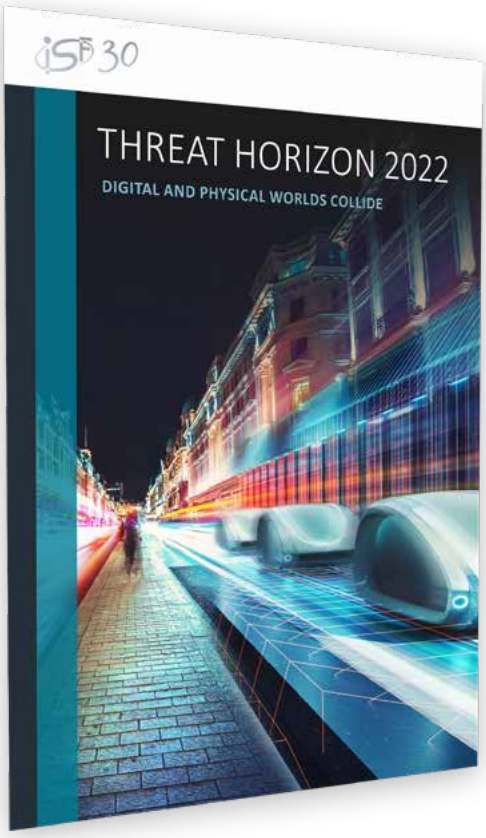
**PRESS RELEASE | 16 APRIL 2020**

# Information Security Forum Launches **Threat Horizon 2022**

## 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), trusted resource for executives and board members on cyber security and risk management, today released ***Threat Horizon 2022***, the latest in a series of annual Threat Horizon reports. Developed for business leaders who need to quickly grasp emerging information security threats and assess the potential business impacts, ***Threat Horizon 2022*** balances today's actualities 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.

"By 2022, organizations will be plunged into crisis as merciless attackers exploit weaknesses in immature technologies and take advantage of an unprepared workforce. At the same time, natural forces will wreak havoc on infrastructure. Invasive technologies will be embraced across both industry and consumer markets, creating an increasingly tumultuous and unpredictable security environment," said Steve Durbin, Managing Director, ISF. "Organizations will have to adapt quickly to survive when digital and physical worlds collide. Those that don't will find themselves exposed to threats that will outpace and overwhelm them."




***Threat Horizon 2022*** 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 – INVASIVE TECHNOLOGY DISRUPTS THE EVERYDAY:** New technologies will further invade every element of daily life with sensors, cameras and other devices embedded in homes, offices, factories and public spaces. A constant stream of data will flow between the digital and physical worlds, with attacks on the digital world directly impacting the physical and creating dire consequences for privacy, well-being and personal safety.

**2 – NEGLECTED INFRASTRUCTURE CRIPPLES OPERATIONS:** The technical infrastructure upon which organizations rely will face threats from a growing number of sources: man-made, natural, accidental and malicious. In a world where constant connectivity and real-time processing is vital to doing business, even brief periods of downtime will have severe consequences. It is not just the availability of information and services that will be compromised – opportunistic attackers will find new ways to exploit vulnerable infrastructure, steal or manipulate critical data and cripple operations.

**3 – A CRISIS OF TRUST UNDERMINES DIGITAL BUSINESS:** Bonds of trust will break down as emerging technologies and the next generation of employee's tarnish brand reputations, compromise the integrity of information and cause financial damage. Those that lack transparency, place trust in the wrong people and controls, and use technology in unethical ways will be publicly condemned. This crisis of trust between organizations, employees, investors and customers will undermine organizations' ability to conduct digital business.

"The purpose of our Threat Horizon series of reports isn't to be alarmist. What these reports are there to do is highlight potential threats that allow organizations to put in place an appropriate response if they consider those threats to be a very real risk to their business," continued Durbin. "What our latest Threat Horizon report does is reflect that yes, digital and physical worlds are combining, but much more importantly, reflects that we're going to have to change our overall thinking about the way that we deal with the risks that emanate from some of these threats. If we're going to be effective, we need to address many of these issues that we've just scratched the surface on all the way through to 2022."

Engaging with senior leaders and risk stakeholders, organizations should further adapt the threats using the ISF Threat Radar (The Radar) to both visualize impacts and to agree business responses to those threats. The Radar has been developed as a visual aid created to accompany Threat Horizon reports and has been 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 visualize the extent of impending threats to the organization and to identify areas that require investment or further development to support the business in the future.

***Threat Horizon 2022***, 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 **ISF website**.

---

## 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. The organization 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 are available and provide ISF 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**