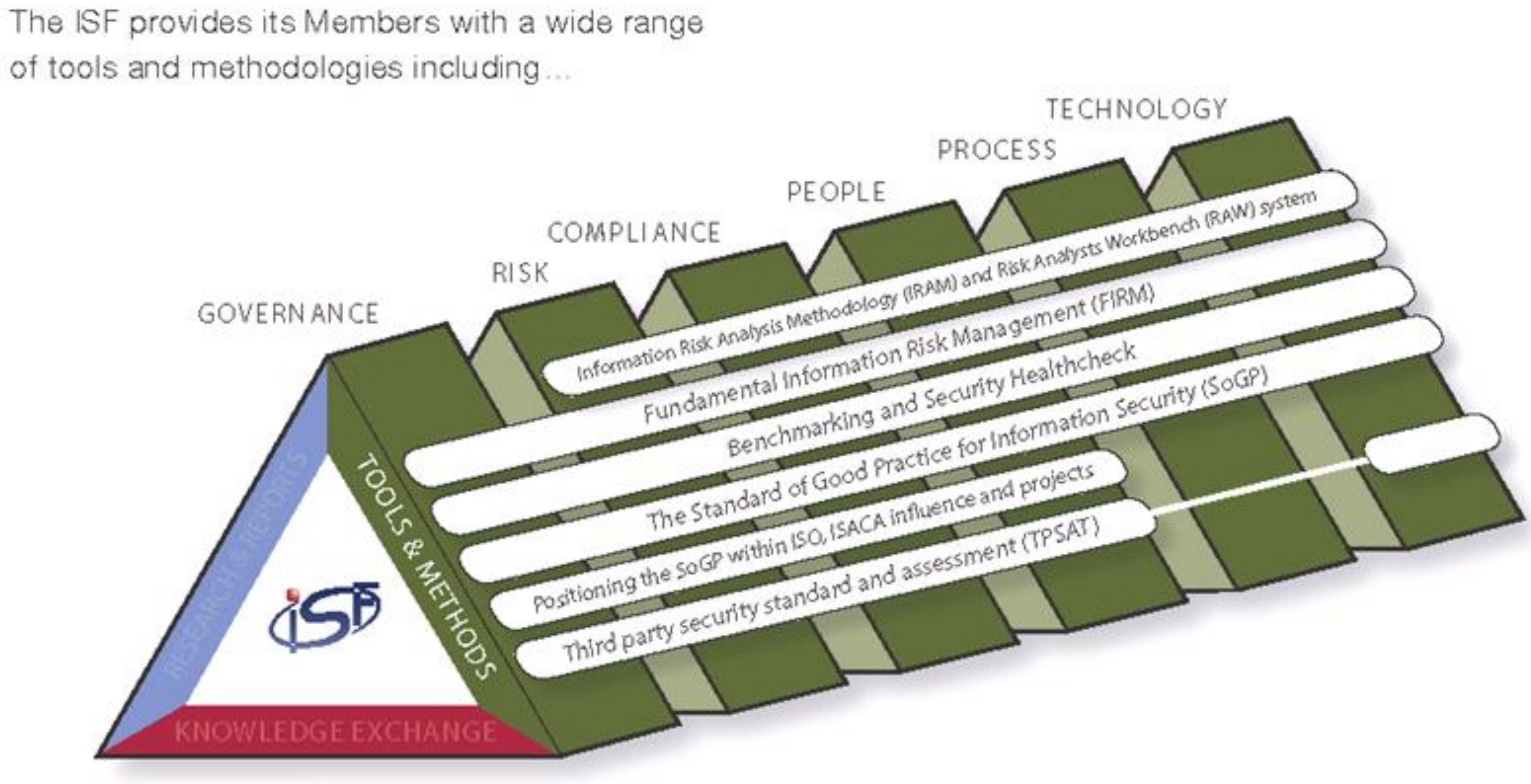


People The executives, staff and third parties with access to information, who need to be aware of their Information Security responsibilities and requirements and whose access to systems and data need to be managed.

Process Business processes, applications and data that support the operations and decision making.

Technology The physical and technical infrastructure, including networks and end points, required to support the successful deployment of secure processes.

The Tools and Methods that ISF provides



The ISF provides its Members with a wide range of tools and methodologies including…

Information Risk Analysis Methodology (IRAM) and Risk Analysts Workbench (RAW) system

Fundamental Information Risk Management (FIRM)

Benchmarking and Security Healthcheck

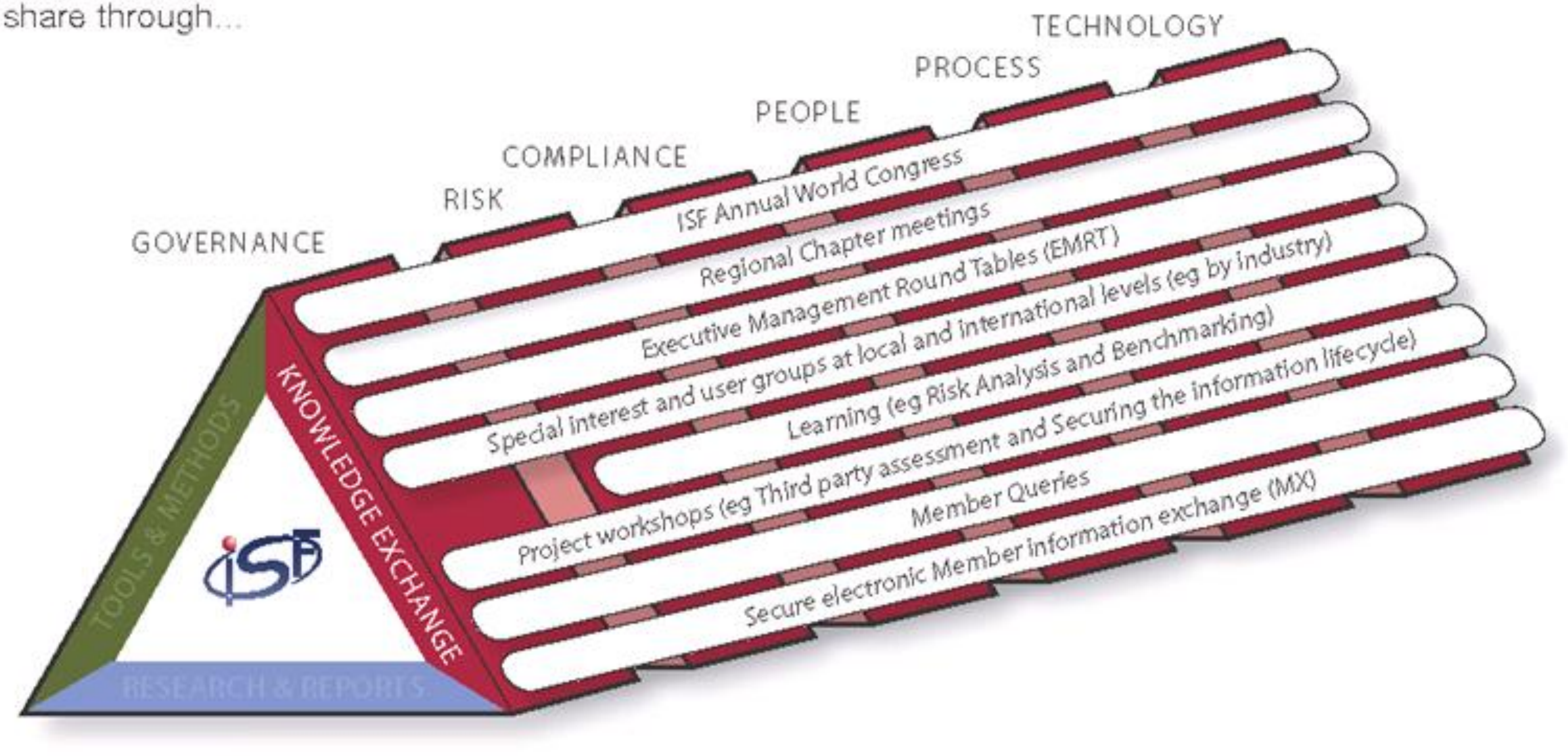
The Standard of Good Practice for Information Security (SoGP)

Positioning the SoGP within ISO, ISACA influence and projects

Third party security standard and assessment (TPSAT)

How the ISF provides Knowledge and Networks Exchange

The ISF brings Members together to network and share through...



GOVERNANCE

RISK

COMPLIANCE

PEOPLE

PROCESS

TECHNOLOGY

- ISF Annual World Congress
- Regional Chapter meetings
- Executive Management Round Tables (EMRT)
- Special interest and user groups at local and international levels (eg by industry)
- Learning (eg Risk Analysis and Benchmarking)
- Project workshops (eg Third party assessment and Securing the information lifecycle)
- Member Queries
- Secure electronic Member information exchange (MX)

