Information Security Forum

Press Release | **27 March 2019**

Information Security Forum launches **Threat Horizon 2021**

Annual report identifies emerging security themes organizations will face over the next two years as a result of technology change.

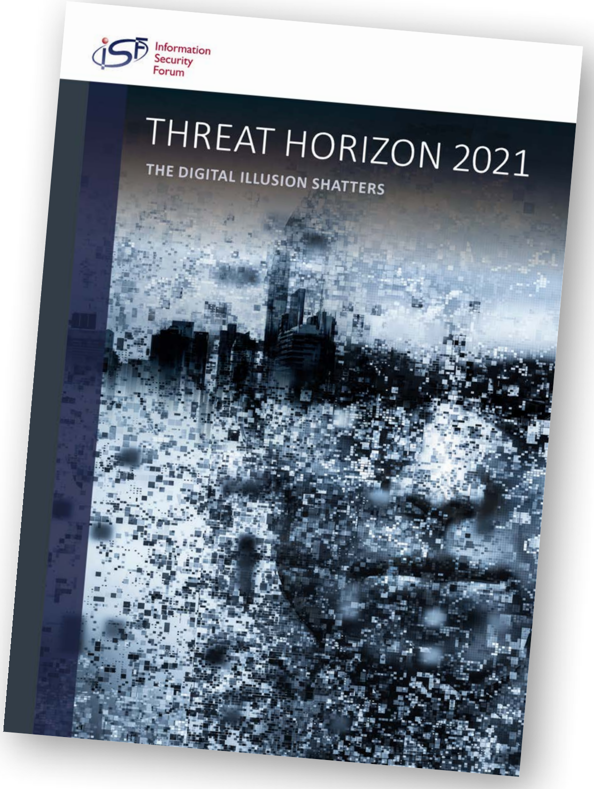
The Information Security Forum (ISF), the trusted resource for executives and board members on cyber security and risk management, today released ***Threat Horizon 2021***, the latest in a series of annual ***Threat Horizon*** reports. Developed for business leaders who need to rapidly grasp emerging information security threats and assess the potential business impacts, ***Threat Horizon 2021*** balances today's realities with forecasts that push the limits of thinking. The latest report highlights nine major threats, broken down into three themes, that organizations can expect to face over the next two years as a result of increasing developments in technology. The impacts of these threats mirror day-to-day operations in today's increasingly fractured world.

"By 2021 the world will be heavily digitized. Technology will enable innovative digital business models and society will be critically dependent on technology to function," said Steve Durbin, Managing Director, ISF. "This new hyperconnected digital era will create an impression of stability, security and reliability. However, it will prove to be an illusion that is shattered by new vulnerabilities, relentless attacks and disruptive cyber threats."

Threat Horizon 2021 focuses on particularly difficult cyber security challenges in a way that is relevant to senior business managers, information security professionals and other key organizational stakeholders.

The three key themes in the latest report include:

1 – DIGITAL CONNECTIVITY EXPOSES HIDDEN DANGERS: Vast webs of intelligent devices, combined with increased speeds, automation and digitisation will create possibilities for businesses and consumers that were previously out of reach. The Internet of Things (IoT) will continue to develop at an astonishing rate, with sensors and cameras embedded into a range of devices across critical infrastructure. The resulting nexus of complex digital connectivity will prove to be a weakness as modern life becomes entirely dependent on connected technologies, amplifying existing dangers and creating new ones.



2 – DIGITAL COLD WAR ENGULFS BUSINESS: Vast webs of intelligent devices, combined with increased speeds, automation and digitisation will create possibilities for businesses and consumers that were previously out of reach. The Internet of Things (IoT) will continue to develop at an astonishing rate, with sensors and cameras embedded into a range of devices across critical infrastructure. The resulting nexus of complex digital connectivity will prove to be a weakness as modern life becomes entirely dependent on connected technologies, amplifying existing dangers and creating new ones.

3 – DIGITAL COMPETITORS RIP UP THE RULEBOOK: Competing in the digital marketplace will become increasingly difficult, as businesses develop new strategies which challenge existing regulatory frameworks and social norms, enabling threats to grow in speed and precision. Vulnerabilities in software and applications will be frequently disclosed online with ever-decreasing time to fix them. Organizations will struggle when one or more of the big tech giants are broken up, plunging those reliant on their products and services into disarray. Organizations will rush to undertake overly ambitious digital transformations in a bid to stay relevant, leaving them less resilient and more vulnerable than ever.

“Organizations that adopt a proactive approach to the management of cyber risks should review the threats – the product of significant ISF Member engagement and research – in their own organizational context. Engaging with senior leaders and risk stakeholders they should further adapt the threats using the ISF Threat Radar to both visualize impacts and to agree business responses to those threats,” continued Durbin. “Above all, ***Threat Horizon 2021*** is a powerful tool to engage and prepare organizations for the digital future.”

The ISF Threat Radar (The Radar) has been developed as a visual aid created to accompany ***Threat Horizon*** reports. The Radar is designed to help record relevant future threats to information presented in ***Threat Horizon*** reports or that are identified as specific to the organization. This includes: assessing the potential impact of these threats, determining the organization’s ability to manage these threats and prioritizing plans and investment needed to remediate threats. The Radar can also facilitate engagement with the board, offering a way to visualise the extent of impending threats to the organisation and to identify areas that require investment or further development to support the business in the future.

Threat Horizon 2021, aimed at senior business executives up to and including board level, provides a practical, 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. For more information on the report, and to download a copy of the executive summary, please visit **www.securityforum.org.**

MEDIA CONTACT

NORTH AMERICA
John Kreuzer
Lumina Communications
Tel: +1 (408) 896 3307
Email: jkreuzer@luminapr.com

About the Information Security Forum

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organizations 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 organizations 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. By working together, ISF Members avoid the major expenditure required to reach the same goals on their own. Consultancy services from the ISF provide Members and Non-Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products.

For more information on ISF Membership, please visit **www.securityforum.org**