

The threat horizon

a two year view of information security-related threats

Andy Jones

ISF Senior Research Consultant

What is the ISF?

An international association of over **290** leading global organisations, which...

- addresses key issues in information risk management through research and collaboration
- develops practical tools and guidance
- is fully independent and driven by its Members
- promotes networking within its membership



Basis for this work

Based on ISF research

Brainstorm sessions

- 150 Member representatives
- North America
- UK
- South Africa

Interviews with ISF specialist organisations including

- Vendors
- CERT and governmental
- Retailers
- National and International police forces



The changing world

POLITICAL

instability, terrorism, energy

LEGAL

compliance, discovery, record management

ECONOMIC

e-economy, organised crime, extreme weather

SOCIO-CULTURAL

techo-generation, remote working, home vs work life

TECHNICAL

digital convergence, device convergence, new products



1. Loss of communication links and loss of power

POLITICAL

- Brown outs are expected to become more common
- Critical National Infrastructure may become a target
- Terrorism is likely to be a continuing threat

2. Risk vs Compliance

LEGAL

- Growing compliance burden from legislation and regulation
- Contention for budget between risk and compliance activities
- Skills in risk analysis will be at a premium



3. Infinite risk acceptance

LEGAL

- Conflicting risk mitigation requirements will lead to a build up of unmitigated risk
- Neglect of operational risk may cause incidents
- A risk fatigue may result in poor attention to mitigating controls

4. Legal discovery

LEGAL

- Record discovery may become a common element of legal actions
- Legal actions are likely to become a common business event
- Cost overheads associated with discovery may become significant

5. Cyber extortion

ECONOMIC

- Organised crime will follow the money
- Hackers will be available to rent
- Traditional and hi-tech techniques may target high risk staff

6. Identity theft

ECONOMIC

- Man in the middle may become a viable threat to authenticated transactions
- Spyware is expected to become increasingly sophisticated
- Spear-phishing will represent an evolution in phishing attacks

7. Evolving malware

ECONOMIC

- Malware will become silent and deadly
- Malware will be written to order
- Malware will become modular and upgradeable

8. Abuse of mobile and personal devices

SOCIO-CULTURAL

- Device convergence may lead to threats to corporate information held on personal devices
- Plug and play connectivity will make it harder to guard against personal devices joining an organisational network
- Consumer oriented behaviour will bleed further into the workplace

9. Exploitation of vulnerabilities of public networks

SOCIO-CULTURAL

- Poorly secured public networks may include home networks
- Erosion of the network boundary may lead to a rethink on the effectiveness of security gateways
- Malicious code may be introduced through home and mobile working

10. Exploitation of patching vulnerabilities of virtual systems

TECHNICAL

- Virtualisation trend challenges existing processes
- Inappropriate resilience may result in business impact
- Conflicting patching regimes

11. Exploitation of vulnerabilities of RFID

TECHNICAL

- RFID adoption requires strict control to guard against fraud
- Privacy concerns may be raised around the use of RFID tags
- Denial of service attacks may become viable against RFID systems in the pursuit of crime

12. Exploitation of vulnerabilities in architectures and products

TECHNICAL

- Service Orientated Architectures may suffer from poorly understood security models
- High assurance SSL certification may become attractive to fuzzers
- Existing and new operating systems are expected to attract new interest from the hacking community

Future headlines

- Assume that non malicious threats will continue to account for the biggest business impacts
- Expect more of the same from malicious threats
- Beware the involvement of organised crime
- Understand the growing threat from within
- Watch out for clustered threats
- Look beyond the 24 month horizon



Andy Jones CISSP
Information Security Forum

Senior Research Consultant
Tel: +44 (0)207 213 4878
E-mail: andy.jones@securityforum.org
Web: www.securityforum.org
www.isfsecuritystandard.com

