Information Security Forum

Threat Horizon 2016 – on the edge of trust

Cyberspace is evolving rapidly. Organisations are facing an increasingly complex threat landscape, one that traditional security approaches are incapable of addressing. Organisations must be aware of a wide range of threats, the most pressing of which they have little control over.

Walking away from cyberspace is not an option and while defending against all threats is unrealistic, there is still time to build resilience to them. It is essential to re-assess assumptions about operating in cyberspace and adapt resilience to this new paradigm. At the same time, organisations need to continually bolster resilience to ongoing threats such as cybercrime and the insider threat.

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. By providing guidance and recommendations, it enables organisations to take a strategic approach to managing and mitigating risk.

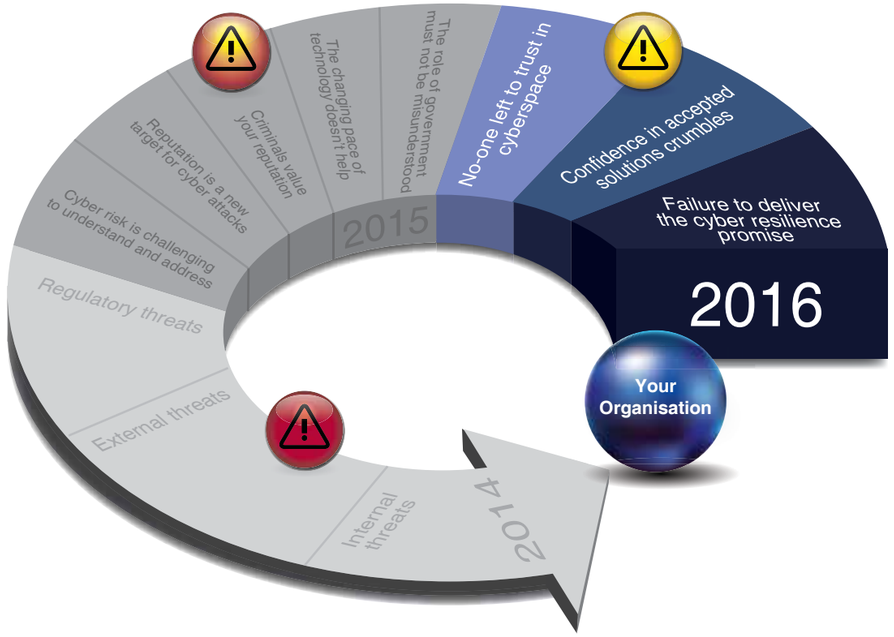
This year's report deals with the following themes:

- **No-one left to trust in cyberspace** – Organisations must prepare to operate in an environment where governments no longer balance national security with citizens' and business's best interests.
- **Confidence in accepted solutions crumbles** – Organisations need to build resilience against cyber threats at a time when a number of accepted solutions are no longer viable.
- **Failure to deliver the cyber resilience promise** – Unless CISOs evolve their skill set to ensure that they can anticipate the CEO's needs and deliver on an increasingly demanding digital agenda, they will fail.

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.

Threat Horizon 2016 – on the edge of trust

The diagram below lists the ten new threats to 2016. It is important that organisations know what is on the horizon for 2016 as well as the threats that are about to hit in 2014. In this way, organisations can build their resilience to a wide range of threats. Failure to do so could result in reputational and brand damage, data leakage and/or monetary fines, to name a few. **Preparing now isn't an option, it's essential!**



	2014 Threats
1	Cyber criminality increases as Malspace matures further
2	The cyber arms race leads to a cyber cold war
3	More causes come online; activists get more active
4	Cyberspace gets physical
5	New requirements shine a light in dark corners, exposing weaknesses
6	A focus on privacy distracts from other security efforts
7	Cost pressures stifle critical investment; an undervalued function can't keep up
8	A clouded understanding leads to an outsourced mess
9	New technologies overwhelm
10	The supply chain springs a leak as the insider threat comes from outside

	2015 Threats
1	The CEO doesn't get it
2	Organisation can't get the right people
3	Outsourcing security backfires
4	Insiders fuel corporate activism
5	Hacktivists create fear, uncertainty and doubt
6	Crime as a Service (Caas) upgrades to v2.0
7	Information leaks all the time
8	BYOC (bring your own cloud) adds unmanaged risk
9	Bring your own device further increases information risk exposure
10	Government and regulators won't do it for you

	2016 Threats
1	Nation-state backed espionage goes mainstream
2	A Balkanized Internet complicates business
3	Unintended consequences of state intervention
4	Service providers become a key vulnerability
5	Big data = big problems
6	Mobile apps become the main route for compromise
7	Encryption fails
8	The CEO gets it, now you have to deliver
9	Skills gap becomes a chasm
10	Information security fails to work with new generations

No-one left to trust in cyberspace

1 Nation-state backed espionage goes mainstream

Government espionage activities that were formerly mostly covert are now out in the open, encouraging all nation states to join in the game. The result will be an even more unruly cyberspace trading environment.