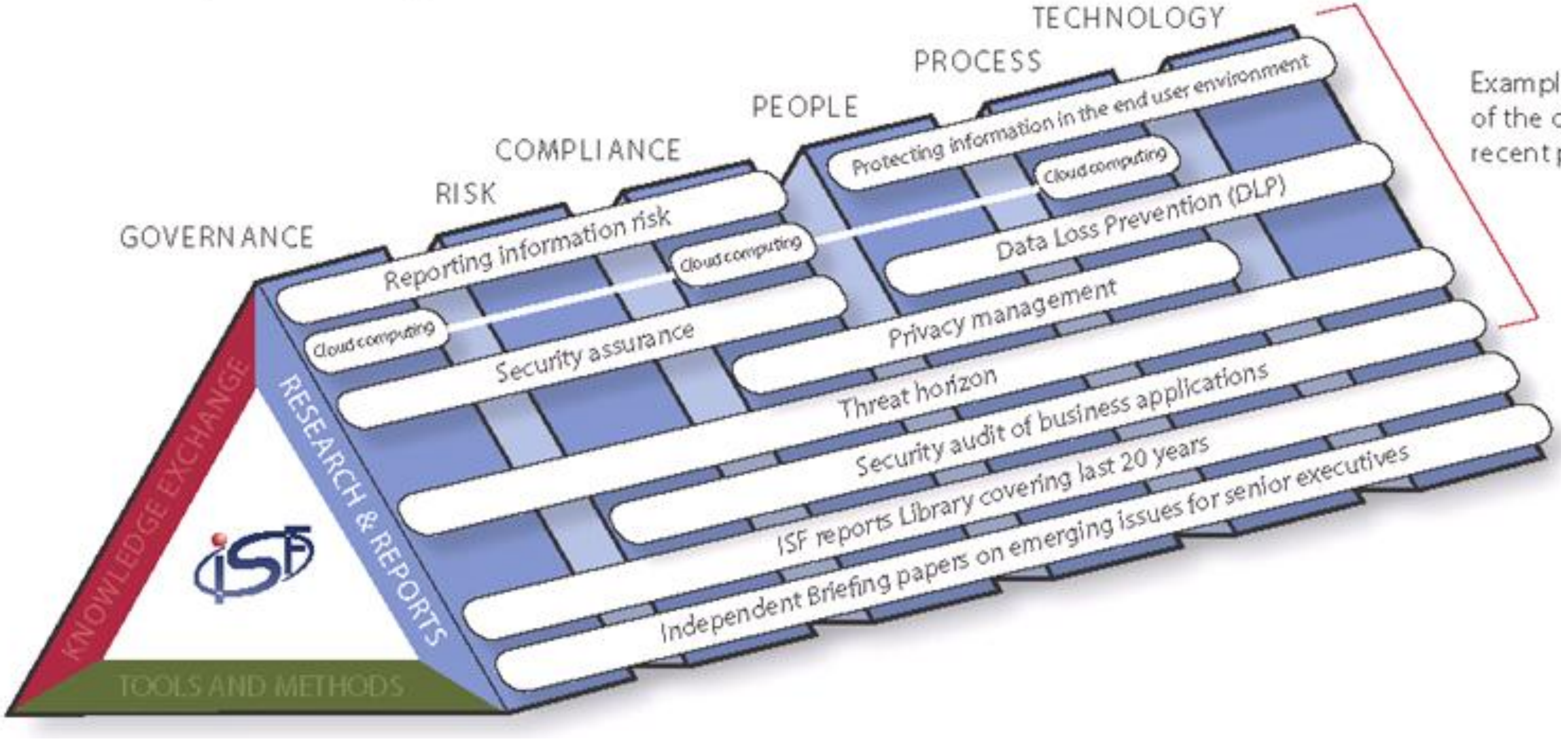
KNOWLEDGE EXCHANGE

TOOLS & METHODS

RESEARCH & REPORTS

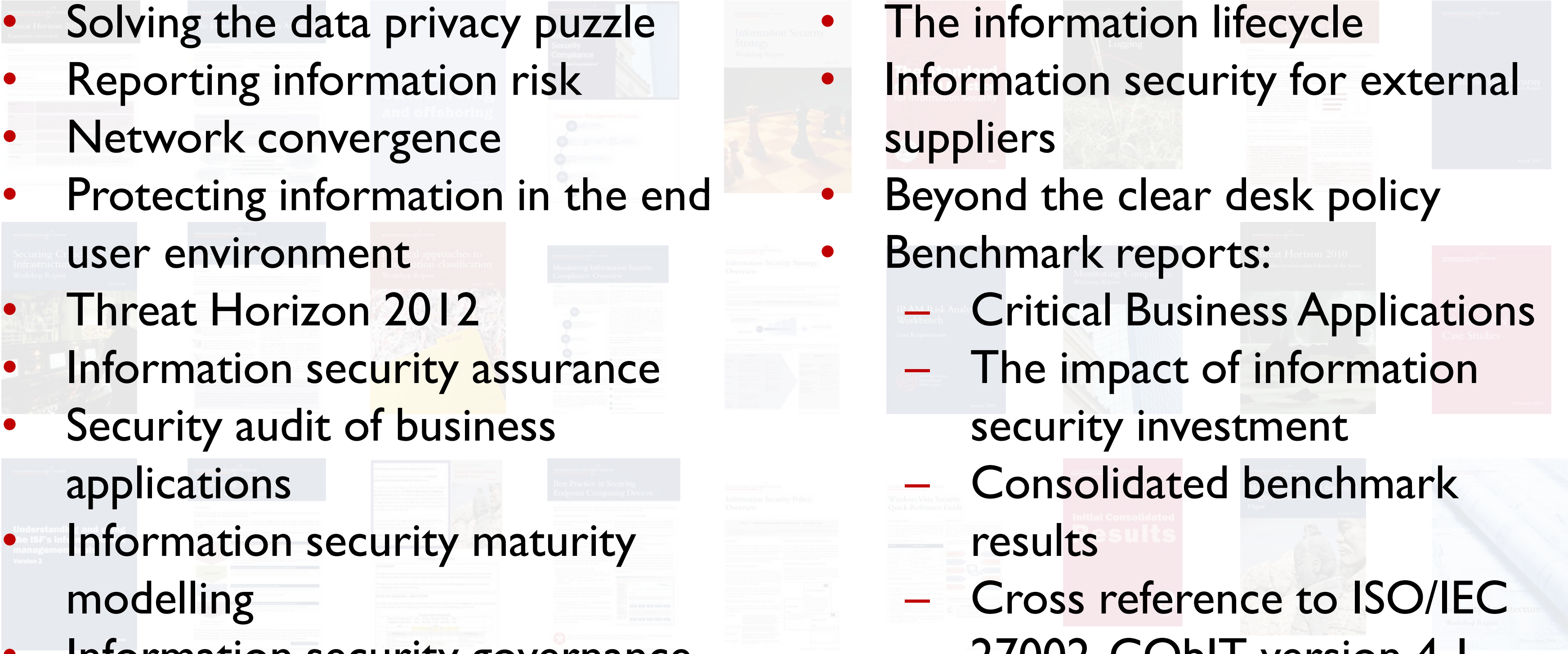
The Research and Reports that ISF provides

The ISF provides its Members with a wide range of research and reports including…


GOVERNANCE
RISK
COMPLIANCE
PEOPLE
PROCESS
TECHNOLOGY
Protecting information in the end user environment
Cloud computing
Reporting information risk
Cloud computing
Data Loss Prevention (DLP)
Cloud computing
Security assurance
Privacy management
Threat horizon
Security audit of business applications
ISF reports Library covering last 20 years
Independent Briefing papers on emerging issues for senior executives
KNOWLEDGE EXCHANGE
RESEARCH & REPORTS
TOOLS AND METHODS
iSF

Examples of some of the current and recent project topics

Research & reports over the past 12 months



- Solving the data privacy puzzle
- Reporting information risk
- Network convergence
- Protecting information in the end user environment
- Threat Horizon 2012
- Information security assurance
- Security audit of business applications
- Information security maturity modelling
- Information security governance
- Information security principles
- The information lifecycle
- Information security for external suppliers
- Beyond the clear desk policy
- Benchmark reports:
  - Critical Business Applications
  - The impact of information security investment
  - Consolidated benchmark results
  - Cross reference to ISO/IEC 27002, CObIT version 4.1

The 2011 work programme (as at Q1)

Workshop-based research and development projects:

- Cloud computing – Avoiding the seven deadly sins
- Organisational Governance

Research based projects:

- Consumerisation: Securing the next generation of end user environment
- Threat Horizon 2013
- Standard of Good Practice update

Information risk management tools:

- Information Risk Analysis Methodology - Risk Analyst's Workbench v1.0

Briefing Papers:

- Cyber citizenship

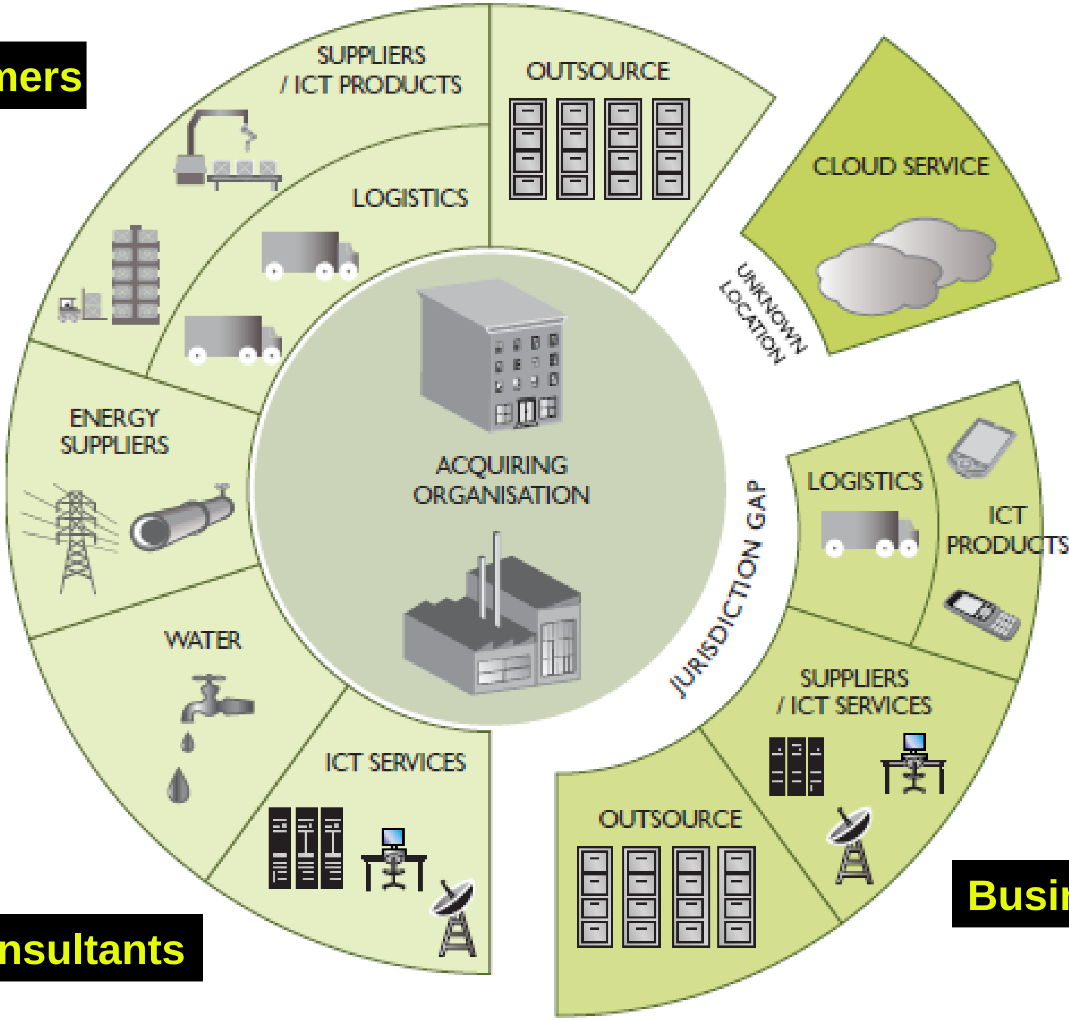
Training workshops:

- Information Risk Analysis Methodology (IRAM)
- Protecting information in the end user environment
- Security audit of business applications

Key challenges in 2010:

