Action

Where next?

Threat Horizon 2015 contains detailed predictions along with trends and other factors that can increase or decrease the probability of the predictions coming true. There is also a description of business impacts and recommended actions.

We recommend that organisations:

- become familiar with the techniques ISF Members have used to implement Threat Horizon
- adopt Threat Horizon for their own use
- use a threat radar to help categorise threats – this can help prioritise and sequence actions when time and budgets are limited
- review those threats that are high priority for your organisation and consider the recommendations in the report
- take advantage of the relevant ISF deliverables
- work with other organisations to collaborate on cyber security intelligence and strategies.

Threat Horizon 2015 is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isflive.org. Non-Members can purchase the report by contacting Steve Durbin at steve.durbin@securityforum.org.

About the ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work program. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

Contacts

For further information contact:
Steve Durbin
UK Tel: +44 (0)20 7213 1745
US Tel: +1 (347) 767 6722
Fax: +44(0)20 7213 4813
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

Disclaimer

Information Security Forum

Threat Horizon 2015

New danger from known threats

Understanding threats is fundamental to enterprise risk management; threats need to be evaluated in the context of the organisation to determine risk.

This year's Threat Horizon report finds that the biggest risk is from known threats. The fact that hacktivism and malicious software have been around for a while doesn't mean they're less threatening and we can relax – quite the opposite. Older threats, because they've matured, are more dangerous and pose more risk to our organisations than ever. They're more sophisticated and more effective. Whether they're old or new is much less important than their potential to do harm.

The annual ISF Threat Horizon report provides a practical way for organisations to take a forward-looking view of the increasing threats in today's always-on, interconnected world. This in turn enables a better prepared, strategic approach to managing and mitigating risk.

This year's report deals with the following themes:

- Cyber risk is challenging to understand and address, from CEOs that simply don't get it to organisations struggling to find the right people.
- Reputation is a new target for cyber attacks, from insider activists who leak information, and hacktivist collectives who vote on who they dislike this week
- Criminals value your information, they're highly motivated to obtain it, or to use what leaks out of your organisation
- The changing pace of technology doesn't help; bring your own cloud (BYOC) and bring your own device (BYOD) also bring their own risks
- The role of governments must not be misunderstood: while they have a key role to play, they won't lead cyber security efforts – they expect organisations to manage risks in cyberspace and prevent information and systems from being compromised

ISF Threat Horizon reports are written for a non-technical audience, and ISF Members use them for many purposes, for example as a communications and awareness tool, to align business and security strategy, and to influence their organisation's risk appetite. This report contains recommendations and references to ISF deliverables and other external resources which can help address these risks.

2015

Predictions from the ISF Threat Horizon 2015 report

Reputation is a new target for cyber attacks

Insiders fuel corporate activism

Business practice will be scrutinised, not only by watchdog bodies, but also by employees, contractors and customers. More insiders will emerge as more people place their own ethics and perspectives above those of their employers. Criticism will go viral and those that come from credible insiders will spread faster. Coordinated action will attract hacktivists who will initiate sympathetic cyber attacks.

Hacktivists create fear, uncertainty and doubt

As long as systems continue to be compromised, claims will be believable. Whether something actually happened is secondary: organisations will be guilty until proven innocent. And the impact will be independent of whether the false claims are intentionally malicious, like a bomb threat, or the result of honest mistakes.

External threat magnifiers include:

- Poor BYOD policy will place confidential information at risk
- Privileged accounts still an issue
- Security of embedded devices raises concerns

Recommended actions include:

- Aligning Business Continuity and Information Security (2006)
- Information Security Incident Management (2006)
- ISF Briefing: Insider threats (2007)
- ISF Briefing: Hacktivism (2011)
- You Could Be Next: (2012)
- The 2012 Standard of Good Practice for Information Security

Criminals value your information

Crime as a Service (CaaS) upgrades to 2.0

Attacks will become more innovative and sophisticated to circumvent organisations' new security mechanisms. Unemployed and disgruntled employees will form a talent pool for criminal groups to gather information needed for these attacks. The value of a person's identity will be eclipsed by organisational profiles such as details about an organisation's vulnerabilities or knowledge of business operations.

Information leaks all the time

Criminals will get better at combining sources from the Internet with information obtained through intrusions and data leaks. It will allow them to launch a new range of attacks, both virtual and physical, targeting individuals based on their ability to provide access to and information about their organisation. Despite social engineering being less risky, some criminals will still break into houses to steal employees' laptops and other devices.

