

PRESS RELEASE



...making excellence a habit.™

AUSTRALIAN ORGANIZATIONS FACING ACUTE THREAT OF CYBER ATTACKS

Australian organizations are facing increasingly demanding challenges, with the risk of cyber attack rising by 250% since 2010¹, warned BSI today.

In an address delivered in Sydney, Mr Howard Kerr, Chief Executive of BSI, warns of the increasing prevalence and complexity of the threats to cyber security.

“Organizations that don’t effectively address the risks and possibility of cyber attack, whether malicious or unintentional, do so at their peril,” cautioned Mr Kerr.

“The changing face of technology has brought great benefits to the work environment and transformed how we work, store and access data,” he explained, “Yet in stark contrast has exposed the majority of organizations to the potential for attack.”

Threats to an organizations cyber security present a critical challenge in terms of scale, complexity and impact – with business assets such as corporate and customers data, intellectual property and brand reputation at risk,” he explained.

Cyber attacks have cost Australia over \$1 billion² in the past year and affected five million people.

Organizations are facing renewed vulnerability³ with technology pervading every aspect of their operations.

The volumes of business data being managed are doubling every 1-2 years⁴ and putting a strain on IT infrastructure and cloud computing has seen strong growth recently with large amounts of commercially sensitive information being stored outside of the corporate perimeter.

Driven by the business benefits they bring, more flexible ways of working are becoming increasingly popular yet paradoxically creating new security challenges.

Outsourcing, mobile working and BYOD (as opposed to company-issued devices) has risen exponentially over the past few years yet almost a quarter of organizations having experienced a serious security incident due to the connection of a personal device onto their network⁵.

¹ Symantec Internet Security Threat Report 2013

² ARN – Cyber crime costs Australians \$1.06 billion. 16 October 2013

³ Sourcefire Vulnerability Research Team, NVD Common Vulnerability Scoring System Support v2 (Incomplete data) <http://nvd.nist.gov/cvss.cfm>

⁴ KnowIT Information Systems - <http://knowwpcarey.com/article.cfm?cid=25&aid=1171>

⁵ Security for Business Innovation Council 2010

PRESS RELEASE

"All of these developments are making information security increasingly difficult to manage with threats are growing in sophistication and impact and greater penalties being imposed by regulators for breaches and the risks associated with reputational damage," continued Mr Kerr.

"The scale of the problem remains unquantifiable: not only are Governments and their supply chains being attacked," he explained, "but the magnitude of the problem remains an unknown.

Governments are attempting to address the risks with the UK, US EC and Australian Governments implementing strategies. But, as Mr Kerr stressed, no one can afford to be complacent and it's imperative that their practices are in line with today's business environment to protect their assets and reputation.

The 2013 revision by BSI of the internationally recognised standard, ISO 27001 Information Security, combined with the launch of Star Certification for cloud security providers represents a comprehensive outcomes-based approach to ensure enterprise confidence in addressing cyber security. ISO 27001 is one of the fastest growing management systems globally and the revision of the standard will enable businesses of all sizes and sectors to address the cyber security threat.

"The challenges currently faced are quite phenomenal and with the introduction of the cloud, these issues potentially impact the whole supply chain," concluded Mr Kerr.

- ENDS -

Notes to Editor

The revised BS ISO/IEC 27001:2013 and BS ISO/IEC 27002:2013 standards have been published. ISO/IEC 27001 is one of the fastest growing management system standards used around the globe. The standard is used for third-party accredited certifications with at least 17,500 certificates having been issued in 100 countries with a continual trend of double digit growth year-on-year. Its use is supported by Code of Practice document ISO/IEC 27002. Both were developed through consensus of the international community with a membership of over 47 national standards bodies.

STAR Certification is a unique new certification which has been developed to address specific issues relating to cloud security as an enhancement to ISO/IEC 27001.

To respond to growing business concerns the Cloud Security Alliance (CSA), a not-for-profit organization with a mission to promote best practice in cloud computing, created the Cloud Control Matrix (CCM). Developed in conjunction with an industry working group, it specifies common controls which are relevant for cloud security.

In partnership with the CSA, BSI has developed STAR Certification based on the matrix which certifies a client against the controls as well as awarding a Gold, Silver or Bronze STAR rating depending on how well the system has been embedded into an organization.

To learn more, please visit: bsigroup.com/en-au

Enquiries:

BSI Marketing Department

Tel: +61 2 8877 7131

Email: marketing.au@bsigroup.com