External suppliers

External suppliers – a visual representation



Customers

Manufacturers

Distributors

Competitors

Consultants

Outsourcers

Regulators

Suppliers

Joint ventures

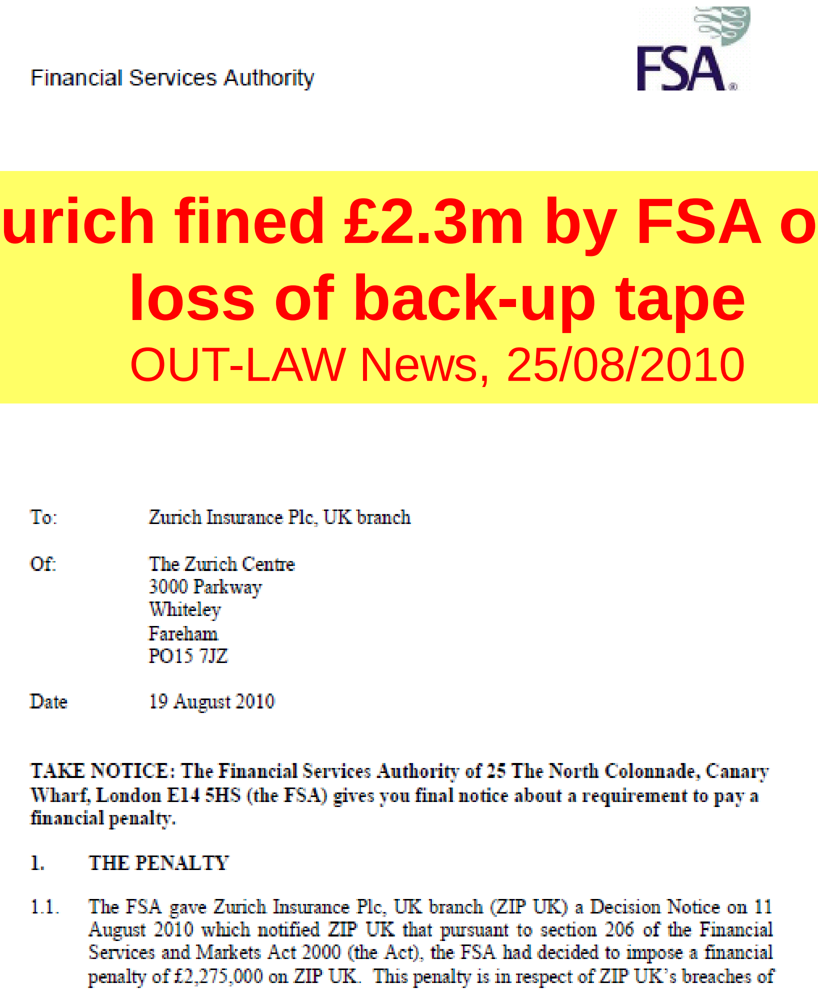
Business partner

Statutory obligations

- Legal and regulatory oversight of data and information is getting stronger
- Organisations are liable even if they did not lose or disclose information
- Third party organisations need to show they will not endanger their clients

Zurich fined £2.3m by FSA over loss of back-up tape

OUT-LAW News, 25/08/2010



Financial Services Authority

FSA

To: Zurich Insurance Plc, UK branch

Of: The Zurich Centre
3000 Parkway
Whiteley
Fareham
PO15 7JZ

Date 19 August 2010

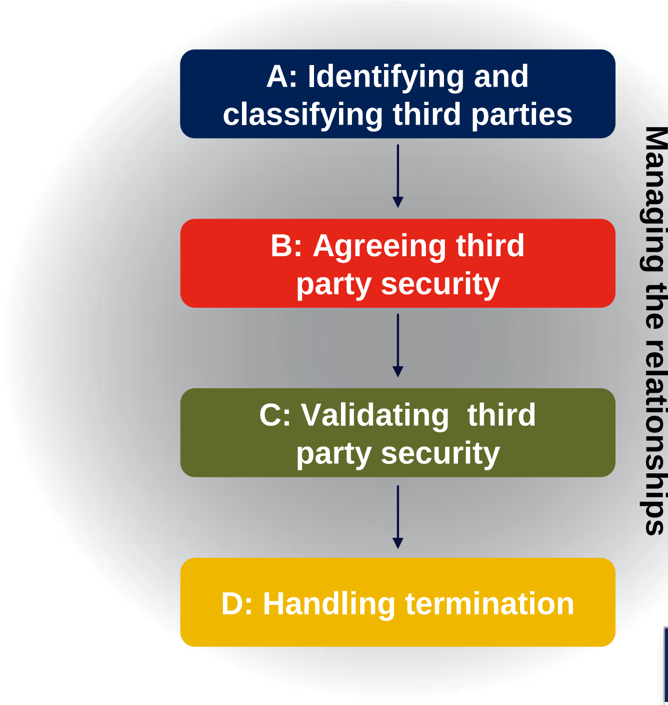
TAKE NOTICE: The Financial Services Authority of 25 The North Colonnade, Canary Wharf, London E14 5HS (the FSA) gives you final notice about a requirement to pay a financial penalty.

1. THE PENALTY

1.1. The FSA gave Zurich Insurance Plc, UK branch (ZIP UK) a Decision Notice on 11 August 2010 which notified ZIP UK that pursuant to section 206 of the Financial Services and Markets Act 2000 (the Act), the FSA had decided to impose a financial penalty of £2,275,000 on ZIP UK. This penalty is in respect of ZIP UK's breaches of

Managing security in external suppliers

- Few tools used to identify and classify third parties
- No ‘agreed’ list of security controls applied to contracts
  - In an organisation
  - By sector / region
- Very little use of current assessment methods / tools (eg BITS, SAS 70)
  - Tools not widely trusted
- Contract termination often handled in an *ad hoc* manner



A: Identifying and classifying third parties

B: Agreeing third party security

C: Validating third party security

D: Handling termination

Managing the relationships

INFORMATION SECURITY FORUM

Information Security in Third Party Relationship Management

The need for a standard…

Member organisations typically work in over 50 jurisdictions

27% of respondents are highly or very highly satisfied about the level of controls implemented by critical third parties

72% of respondents are highly or very highly concerned about third party security arrangements

A typical Member organisation has over 2030 third party relationships

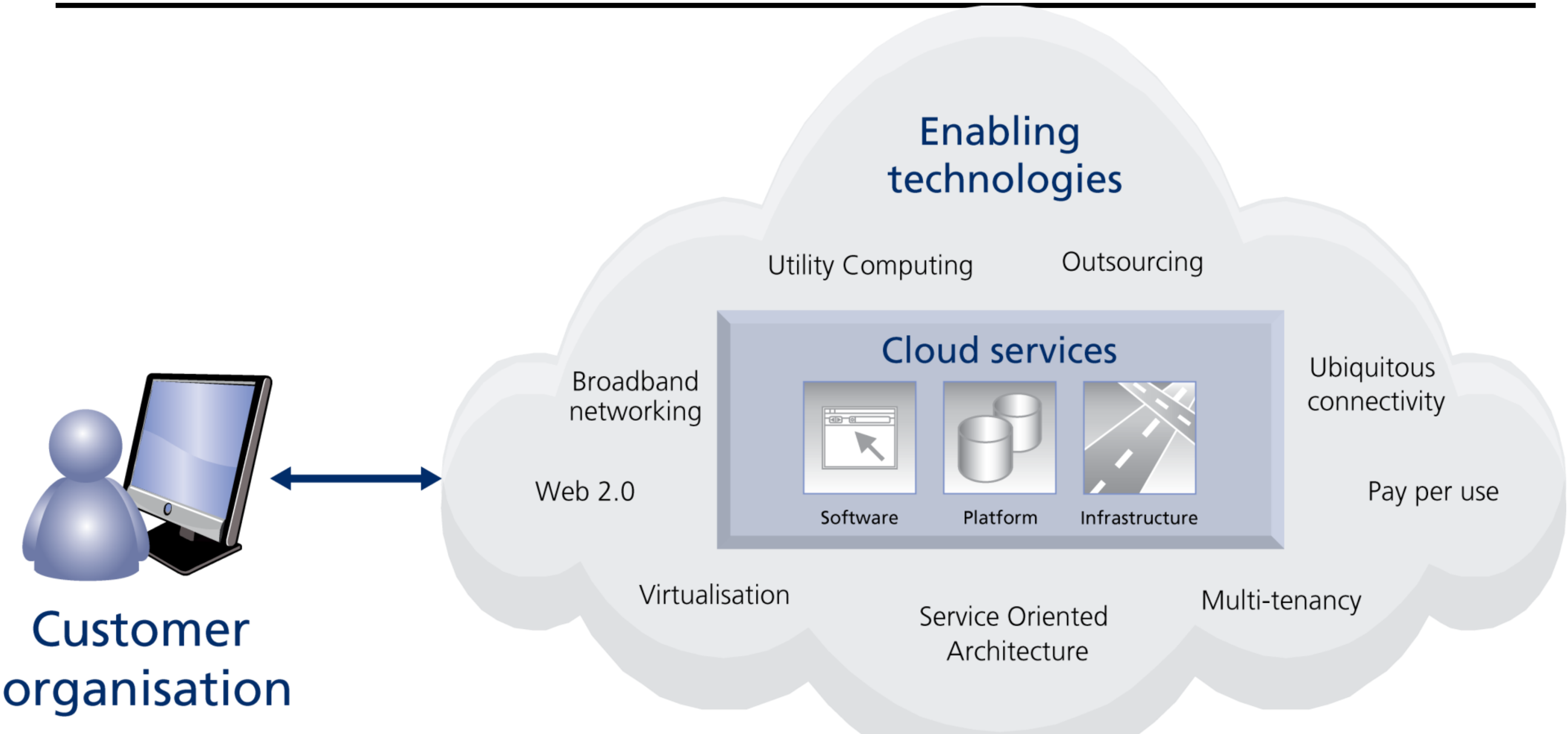
52% of respondents are highly or very highly exposed to third party risks

25% of respondents are highly or very highly satisfied about the level of controls implemented by non-critical third parties

Key Challenges in 2010:

The Cloud

Background: the ISF view of the cloud



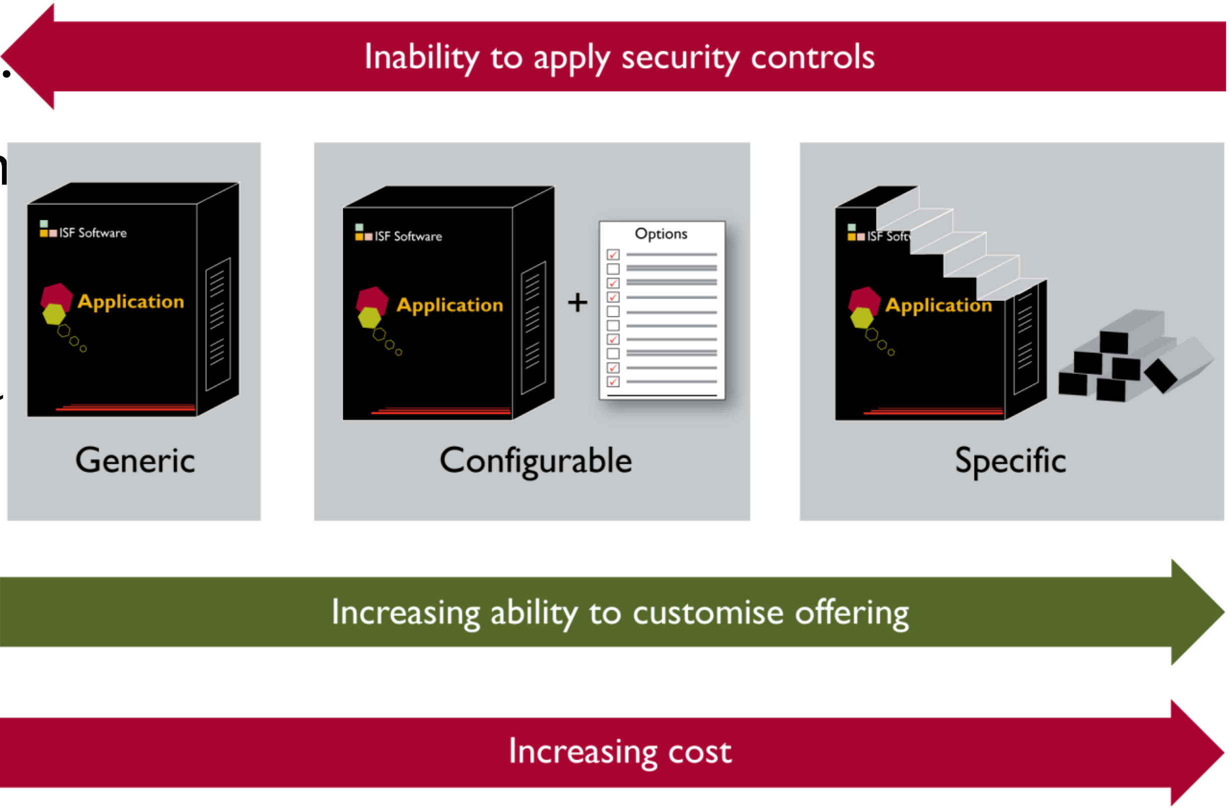
Distributed, on-demand computing services delivered across networks

Background: technical vs. business

- Common model of the cloud – SaaS, PaaS and IaaS - provides a technical perspective
- Misses the ***business*** perspectives:
  - Economics
  - Flexibility / ease of use
  - Accessibility
- Misses how cloud is ***really*** used

Background: how the business views the cloud

- I have a problem...
- ...I need a solution
- Ah-ah! I can buy a ready-made solution (and I don't have to involve IT, procurement or anybody else!)



Inability to apply security controls

Generic

Configurable

Specific

Increasing ability to customise offering

Increasing cost

Do you know what the business is doing?

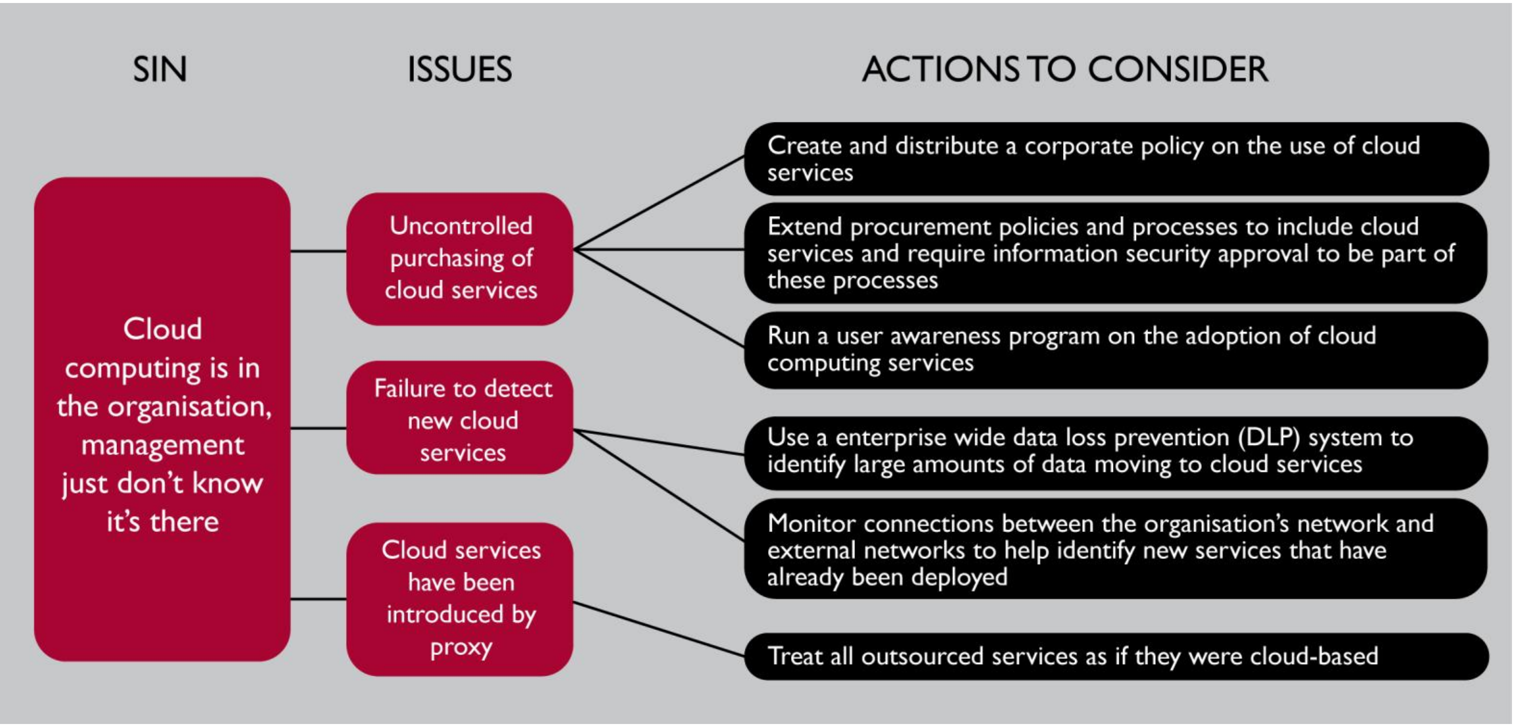
- Will cloud become the new business-critical spreadsheet?
- Cost of entry for cloud deployments can be zero
- On-going costs for a small department will fall within credit card authority limits
- Can you even monitor this?

Cloud security: the seven deadly sins

1. Ignorance: no-one knows if cloud is in the organisation – or cares
2. Ambiguity: security requirements are not specified in contracts, SLA or EULA
3. Doubt: assurance about security arrangements is difficult to obtain
4. Trespass: laws or regulations are not understood and may be breached
5. Chaos: information released to the cloud isn't classified, stored, destroyed in a managed fashion
6. Conceit: the organisation believes it's security infrastructure is cloud-ready – typically, it's not
7. Complacency: 24/7 availability is assumed – there is no fallback in the event of a major security incident

Committed by the organisation as a whole, not just the techies!

Sample sin – with issues and actions



SIN

ISSUES

ACTIONS TO CONSIDER

Cloud computing is in the organisation, management just don't know it's there

Uncontrolled purchasing of cloud services

Failure to detect new cloud services

Cloud services have been introduced by proxy

Create and distribute a corporate policy on the use of cloud services

Extend procurement policies and processes to include cloud services and require information security approval to be part of these processes

Run a user awareness program on the adoption of cloud computing services

Use a enterprise wide data loss prevention (DLP) system to identify large amounts of data moving to cloud services

Monitor connections between the organisation's network and external networks to help identify new services that have already been deployed

Treat all outsourced services as if they were cloud-based

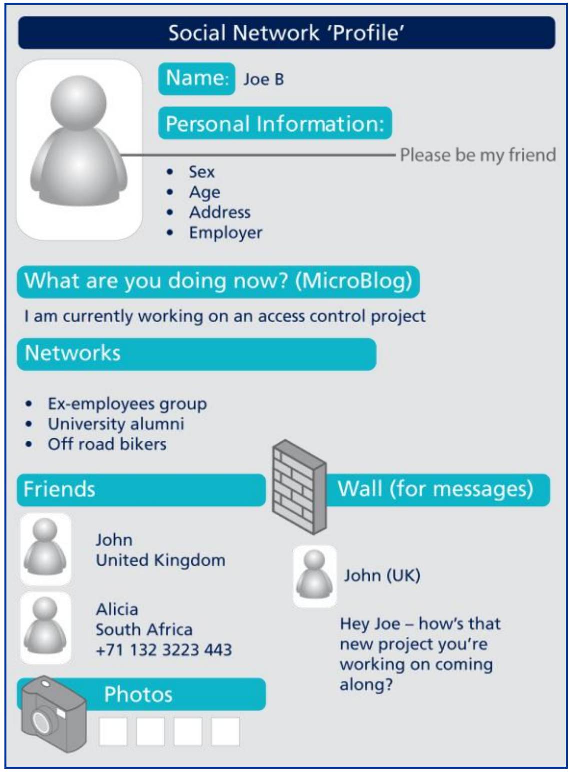
Key Challenges in 2010:

Social Media

So why should I worry?

Site	Approximate number of users (millions)
Facebook	500
Friendster	115
Twitter	100
LinkedIn	75
Viadeo	30
Xing	9

Social and networking



Social Network 'Profile'

Name: Joe B

Personal Information:

Please be my friend

- Sex
- Age
- Address
- Employer

What are you doing now? (MicroBlog)

I am currently working on an access control project

Networks

- Ex-employees group
- University alumni
- Off road bikers

Friends

John
United Kingdom

Alicia
South Africa
+71 132 3223 443

Wall (for messages)

John (UK)

Hey Joe – how's that new project you're working on coming along?

