Information Security Forum

THREAT HORIZON **2018**

Lost in a maze of uncertainty

Information security threats are set to worsen. Organisations risk becoming disoriented and losing their way in a maze of uncertainty, as they grapple with complex technology, proliferation of data, increased regulation, and a debilitating skills shortage.

To assist ISF Members, the annual ISF ***Threat Horizon*** report takes a two-year perspective of major threats, describing potential implications and providing recommendations to organisations.

This year's report identifies nine specific threats that are set out under three thought-provoking themes. The themes engage with particularly difficult cyber security challenges in a way that is relevant to senior business managers, information security professionals and other key organisational stakeholders.

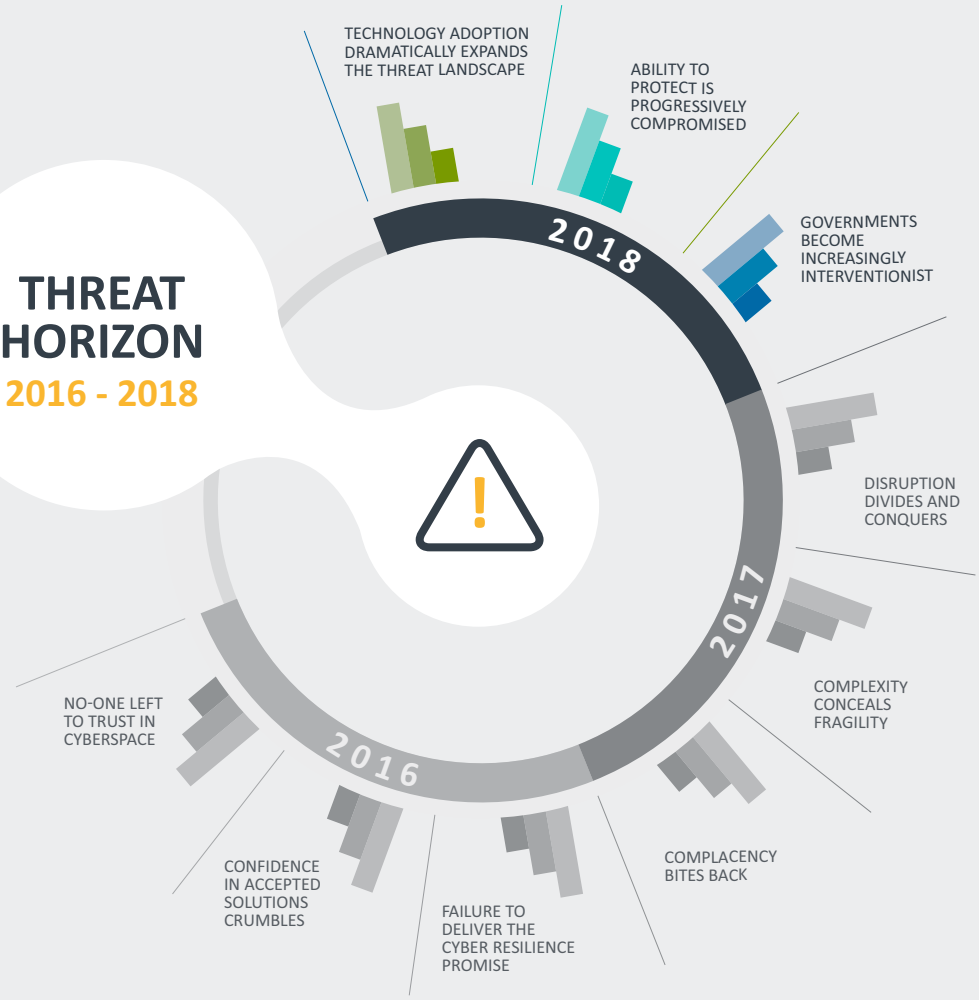
THE THEMES ARE:

- **Technology adoption dramatically expands the threat landscape:** Technology increasingly becomes an integral part of even the most mundane everyday activities, resulting in an expanded and more complex threat landscape.
- **Ability to protect is progressively compromised:** Established methods of information risk management are eroded or compromised by internal or external non-malicious actors.
- **Governments become increasingly interventionist:** Governments adopt a more intrusive approach to organisations, which is often justified as combating organised crime or deterring anti-competitive practices.

The ISF ***Threat Horizon*** report can be used in a variety of ways: stimulating discussion and debate, analysing threats, and formulating potential business impacts and responses. It offers a basis for developing a forward-looking cyber resilience strategy and bringing clarity to the complex cyber security risks that sit on the horizon.

