The Information Security Forum (ISF), the world’s leading independent authority on cyber security and information risk management, today released *Threat Intelligence: React and Prepare*, the organization’s latest report which equips organizations to gain value from threat intelligence by implementing the ISF Approach for Managing a Threat Intelligence Capability. Threat intelligence has been growing in prominence and most organizations have considered building a threat intelligence capability, however many question the potential value. The answer lies in understanding how threat intelligence is produced, its content and how it can be used.

“While organizations continue to rely on well-established security practices, many are seeking additional ways to keep pace with the increasing torrent of attacks” said Steve Durbin, Managing Director, ISF. “To efficiently manage cyber risks, organizations must build an accurate view of the threats they face – their capabilities, intentions and actions – and respond accordingly. Many organizations are looking to threat intelligence for this view of their adversaries, but often find it to be ill-defined, costly to buy or produce, and difficult to integrate into decision making. This leads to a failure to deliver the expected business aims.”

Threat intelligence is information about past, present and predicted attacks against an organization from adversarial threats and is produced through analysis of available information. This insight supports information security professionals to make better decisions when managing cyber risk and enables actions that prepare the organization to not only react to today’s threats, but also prepare for the future.

In today’s climate of insecurity, threat intelligence is fast becoming a crucial tool which delivers advantage over adversaries and competitors alike.
However, ISF research has found that threat intelligence is failing to deliver on its promise. While 82% of ISF Members surveyed have a threat intelligence capability, with the remaining 18% planning to implement one in the next twelve months, only 25% of those surveyed believe their capability is fully delivering the expected business objectives. *Threat Intelligence: React and Prepare* addresses the five common problems that cause this failure and explains how to build and manage a threat intelligence capability which delivers palpable value. Only once these actions have been taken will threat intelligence deliver on its promised value, supporting those business goals which so often remain unfulfilled.

“While threat intelligence seldom leads to control over adversaries, it enables the organization to make more informed decisions in the areas it does control, the vulnerabilities and associated business impact,” continued Durbin. “To ensure threat intelligence delivers value, we recommend that organizations use the ISF Approach for Managing a Threat Intelligence Capability, which provides the ISF definition for threat intelligence, reinforced by three key concepts: the production, content and use of threat intelligence. The ISF Approach for Managing a Threat Intelligence Capability uses the intelligence cycle to produce threat intelligence which meets the requirements to inform decisions and enable actions. It also addresses a number of practical considerations which affect the management of a threat intelligence capability.”

Organizations must prepare themselves for unprecedented levels of collaboration to counter threats. Innovations such as machine learning, big data and predictive analytics are already being explored by leading organizations to transform threat intelligence capabilities. The ISF Approach for Managing a Threat Intelligence Capability explains the concepts of effective threat intelligence and how they can be achieved using the intelligence cycle. Requirements-driven and skilfully produced through analysis, threat intelligence harnesses the expertise and experience of others to provide insight into past, present and predicted attacks against an organization. This insight bolsters security decision making and enables organizations to act.

*Threat Intelligence: React and Prepare* is aimed at senior business executives, up to and including board level, who are considering, planning, building or operating a threat intelligence capability. For more information on the report, and to download a copy of the executive summary, please visit [www.securityforum.org](http://www.securityforum.org).

### 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](http://www.securityforum.org)

### MEDIA CONTACT

**NORTH AMERICA**

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