Photos

Social

- Humans are fundamentally social creatures
- Modern life impinges on the opportunities for social interaction
- Social networking fulfils a need to interact

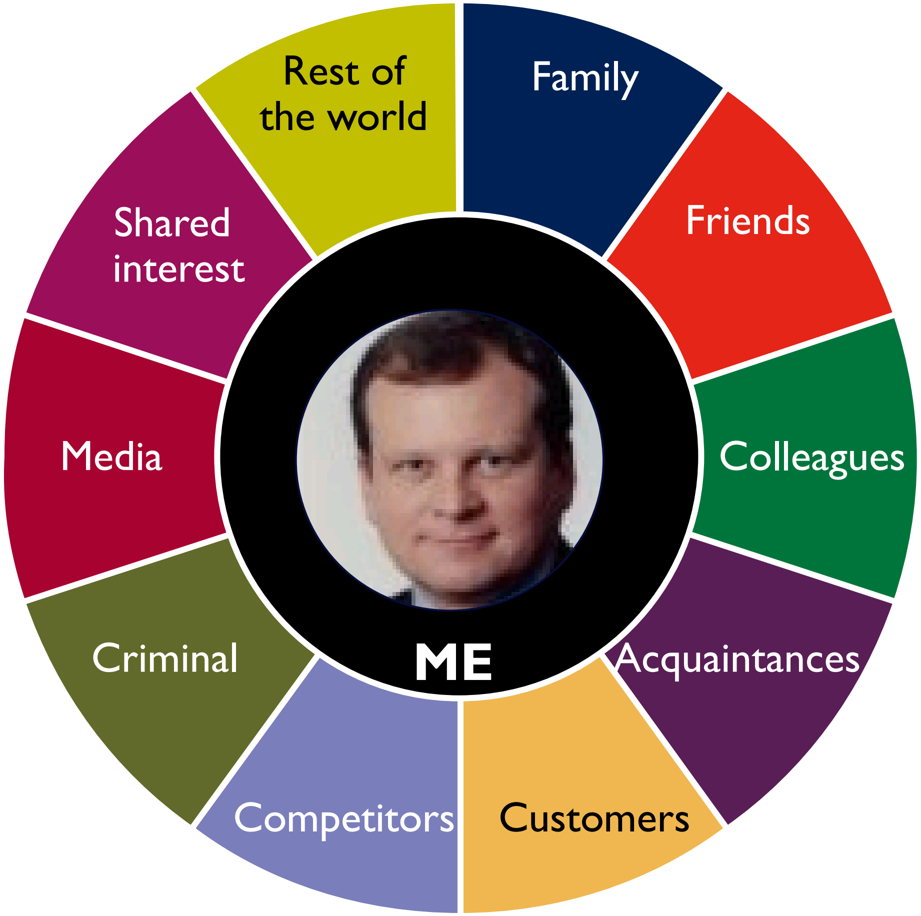
Networking

- The exchange of information amongst groups
- The cultivation of productive relationships for business*
- With a global public scope

Are the two mutually compatible?

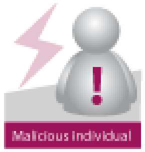
* Def - Mirriam Webster

Friends and enemies



All of the groups have different motivations and different information *needs* from the relationship with me. This creates different risks according to the stakeholder perspective

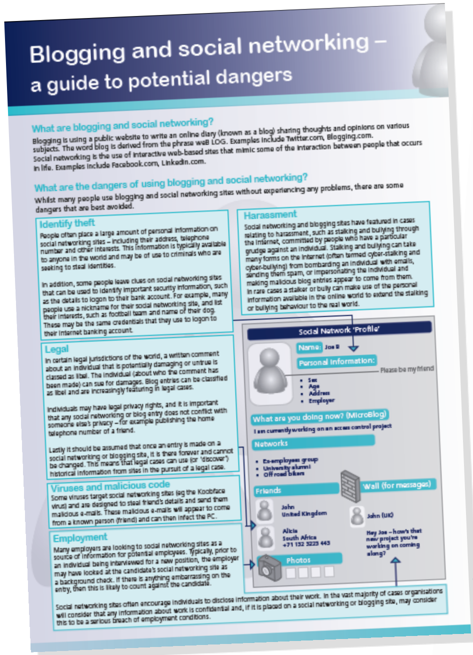
Threats

Origin of threat


Threat	Potential business impact
System overload	• Time wasting • System outages • Degraded performance
Malicious code	• Identity theft • Breach of privacy legislation • Virus causing system outage
Disclosure of business information	• Reputational damage to organisation • Loss of organisational intellectual property
Legal liabilities	• 'Libellous' comment against a reputable third party resulting in legal damages being awarded • Breach of privacy requirements due to identify theft
External attack	• Reputational damage to organisation • Identity theft • Cost of investigation and implementation of new controls
Intimidation (such as cyber-bullying or cyber-stalking)	• Reduced staff morale • Cost of investigation

…and what to do about them

- Deploy technical controls
- Revise policies
- Educate
- Educate
- Educate



Blogging and social networking – a guide to potential dangers

What are blogging and social networking?

Blogging is using a public website to write an online diary (known as a blog) sharing thoughts and opinions on various
subjects. The word blog is derived from the phrase weB LOG. Examples include Twitter.com, Blogging.com.
Social networking is the use of interactive web-based sites that mimic some of the interaction between people that occurs
in life. Examples include Facebook.com, LinkedIn.com.

What are the dangers of using blogging and social networking?

Whilst many people use blogging and social networking sites without experiencing any problems, there are some
dangers that are best avoided.

Identify theft

People often place a large amount of personal information on
social networking sites – including their address, telephone
number and other interests. This information is typically available
to anyone in the world and may be of use to criminals who are
seeking to steal identities.

In addition, some people leave clues on social networking sites
that can be used to identify important security information, such
as the details to logon to their bank account. For example, many
people use a nickname for their social networking site, and list
their interests, such as football team and name of their dog.
These may be the same credentials that they use to logon to
their internet banking account.

Harassment

Social networking and blogging sites have featured in cases
relating to harassment, such as stalking and bullying through
the internet, committed by people who have a particular
grudge against an individual. Stalking and bullying can take
many forms on the internet (often termed cyber-stalking and
cyber-bullying) from bombarding an individual with emails,
sending them spam, or impersonating the individual and
making malicious blog entries appear to come from them.
In rare cases a stalker or bully can make use of the personal
information available in the online world to extend the stalking
or bullying behaviour to the real world.

Legal

In certain legal jurisdictions of the world, a written comment
about an individual that is potentially damaging or untrue is
classed as libel. The individual (about who the comment has
been made) can sue for damages. Blog entries can be classified
as libel and are increasingly featuring in legal cases.

Individuals may have legal privacy rights, and it is important
that any social networking or blog entry does not conflict with
someone else's privacy – for example publishing the home
telephone number of a friend.

Lastly it should be assumed that once an entry is made on a
social networking or blogging site, it is there forever and cannot
be changed. This means that legal cases can use (or 'discover')
historical information from sites in the pursuit of a legal case.

Viruses and malicious code

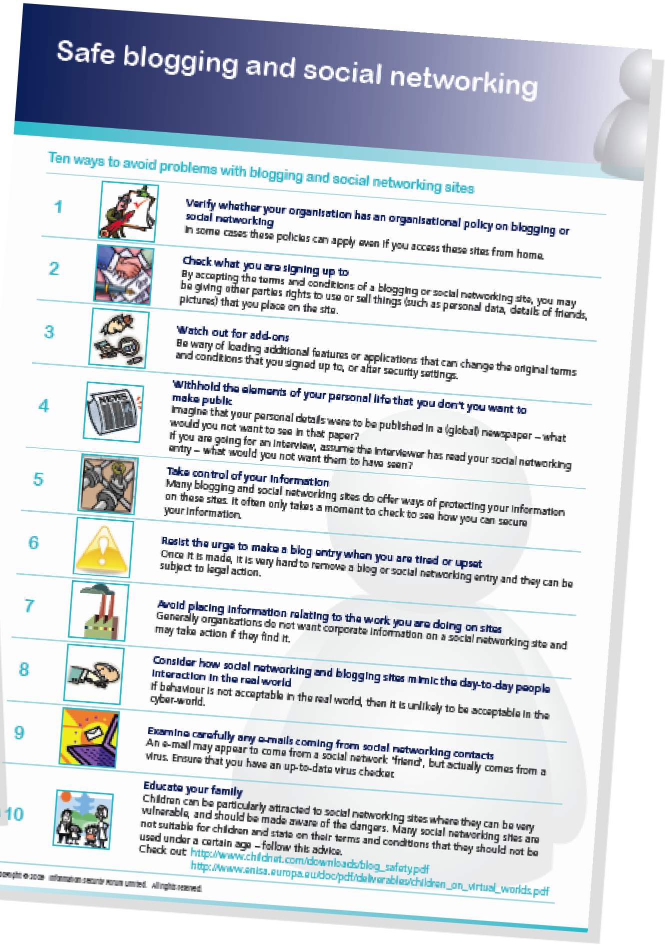
Some viruses target social networking sites (eg the Koobface
virus) and are designed to steal friend's details and send them
malicious e-mails. These malicious e-mails will appear to come
from a known person (friend) and can then infect the PC.

Employment

Many employers are looking to social networking sites as a
source of information for potential employees. Typically, prior to
an individual being interviewed for a new position, the employer
may have looked at the candidate's social networking site as
a background check. If there is anything embarrassing on the
entry, then this is likely to count against the candidate.

Social networking sites often encourage individuals to disclose information about their work. In the vast majority of cases organisations
will consider that any information about work is confidential and, if it is placed on a social networking or blogging site, may consider
this to be a serious breach of employment conditions.

Social Network 'Profile'
Name: Joe B
Personal Information:
Please be my friend
Sex
Age
Address
Employer
What are you doing now? (MicroBlog)
I am currently working on an access control project
Networks
Ex-employees group
University alumni
Off road bikers
Friends
John
United Kingdom
Alicia
South Africa
+71 132 3223 443
Wall (for messages)
John (UK)
Hey Joe – how's that new project you're working on coming along?
Photos



Safe blogging and social networking

Ten ways to avoid problems with blogging and social networking sites

1 **Verify whether your organisation has an organisational policy on blogging or social networking**
In some cases these policies can apply even if you access these sites from home.

2 **Check what you are signing up to**
By accepting the terms and conditions of a blogging or social networking site, you may
be giving other parties rights to use or sell things (such as personal data, details of friends,
pictures) that you place on the site.

3 **Watch out for add-ons**
Be wary of loading additional features or applications that can change the original terms
and conditions that you signed up to, or alter security settings.

4 **Withhold the elements of your personal life that you don't you want to make public**
Imagine that your personal details were to be published in a (global) newspaper – what
would you not want to see in that paper?
If you are going for an interview, assume the interviewer has read your social networking
entry – what would you not want them to have seen?

5 **Take control of your information**
Many blogging and social networking sites do offer ways of protecting your information
on these sites. It often only takes a moment to check to see how you can secure
your information.

6 **Resist the urge to make a blog entry when you are tired or upset**
Once it is made, it is very hard to remove a blog or social networking entry and they can be
subject to legal action.

7 **Avoid placing information relating to the work you are doing on sites**
Generally organisations do not want corporate information on a social networking site and
may take action if they find it.

8 **Consider how social networking and blogging sites mimic the day-to-day people interaction in the real world**
If behaviour is not acceptable in the real world, then it is unlikely to be acceptable in the
cyber-world.

