The Information Security Forum's Threat Horizon 2015 Report - More danger from known threats

- Area: ROADMAP FOR THE FURTHER EVOLUTION OF THE INTERNET GOVERNANCE ECOSYSTEM
- Entitled by: William Beer
- Region: Brazil
- Organization: Alvarez & Marsal (Information Security Forum Agent for Brazil)
- Sector: Private Sector
- Keywords: Cyber, Risk, Governance, Threats
- Doc Attached: Click here to see the doc 1
- Doc Attached: Click here to see the doc 2

Abstract

The Information Security Forum (ISF) is the world's leading authority on information risk management. A not-for-profit organisation, that supplies authoritative opinion & guidance on all aspects of information security. The annual ISF Threat Horizon report provides a practical way for organisations to take a 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. Understanding threats is fundamental to enterprise risk management; threats need to be evaluated in the context of the organisation to determine risk. The ISF?s 2015 Threat Horizon report finds that the biggest risk is from known threats. The fact that hacktivism and malicious software have been around for sometime doesn?t mean they?re less threatening and we can relax - quite the opposite.

Document

Understanding threats is fundamental to enterprise risk management; threats need to be evaluated in thecontext of the organisation on to determine risk.

This year’s Threat Horizon report fi nds that the biggest risk is from known threats. The fact that hacktivism and malicious software have been around for some it me doesn’t mean they’re less threatening and we can relax – quite the opposite. Known threats, because they’ve matured, are more dangerous and pose more risk to our organisation ons than ever. They’re more sophisticated and more effective. Whether they’re old or new is much less important than their potential to do harm.

The annual ISF Threat Horizon report provides a practice cal way for organisations to take a 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.

This year’s report deals with the following themes:

• Cyber risk is challenging to understand and address, from CEOs that simply don’t get it to organisati ons struggling to fi nd the right people.

• Reputation is a new target for cyber attacks, from insider activists who leak information, and hackativist collectives who vote on who they dislike this week

• Criminals value your information, they’re highly motivated to obtain it, or to use what leaks out of your organisation

• The changing pace of technology doesn’t help; bring your own cloud (BYOC) and bring your own device (BYOD) also bring their own risks

• The role of governments must not be misunderstood: while they have a key role to play, they won’t lead cyber security eff orts – they expect organisations to manage risks in cyberspace and prevent information and systems from being compromised

ISF Threat Horizon reports are written for a non-technical audience, and ISF Members use them for many purposes, for example as a communications and awareness tool, to align business and security strategy, and to influence their organisation’s risk appettite. This report contains recommendations and references to ISF influence on s te.deliverables and other external resources which can helpaddress these risks.