Actions to take now:

- Participate in threat intelligence sharing forums and build relationships with other organisations within and across industry sectors.
- Ensure appropriate information security knowledge and awareness is in place across the organisation.

2 A Balkanized Internet complicates business

Nation states will take a local approach to Internet governance, attempting to draw geopolitical borders on the Internet.

Actions to take now:

- Coordinate and maintain partnerships for information sharing across industry sectors to support cyber resilience.
- Engage in external multi-stakeholder governance processes to share intelligence.

3 Unintended consequences of state intervention

Organisations that are not directly implicated in wrong-doing will increasingly suffer collateral damage as authorities try to police 'their corner of the Internet'.

Actions to take now:

- Build resilience and implement proportional security measures in the event that this threat materialises.
- Work closely with public relations and marketing to prepare a message for customers in the event that customer-facing interfaces are taken offline.

Confidence in accepted solutions crumbles

4 Service providers become a key vulnerability

Service providers will become a key vulnerability in organisations' supply chains as cybercriminals target them rather than organisations directly.

Actions to take now:

- Foster strong working relationships with service providers with the aim of becoming partners.
- Understand clearly which legal jurisdictions govern your organisation's information.

5 Big data = big problems

Organisations that put blind faith in big data will base strategic decisions on faulty or incomplete datasets.

Actions to take now:

- Ensure the organisation has adequate skillset to analyse big data.
- Outline a process for applying big data analytics to information security problem.

6 Mobile apps become the main route for compromise

The evolution of mobile computing, its fast-paced development cycle and lack of security considerations, will make mobile apps a prime route for cybercriminals and hackers.

Actions to take now:

- Incorporate user devices into existing standards for access management.
- Promote education and awareness of BYOx (Bring Your Own Anything) risk in innovative ways.

7 Encryption fails

The default approach to secure Internet interactions, encryption, will fail to deliver due to vastly improved computing power combined with back-doors in software.

Actions to take now:

- Classify information and know where the sensitive information assets are to understand where you face the most risk.
- Identify current cryptographic solutions used across the organisation. Determine a strategy for improving their implementation.

Failure to deliver the cyber resilience promise

8 The CEO gets it, now you have to deliver

The CEO will call upon the CISO to demonstrate value that they may be unable to deliver.

Actions to take now:

- Build strong credibility for the CISO by positioning the security function as a centre of excellence.
- Align the security function with the organisation's approach to risk management.

9 Skills gap becomes a chasm

The skills gap will widen. At the same time it has never been more pressing for organisations to get the right people to be able to get ahead of the competition and innovate securely.

Actions to take now:

- Develop talent within the organisation and create incentives to retain existing talent, by putting in place mentoring programmes, external coaching opportunities, and promoting from within.
- Support external initiatives to develop and source new talent.

10 Information security fails to work with new generations

The business will embrace generations Y and Z whose approach to information security is in sharp contrast to current methods, challenging CISOs.

Actions to take now:

- Understand that the new generations' approach to work, socialising and privacy are vastly different from previous generations' and that they won't fit with traditional security models.
- Adapt existing policies and procedures to engage with generations Y and Z.

Where next?

Threat Horizon 2016 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
- adapt Threat Horizon for their own use
- use the ISF Threat Radar to help categorise threats – this can help prioritise and sequence actions when time and budgets are limited
- review the threats that are high priority for your organisation and consider the recommendations in the report
- refer to relevant ISF deliverables, such as ***Securing the Supply Chain: Preventing Your Suppliers' Vulnerabilities From Becoming Your Own***, ***Engaging with the Board: Balancing cyber risk and reward***, and ***Managing BYOD Risk: Staying ahead of your mobile workforce***.
- work with other organisations to collaborate on cyber security intelligence and strategies.

Threat Horizon 2016 is available free of charge to ISF Members, and can be downloaded from the ISF Member website **www.isflive.org**. Non-Members interested in purchasing the report or running the ISF Threat Radar, should contact Steve Durbin at steve.durbin@securityforum.org.

Contact

For more information, please contact:
Steve Durbin, Global Vice President
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
Email: steve.durbin@securityforum.org
Web: www.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 by 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 programme. 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.

Disclaimer