9 **Examine carefully any e-mails coming from social networking contacts**
An e-mail may appear to come from a social network 'friend', but actually comes from a
virus. Ensure that you have an up-to-date virus checker.

10 **Educate your family**
Children can be particularly attracted to social networking sites where they can be very
vulnerable, and should be made aware of the dangers. Many social networking sites are
not suitable for children and state on their terms and conditions that they should not be
used under a certain age – follow this advice.
Check out http://www.childnet.com/downloads/blog_safety.pdf
http://www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf

Copyright © 2008 Information Security Forum Limited. All rights reserved.

Threat Horizon

Why look into the future?

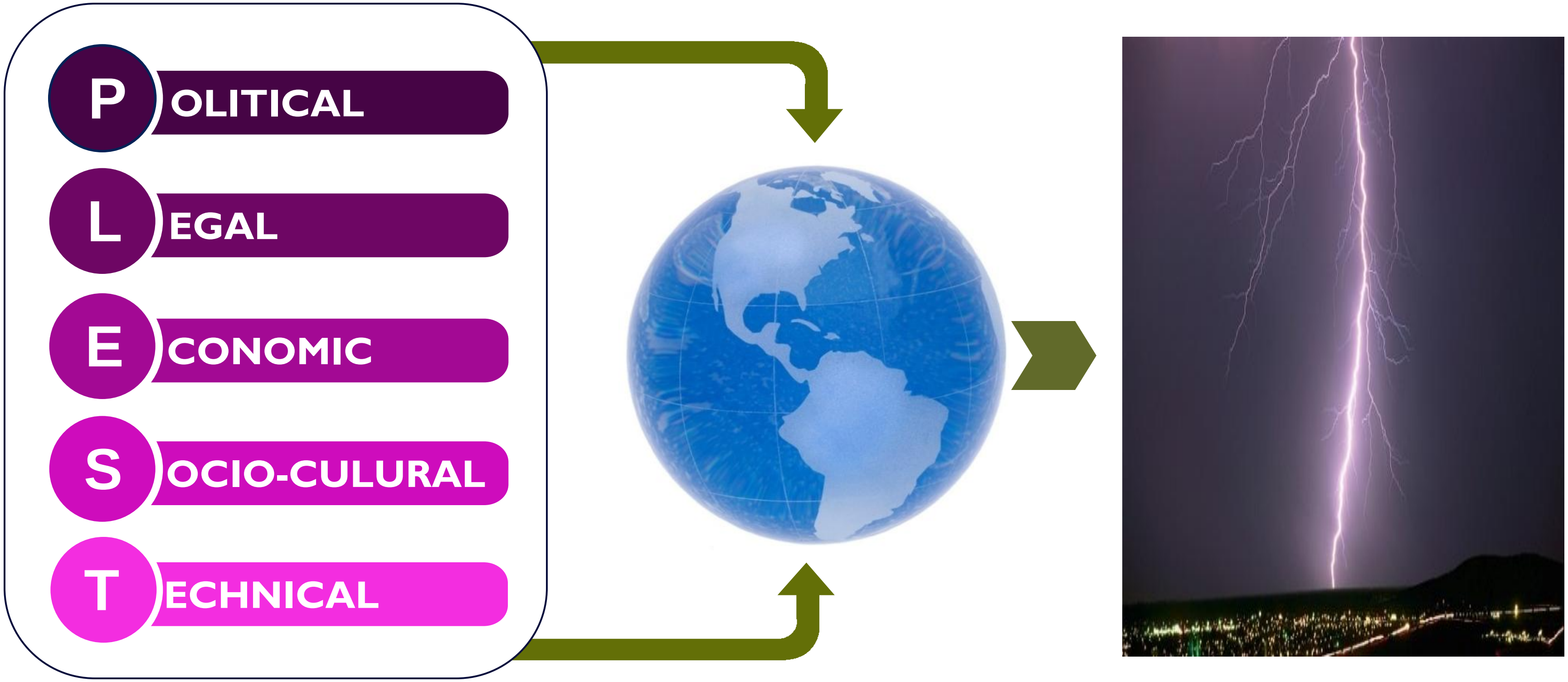
In order to understand how good practice should change in the future we need to understand what threats that we will face in the future and how we should respond to them.

The ISF call this the

Threat Horizon

Threat horizon methodology

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



P OLITICAL

L EGAL

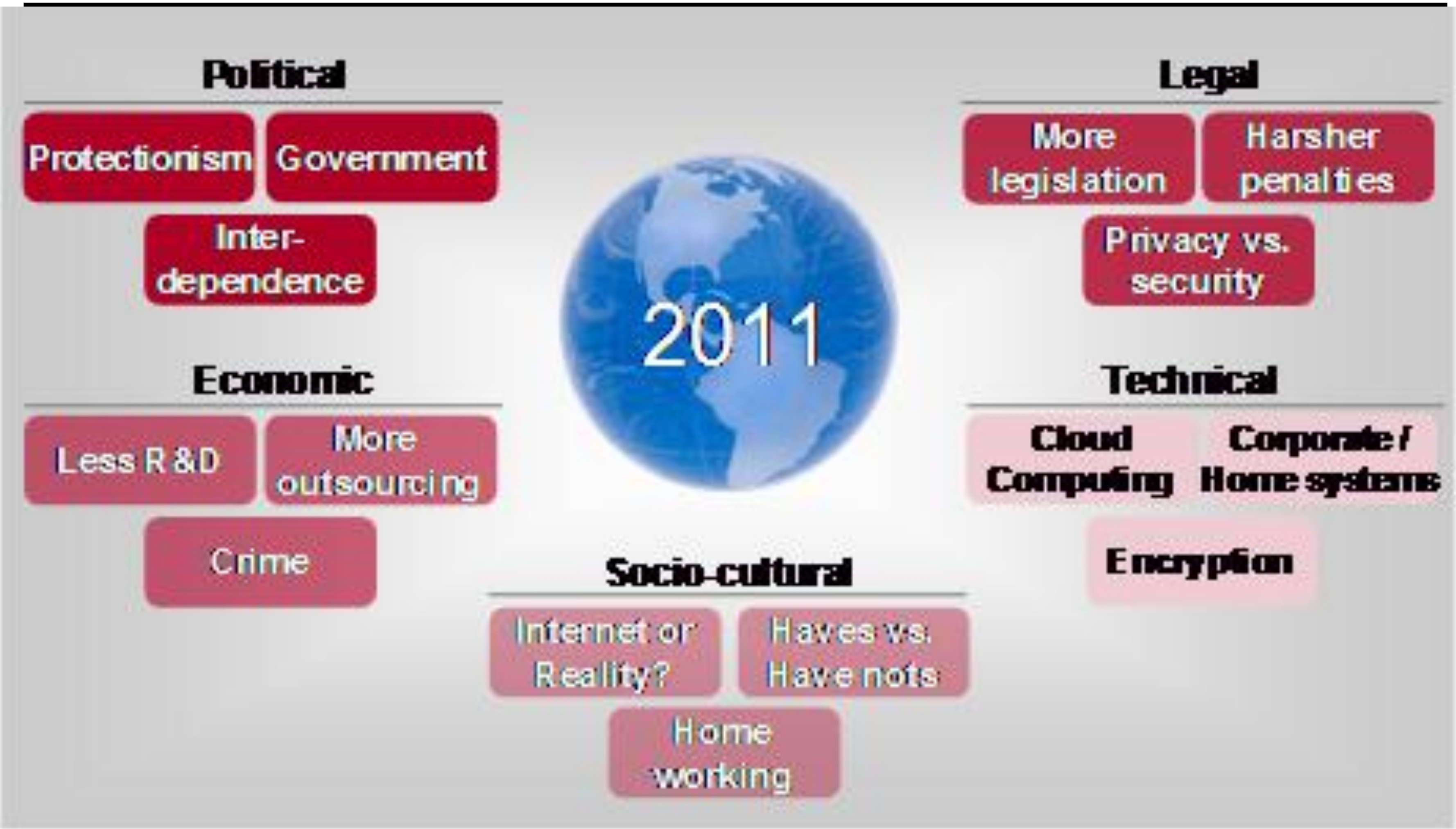
E CONOMIC

S OCIO-CULURAL

T ECHNICAL

2011…

What will world look like in 2011?



Political

Protectionism

Government

Inter-dependence

Legal

More legislation

Harsher penalties

Privacy vs. security

2011

Economic

Less R&D

More outsourcing

Crime

Technical

Cloud Computing

Corporate / Home systems

Encryption

Socio-cultural

Internet or Reality?

Haves vs. Have nots

Home working

Key trends impacting information security to 2011

- Infrastructure revolution
- Data explosion
- An always-on, always-connected world
- Future finance
- Tougher regulation and standards
- Multiple internets
- New identity and trust models

Source: Revolution or evolution?
Information Security 2020

Technology Strategy Board

Information security threats for 2011….

Criminal attacks
Weaknesses in infrastructure
Tougher regulatory legislation
Pressures on offshoring / outsourcing
Eroding network boundaries

Mobile malware
Vulnerabilities of Web 2.0
Incidents of espionage
Insecure coding and development practices
Changing cultures

