Information Security Forum

Press Release | **29 November 2018**

Information Security Forum Forecasts **2019 Global Security Threat Outlook**

Ransomware, legislation, supply chains and smart devices top list of key threats to businesses.

The Information Security Forum (ISF), the trusted source that senior security professionals and board members turn to for strategic and practical guidance on information security and risk management, has announced the organization's outlook for the top global security threats that businesses will face in 2019. Key threats for the coming year include:

- The Increased Sophistication of Cybercrime and Ransomware
- The Impact of Legislation
- Smart Devices Challenge Data Integrity
- The Myth of Supply Chain Assurance

The coming year will bring a hyper-connected world where the pace and scale of change, particularly in terms of technology, will have accelerated substantially. People will find themselves caught in a vortex of economic volatility and political uncertainly far beyond the levels experienced before. As for organizations, some will prosper in this new world, many will struggle – the key differentiating factor will be the degree to which organizations are prepared to meet the challenges.

"In 2019, business leaders need to develop cutting-edge ways to deal with new regulation, advanced technology and distorted information," said Steve Durbin, Managing Director of the ISF. "Organizations must also prepare themselves for unprecedented levels of collaboration. Legal, compliance, audit, HR, IT, information security and other stakeholders must congregate to assess risks and inform the decision-making process. This collaboration should be extended to partners, manufacturers, vendors and regulators to ensure information security requirements are met."

The top threats identified are not mutually exclusive and can combine to create even greater threat profiles. The most prevalent threats include:

THE INCREASED SOPHISTICATION OF CYBERCRIME AND RANSOMWARE

Criminal organizations will continue their ongoing development and become increasingly more sophisticated. Some organizations will have roots in existing criminal structures, while others will emerge focused purely on cybercrime. Organizations will also struggle to keep pace with this increased sophistication and the impact will extend worldwide, with malware in general and ransomware in particular becoming the leading means of attack. While overall damages arising from ransomware attacks are difficult to calculate, some estimates suggest that there was a global loss in excess of $5 billion in 2017. On the whole, the volume of new mobile malware families grew significantly throughout 2017, in particular mobile ransomware. This should be expected to continue in 2019. Email-based attacks such as spam and phishing (including targeted spear phishing) are most commonly used to obtain an initial foothold on a victim's device. Cyber criminals behind ransomware will shift their attention to smart and personal devices as a means of spreading targeted malware attacks.

THE IMPACT OF LEGISLATION

National and regional legislators and regulators that are already trying to keep pace with existing developments will fall even further behind the needs of a world eagerly grasping revolutionary technologies. At present, organizations have insufficient knowledge and resources to keep abreast of current and pending legislation. Additionally, legislation by its nature is government and regulator driven, resulting in a move towards national regulation at a time when cross border collaboration is needed. Organizations will struggle to keep abreast of such developments which may also impact business models which many have taken for granted. This will be of particular challenge to cloud implementations where understanding the location of cloud data has been an oversight.

SMART DEVICES CHALLENGE DATA INTEGRITY

Organizations will adopt smart devices with enthusiasm, not realizing that these devices are often insecure by design and therefore offer many opportunities for attackers. In addition, there will be an increasing lack of transparency in the rapidly-evolving IoT ecosystem, with vague terms and conditions that allow organisations to use personal data in ways customers did not intend. It will be problematic for organizations to know what information is leaving their networks or what is being secretly captured and transmitted by devices such as smartphones, smart TVs or conference phones. When breaches occur, or transparency violations are revealed, organizations will be held liable by regulators and customers for inadequate data protection.

THE MYTH OF SUPPLY CHAIN ASSURANCE

Supply chains are a vital component of every organization's global business operations and the backbone of today's global economy. However, a range of valuable and sensitive information is often shared with suppliers and, when that information is shared, direct control is lost. In 2019, organizations will discover that assuring the security of their supply chain is a lost cause and instead, it is time to refocus on managing their key data and understanding where and how it has been shared across multiple channels and boundaries, irrespective of supply chain provider. This will cause many organizations to refocus on the traditional confidentiality and integrity components of the information security mix, placing an additional burden on already overstretched security departments. Businesses that continue to focus on assuring supply chain security with traditional approaches, such as self certified audit and assurance, may preserve the illusion of security in the short term but will discover to their peril that the security foundations they believed to be in place were lacking.

ISF THREAT HORIZON REPORTS

Each year, the ISF releases their latest ISF Threat Horizon series of reports, aimed at both senior business executives and information security professionals. These reports are designed to help organizations take a proactive stance to security risks by highlighting challenges in the threat landscape and identifying how the confidentiality, integrity and availability of information may be compromised in the future. For more information, please visit the ISF website and register for Steve Durbin's presentation detailing these threats, which takes place Tuesday, December 11 at 8 a.m. (ET), via this link.

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 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**