THREAT HORIZON **2018**

Lost in a maze of uncertainty



2016

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

2017

1.1 Supercharged connectivity overwhelms defences
1.2 Crime syndicates take a quantum leap
1.3 Tech rejectionists cause chaos

2.1 Dependence on critical infrastructure becomes dangerous
2.2 Systemic vulnerabilities are weaponised
2.3 Legacy technology crumbles
2.4 Death from disruption to digital services

3.1 Global consolidation endangers competition and security
3.2 Impact of data breaches increases dramatically

2018

1.1 The IoT leaks sensitive information
1.2 Opaque algorithms compromise integrity
1.3 Rogue governments use terrorist groups to launch cyber attacks

2.1 Unmet board expectations exposed by a major incident
2.2 Researchers silenced to hide security vulnerabilities
2.3 Cyber insurance safety net is pulled away

3.1 Disruptive companies provoke governments
3.2 Regulations fragment the cloud
3.3 Criminal capabilities expand gaps in international policing

The themes and threats for 2018 are summarised below, along with some key recommendations arising from the full report.

THEME 1: Technology adoption dramatically expands the threat landscape	RECOMMENDATIONS
1.1 The IoT leaks sensitive information Organisations will adopt IoT devices with enthusiasm, not realising that these devices are often insecure by design and offer many opportunities for attackers.	• Implement security processes for adding IoT devices to a network. • Before IoT deployment, consider what information is collected and allowed to be shared, and with whom.
1.2 Opaque algorithms compromise integrity Organisations will increasingly use algorithms to maximise efficiency. However, a lack of transparency in how these algorithms interact will pose significant information security risks.	• Identify exposure to algorithm-controlled systems and understand when human involvement is a liability. • Identify alternative ways of treating risk from algorithm-related incidents.
1.3 Rogue governments use terrorist groups to launch cyber attacks These partnerships will evolve to include persistent and damaging cyber incidents, leading to business disruption and loss of trust in the effectiveness of existing security controls.	• Adapt risk management processes to account for threat actors with new capabilities. • Explore possibilities for threat intelligence collaboration with governments and organisations facing similar threats.

THEME 2: Ability to protect is progressively compromised	RECOMMENDATIONS
2.1 Unmet board expectations exposed by a major incident Board expectations will accelerate beyond the capability of their information security functions to deliver. A major incident will reveal this misalignment and create substantial business impact.	• Engage with the board regularly to provide a credible view of risk in line with their risk appetite. • Align board expectations of security improvements based on the information security function's current and future capability.
2.2 Researchers silenced to hide security vulnerabilities As security researchers uncover vulnerabilities, manufacturers will threaten them with legal action. As a result, organisations will continue to use vulnerable software that puts them at risk.	• Consider offering financial rewards to researchers who responsibly disclose vulnerabilities. • Use mediation services to agree satisfactory disclosure practices between parties.
2.3 Cyber insurance safety net is pulled away Large data breaches will drive many insurers out of the cyber insurance market and disrupt a primary method for organisations to transfer cyber risk.	• Re-assess risk management strategies in advance of a crisis. • Examine cyber insurance policies for potential costly exclusions.

THEME 3: Governments become increasingly interventionist	RECOMMENDATIONS
3.1 Disruptive companies provoke governments Aggressive commercial strategies (by companies disrupting their sector) will prompt politicians and regulators to look at the domestic commercial and security impacts of new technologies.	• Avoid political opposition by understanding the local context within which products and services are delivered. • Develop a strategy for political influence and engagement, focusing on a principle-based system of regulation.
3.2 Regulations fragment the cloud Regulatory and legislative changes will impose new restrictions on how personal data is handled. This will delay the deployment of cloud services, without necessarily achieving the desired improvements to data protection.	• Understand how regulations and legislation could evolve in light of growing demand for greater data protection. • Be proactive and prepare for change in regions where regulatory sentiment is shifting.
3.3 Criminal capabilities expand gaps in international policing The technical capabilities of cyber criminals will surpass those of organisations. The ability of current control mechanisms to protect organisations is likely to diminish, exposing them to greater impact.	• Put appropriate controls and systems in place and build a threat intelligence capability • Proactively influence governments to cooperate and build effective international legal frameworks.

WHERE NEXT?

Threat Horizon 2018 contains detailed descriptions of nine key threats along with details of potential business impacts, recommended actions and other ISF material which enables you to build your cyber resilience.

We recommend that ISF Members:

- review the threats in the report, identifying those that are of high priority
- use ***ISF Live*** to become familiar with the techniques ISF Members have used to implement ***Threat Horizon***
- consider how the contents of ***Threat Horizon*** can be adapted to work best within your organisational culture, for example to:
  - develop a forward-looking cyber resilience strategy
  - enable threat analysis and formulation of potential impacts and responses
  - brainstorm risk treatments
- use the ISF Threat Radar with senior business managers to help categorise and prioritise threats and actions: particularly when time and budgets are limited
- give careful consideration to the ISF resources in this report including ***Information Risk Assessment Methodology 2 (IRAM2), The Standard of Good Practice for Information Security, Engaging the Board: Balancing cyber risk and reward, Supply Chain Assurance Framework: Contracting in confidence,*** and ***Cyber Insurance: Covering the basics***
- work with other organisations to collaborate on threat intelligence and strategies.

The report 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 should contact Steve Durbin at steve.durbin@securityforum.org.

CONTACT

For further information contact:

Steve Durbin, Managing Director
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