Top five threats in detail

Criminal attacks

- Crimeware as a service
- Insider attacks
- Infiltration

Weak infrastructure

- Reduced investment
- Complexity
- Zero-day attacks

Tougher rules

- Emphasis on privacy
- Incompatible laws
- Increasing punishment

Outsourcing / Offshoring

- More outsourcing
- Meeting compliance
- Instability of providers

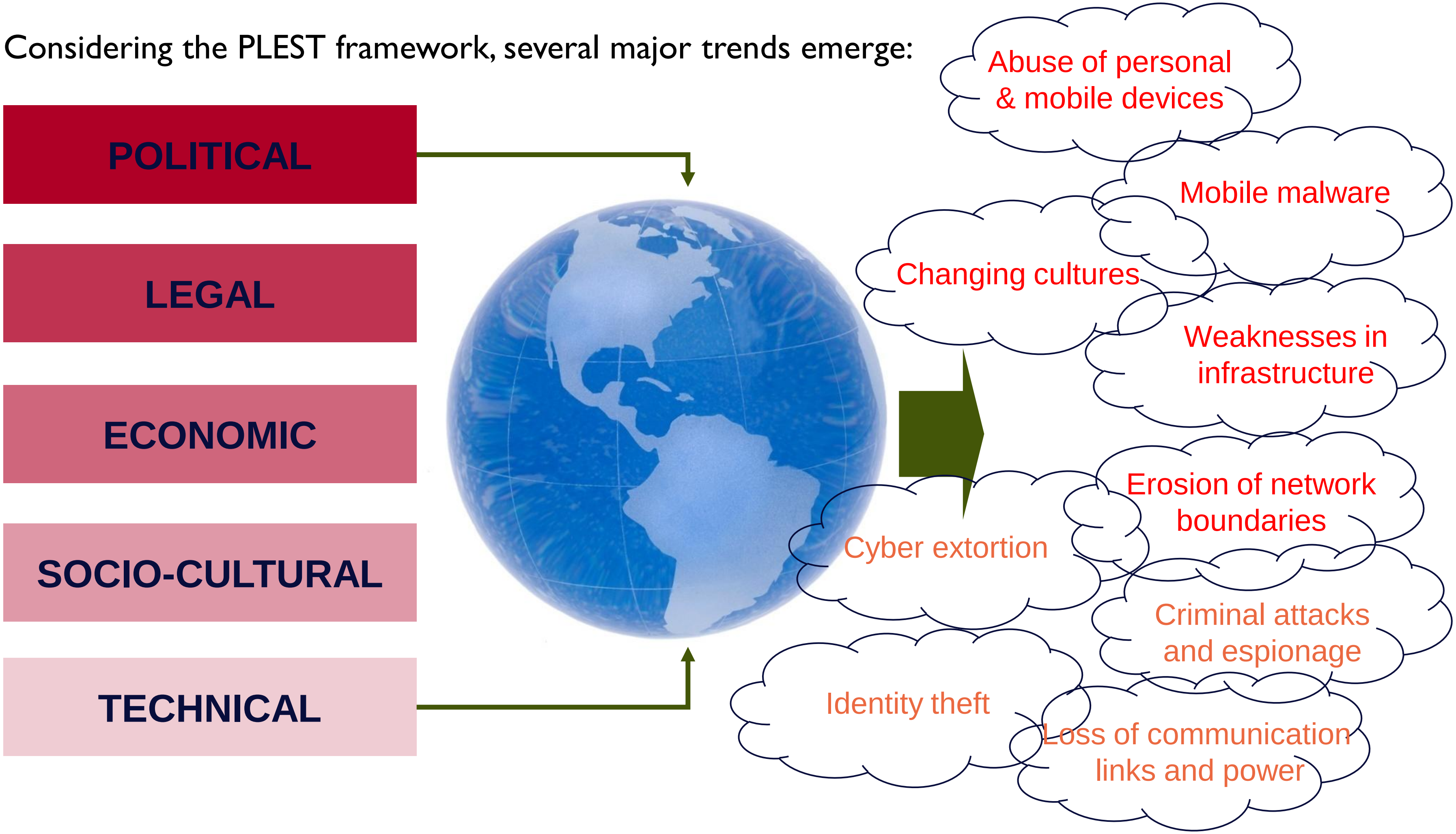
Eroding boundaries

- Cloud computing
- More connections
- Bypass of defences

2012…

The world in 2012

Considering the PLEST framework, several major trends emerge:



POLITICAL

LEGAL

ECONOMIC

SOCIO-CULTURAL

TECHNICAL

Abuse of personal & mobile devices

Mobile malware

Changing cultures

Weaknesses in infrastructure

Erosion of network boundaries

Cyber extortion

Criminal attacks and espionage

Identity theft

Loss of communication links and power

Key longer term drivers

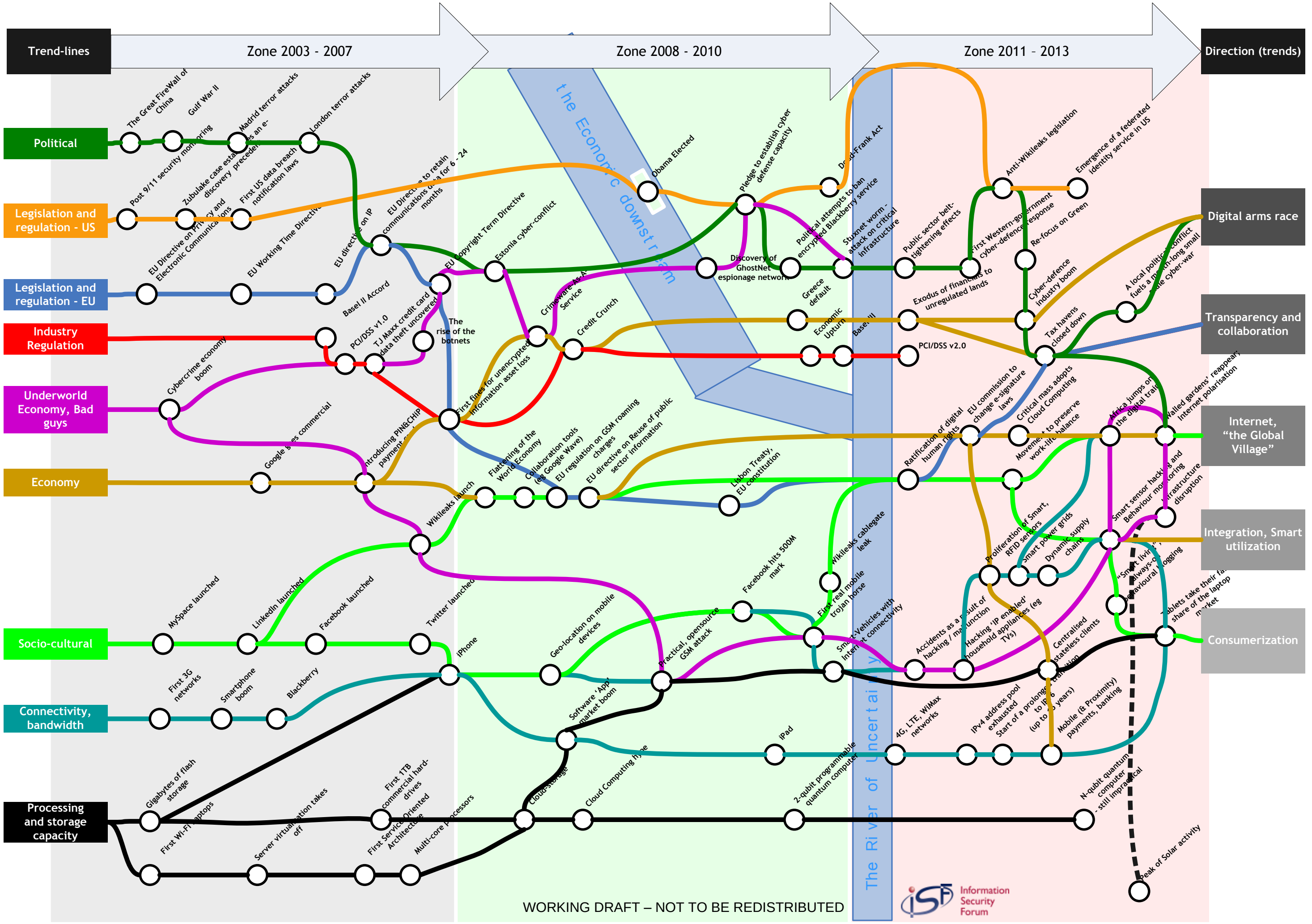
- Globalisation
- Increased focus on climate change
- Shifting global economic centres
- Changing demographics
- Increasing regulation / governance
- Increasing reliance on technology and information
- Changing attitudes towards privacy
- Evolving work / home balance

Source: Revolution or evolution? Information Security 2020

Technology Strategy Board

2013...

2013 PLEST



Trend-lines

Zone 2003 - 2007

Zone 2008 - 2010

Zone 2011 - 2013

Direction (trends)

Political

Legislation and regulation - US

Legislation and regulation - EU

Industry Regulation

Underworld Economy, Bad guys

Economy

Socio-cultural

Connectivity, bandwidth

Processing and storage capacity

The Great FireWall of China

Gulf War II

Madrid terror attacks

London terror attacks

Post 9/11 security monitoring

Zubulake case establishes an e-discovery precedent

First US data breach notification laws

EU Directive on Privacy and Electronic Communications

EU Working Time Directive

EU directive on IP

EU Directive to retain communications data for 6 - 24 months

Basel II Accord

PCI/DSS v1.0

TJ Maxx credit card data theft uncovered

The rise of the botnets

Cybercrime economy boom

Google goes commercial

Introducing PIN&CHiP payment card

Wikileaks launch

MySpace launched

LinkedIn launched

Facebook launched

Twitter launched

First 3G networks

Smartphone boom

Blackberry

Gigabytes of flash storage

First Wi-Fi laptops

Server virtualization takes off

First 1TB commercial hard-drives

First Service Oriented Architecture

Multi-core processors

the Economic downstream

Obama Elected

Pledge to establish cyber defense capacity

EU Copyright Term Directive

Estonia cyber-conflict

Discovery of GhostNet espionage network

Crimeware-As-A-Service

Credit Crunch

First fines for unencrypted information asset loss

Flattening of the World Economy

Collaboration tools (eg Google Wave)

EU regulation on GSM roaming charges

EU directive on Reuse of public sector information

Lisbon Treaty, EU constitution

Greece default

Economic Upturn

Basel III

Dodd-Frank Act

Political attempts to ban encrypted Blackberry service

Stuxnet worm - attack on critical infrastructure

Wikileaks cablegate leak

Facebook hits 500M mark

First real mobile trojan horse

Smart-Vehicles with Internet connectivity

iPhone

Geo-location on mobile devices

Practical, opensource GSM attack

Software 'App' market boom

Cloud-storage

Cloud Computing hype

iPad

2-qubit programmable quantum computer

The River of Uncertainty

Public sector belt-tightening effects

First Western-government cyber-defence response

Anti-Wikileaks legislation

Emergence of a federated identity service in US

Re-focus on Green

Exodus of financials to unregulated lands

Cyber-defence industry boom

PCI/DSS v2.0

Tax havens closed down

A local political conflict fuels a month-long small scale cyber-war

Ratification of digital human rights

EU commission to change e-signature laws

Critical mass adopts Cloud Computing

Movement to preserve work-life balance

Africa jumps on the digital train

Walled gardens' reappear; Internet polarisation

Smart sensor hacking and Behaviour monitoring

Infrastructure disruption

Proliferation of Smart, RFID sensors

Smart power grids

Dynamic supply chains

"Smart living", always-on, behavioural logging

Tablets take their fair share of the laptop market

Accidents as a result of hacking / malfunction

Hacking 'IP enabled' household appliances (eg TVs)

Centralised stateless clients

4G, LTE, WiMax networks

IPv4 address pool exhausted

Start of a prolonged transition to IPv6 (up to 15 years)

Mobile (& Proximity) payments, banking

N-qubit quantum computer - still impractical

Peak of Solar activity

Digital arms race

Transparency and collaboration

Internet, "the Global Village"

Integration, Smart utilization

Consumerization

WORKING DRAFT – NOT TO BE REDISTRIBUTED

Information Security Forum

An overview of the threats

EXPECTED

On the radar threats
These threats were gathered directly from contributing ISF Members who expressed their opinion by participating in a Threat Horizon exercise at one of the Chapter Meetings or have attended the Congress Workshop. There is a general cross-industry consensus that the information security profession will need to focus on these problems over the next 24 months.