External threat magnifiers include:

- Cyberwar career path with cyber arm qualifications
- Competitor espionage & IP theft using criminals
- Cyber Security Awareness campaign in the UK: The Devil is in Your Details
- Facebook ID as proof of identity
- Realisation of value of information

Recommended actions include:

- ISF Briefing: Insider threats (2007)
- ISF Briefing: Profit-Driven Attacks (2008)
- SF Briefing: DLP Tools (2009)
- Protecting Information in the End User Environment (2010)
- Solving the data privacy puzzle: Achieving compliance (2010)
- The 2012 Standard of Good Practice for Information Security

Cyber risk is challenging to understand and address

The CEO doesn't get it

If organisations' senior executives don't understand cyberspace they will either take on unknown, unquantified risk, or miss opportunities to achieve objectives such as increasing market share. Organisations that can't maintain a trusted environment to interact with customers could suffer or collapse. The gulf will widen between those that get it and those that don't – and the longer they wait, the harder it will be to catch up.

Organisations can't get the right people

Despite high unemployment rates, skilled technical and managerial positions will be more difficult to fill. Education systems are gearing up to teach skills but will not provide people with relevant experience. Without technical and management expertise, organisations will be challenged to prevent, manage and recover from incidents.

Outsourcing security will backfire

Organisations that consider information security and other technology to be a cost centre will suffer if they don't keep the authority and understanding necessary to manage their service providers. Organisations unable to build and drive their information security strategy will lose control and be unable to meet the needs of the business or respond to changing threats.

External threat magnifiers include:

- The role of the CISO is evolving within the organisation
- Failure to ease and adapt immigration rules and nationalism make the situation worse
- Loss of 1st generation skills
- Organisations are overwhelmed by cyber security complexity

Recommended actions include:

- Role of Information Security in the Enterprise (2008)
- Risk Convergence - Implications for Information Risk Management (2009)
- The Information Lifecycle: A New Way of Looking at Information Risk (2010)
- Cyber Security Strategies: Achieving cyber resilience (2011) and Cyber SIG
- Information Security Governance: Raising the game (2011)
- The 2012 Standard of Good Practice for Information Security
- How to get the Attention of the Board (upcoming 2013)
- The Changing Role of the CISO (upcoming 2013)

The changing pace of technology doesn't help

BYOC (bring your own cloud) adds unmanaged risk

If an organisation's IT function or technology provider is unable to meet business needs, people will move to the cloud. Unmanaged deployment of cloud solutions within organisations will create duplicated and incomplete repositories of information – which could have consequences considerably worse than a data breach. Organisations that can't determine where their information is now certainly won't be able to do so in two years' time when information volumes will have increased exponentially.

Bring your own device further increases information risk exposure

Organisations won't be able to ignore bring your own device (BYOD) initiatives; they're needed to create a differentiator for organisations wanting to attract and retain talent, and the benefits of productivity and collaboration are promising. But organisations that do not manage the integration of privately owned devices into the organisation's network will expose themselves to significant risks.

External threat magnifiers include:

- Consolidation of cloud providers
- Intrusion in cloud providers' infrastructure
- Organisations, pressured by executives and boards, deciding to implement BYOD without considering security

Recommended actions include:

- Best Practice in Securing Endpoint Computing Devices (2007)
- Protecting Information in the End User Environment (2010)
- Securing Cloud Computing: Addressing the Seven Deadly Sins (2011)
- The 2012 Standard of Good Practice for Information Security
- Securing the Supply Chain (upcoming 2013)
- Mobile Device Special Interest Group (MDSIG)

The role of government must not be misunderstood

Governments and regulators won't do it for you

Governments have a key role to play in securing cyberspace, from coordination to raising public awareness and sharing threat information. But they have no intention of leading cyber security efforts. They expect organisations to manage risks in cyberspace, and to prevent information and systems from being compromised. Organisations that depend on governments to lead or secure cyberspace will suffer, as will those who focus only on complying with regulations.

External threat magnifiers include:

- More regulations and stronger regulation might create conflicts
- Conflicting interests with governments around cybercrime prevention, preventing networks from attack while promoting human rights by allowing online communications
- Cyber compliance over cyber cooperation

Recommended actions include:

- Security and Legislation: Complying with information security-related legislation (2005)
- The 2012 Standard of Good Practice for Information Security