Government, justice require access or software source code (eg for interception of traffic)	Stricter regulation on data segregation (PII)	Social engineering & increased consumer naivety	Cyberwar increases, state sponsored hacking	Mobile loss, business misuse	Industrial, government espionage (human and cyber factor)	Regulatory penalties	Consumerisation introduces new attack vectors	New attack vectors through third parties	Video sensitivity (conferencing, surveillance)
Availability impact from natural disasters and adverse weather conditions	Intelligent, tailored malware, Advanced trojans making better use of stolen customer data	Inability to see new threats, increase quantity and speed of 0-day threats	Customer ID theft defrauding organisations and Corporate Brand theft deceiving customers	Social media abuse, a political tool	Authentication in multi channel multi device technology becomes more difficult to secure	Security impact from increased globalisation with disconnected laws and regulations	Whaling – targeted attacks aimed at high net worth individuals (eg CEOs, celebrities)	Increased attacks on devices embedded on SCADA systems (Stuxnet offspring)	IPv4 to IPv6 transition period vulnerabilities
Quantity of information (data) increases, quality of information decreases	Power grid outages	Internet enabled house appliances and vehicle, vulnerabilities	Moving to Cloud infrastructure, Loss of control	Mobile device GPS tracking – privacy - theft Embedded location services used for crime	More company data on consumer devices	Low-level chip attacks	Data leakage from - unencrypted media loss - breach - insiders, including Wikileaks whistleblowers	Loss of workforce loyalty due to outsourcing	Proliferation of IP-networked systems in key IT infrastructure
Increase in blended attacks exploiting a combination of people, process and technology vulnerabilities in real time.	Increase in attacks provoked by single issue activism (Hacktivism)	Expectations of Generation Y	SSL / TLS vulnerabilities	Hack for profit	Loss of boundary between work and personal life resulting in accidental disclosures	Social networking in low risk tolerance companies	Undetectable malware stealing proprietary information	RFID enabled devices and wireless sensors insecurity, weak authentication	Development of business applications without security to decrease time to market, startup costs

NON MANAGEABLE

MANAGEABLE

Below the radar threats
These threats are put forward by ISF research team to be the big deal things by 2013.

Hacktivism	Shortage of the right skill in the information security field (mixture of business and technical)	**IT crisis over rare earths** Estimated remaining global supply of certain non renewable resources critical for IT devices and infrastructure is fast depleting with only 10 years left for some. This may have a big impact over the availability and cost of IT components.	**Data vs information**	IPv6 transition	**(dynamic) Supply chain complexity** M&A, cross-border,	**Data integrity management** Volume vs age vs value vs type and lack of security and classification	**IT systems complexity** Scope creep, inability to assess security

'The Black Swan' Events
A rare and underrated event with potentially catastrophic impact has been named 'the Black Swan' by Nicholas Taleb, author of the book with the same title. The importance of such events lies in their uncertainty and randomness, and consequentially the inability to predict their likelihood with a normal risk-management approach.
The ISF has identified a number of such disruptive information security related events that Members may wish to consider despite the low likelihood of them actually materialising.

Peak of Solar Activity
The Sun's periodic electromagnetic flare outbursts can have a disruptive impact on power and telecommunications infrastructure, especially satellites which are unprotected by Earth's magnetic shield. Solar flares are a cyclic phenomenon and nothing unusual, however we are currently facing an unusual period of prolonged solar inactivity, which could end with a bigger than usual solar flare and a peak of activity predicted for 2013, that may leave an impact on our infrastructure. The last solar flare of such proportion happened in 1859.

Internet / Telecomms Blackouts
In addition to solar flares, long periods of telecommunications unavailability could be caused by a particularly aggressive piece of malware, DNS disruption, cyber-war, EMP blast in the high atmosphere or other.

Failure of a global information system
The increasing dependency on certain global systems, for international funds transactions (eg SWIFT), Air traffic control systems or passport information system (eg SIS), may result in a great impact if the availability of such a system was disrupted or its integrity compromised.
A targeted attack that mirrors the sophistication of the Stuxnet worm or a fundamental design flaw would have the power to cause unprecedented impact.

UNEXPECTED

Upheaval in the country of your outsource provider
The cost-benefit analysis was sound and the political atmosphere stable and a low risk when the outsourcing deal in a developing country was concluded. Emerging economies however are more likely to undergo radical political changes or face disruptive civil unrests that could bring a full hold on outsourcer's service. The situation could deteriorate even further where the contracting organisation's data were 'held for ransom' or intellectual property appropriated by the new regime.

An update gone wrong
A compromised or malfunctioning software update (OS fix, Application fix, Anti-virus definitions) from a trusted source could potentially cripple IT from within.

Trusted encryption algorithm defeated
Just as GSM encryption has been cracked, other undisputed algorithms (AES) or solutions (PKI) will eventually fall over as a result of the rising computational capacity (the cloud) and increased scrutiny. The main question is when, and how does that impact an organisation using encryption.

Death of a Major IT supplier
'The bigger they are, the harder they fall.' It has happened to Enron and Lehman Brothers, there is no reason it could not happen to a trusted cloud service, IT service provider, software or hardware vendor that organisations have contracted and are increasingly reliant on.

Threats....

- Increasing attacks on RFID, sensors and control systems
- Loss of trust / inability to prove identity and authenticate
- Co-ordinated attacks for extortion, blackmail, bribery or stock manipulation
- New attack vectors
- Governmental interception of all traffic
- Hardware back doors (low-level attacks / vulnerabilities) in chips, SCADA
- Loss of workforce loyalty – loss of organisational culture and knowledge
- Solar activity disrupts communications globally

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

Sometimes 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 – a guide to potential dangers

Solving the data privacy puzzle
Achieving compliance

ISF Briefing: Legal aspects of encryption

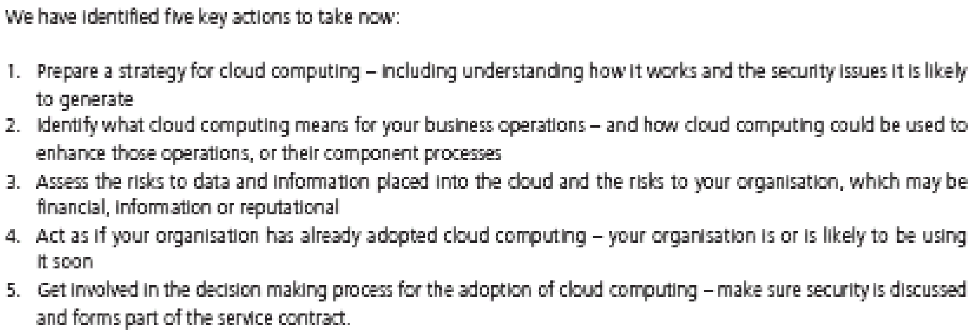
Security Implications of Cloud Computing
July 2009

Risk Convergence
Implications for information risk management

Outsourcing and Third Party Risk Management – ISF deliverables

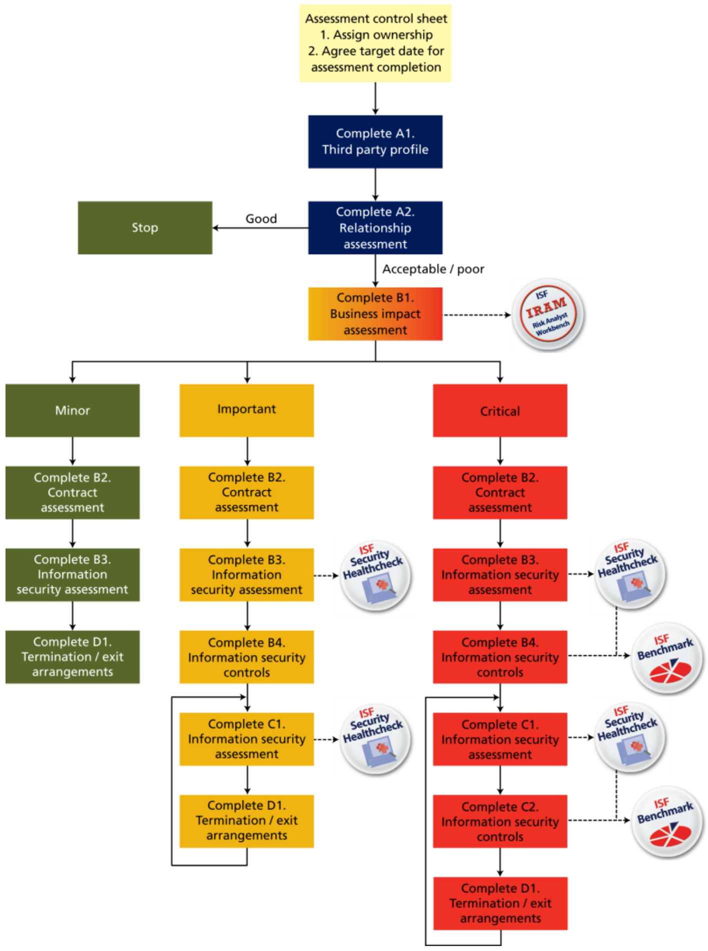
What do I do now? – at a practical level

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.


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
ISF IRAM Risk Analyst Workbench
Minor
Important
Critical
Complete B2. Contract assessment
Complete B2. Contract assessment
Complete B2. Contract assessment
Complete B3. Information security assessment
Complete B3. Information security assessment
ISF Security Healthcheck
Complete B3. Information security assessment
ISF Security Healthcheck
Complete D1. Termination / exit arrangements
Complete B4. Information security controls
Complete B4. Information security controls
ISF Benchmark
Complete C1. Information security assessment
ISF Security Healthcheck
Complete C1. Information security assessment
ISF Security Healthcheck
Complete D1. Termination / exit arrangements
Complete C2. Information security controls
ISF Benchmark
Complete D1. Termination / exit arrangements

Conclusion

Keeping up with business change

- Social environment (demographics, attitudes, cultures)
- Business environment (activities, operations, markets)
- Economic environment (credit crunch, realignment of world economy, rise of China)
- Global environment (global warming, interconnectivity, competition for resources)
- Technological environment (mobile phones, nanotechnology, pervasiveness)

ACTIONS

- Engage with the business
- Question the beliefs
- Craft a new security strategy
- Plan for uncertainty
- Prepare for change

Thank you for your attention

Steve Durbin

Global Vice President
E-mail: steve.durbin@securityforum.org
Web: www.securityforum.org