



PRESS RELEASE

Contacts:

Josh Anstey
Elcom
josha@elcom.com.au
1300 435 266

Guy Lerner
Watterson Marketing Communications
guy.lerner@watterson.com.au
(02) 9929 7533

Australian companies unconcerned about Web 2.0 security

Survey shows majority of companies give users access to Web 2.0 applications despite acknowledging security threats

Sydney, Australia (March 17, 2009) – A local industry survey conducted this month has revealed a startling paradox between the acknowledged security threat of Web 2.0 applications and the access given to everyday users during business hours.

While 92 per cent of respondents claimed to allow their employees access to Web 2.0 applications such as social networking, blogs and wikis, 71 per cent considered the consumer technology typically used to access these services as security threats.

The survey, which sampled high-level decision makers, managers, Web specialists, system analysts and engineers at a Web 2.0 security seminar hosted by Sydney-based enterprise content management company, Elcom, and IT systems integrator Regal IT, also showed that 47 per cent of companies were not increasing their spend on security despite the perceived threat.

“Most of the people we surveyed said they were comfortable with their current security platforms, which suggests we’re on the right road when it comes to the platforms we’re building,” said John Anstey, CEO, Elcom.

“That doesn’t mean we should become complacent about security, and I think the current economic situation we find ourselves in could well be a mitigating factor in companies’ hesitation on spending more, despite the threat. What this does is elevate the risk level for everyone, so as an industry we have to stay on our guard and make sure we continue to follow best practices when it comes to developing Web platforms and deploying Web 2.0 applications.”

Anstey’s comments were backed up by security firms Websense and Sense of Security, who presented at the briefing. Phil Vasic, ANZ country manager for Websense, said that in the last six months criminals have really stepped up their game

in a few notable areas.

“Spammers are increasingly using links to malicious Web sites and spam sites in their email campaigns to lure users and evade security systems that lack Web intelligence,” said Vasic.

“We're also seeing an increase in cybercriminals taking advantage of the growing number of Web 2.0 properties that allow user-generated content. More than ever we're seeing attackers inject Web sites with links and iFrames to direct users to malicious and compromised sites with the ultimate purpose of stealing data.”

Sense of Security's Murray Goldschmidt said a major threat comes from corporations developing and deploying applications, which are not securely coded, that end up being vulnerable to attack and are easily exploited.

“The current top Web 2.0 security risks are similar to those we have seen for many years in more traditional Web applications,” he said. “You need to get down to the basics and design applications from the ground up with a security mindset. In other words, when developing or deploying Web 2.0 applications, you need to understand the purpose of the application, embrace the benefits and cover all the attack vectors through appropriate controls and sound security principles.”

Regal IT managing director Mark Gluckman had a more sobering view: “the biggest risk companies face is their own staff.”

“IT departments can always upgrade to the newest and best security technologies, but it's their own people that will always be the weakest link,” he said.

“Cybercriminals will always manage to find ways to attract people using new and appealing methods, using this to gather or alter important information. Companies need to decide what data is important and ensure that this data is protected from theft and any sort of unauthorised changes. These technologies are available, at a price, and companies will need to consider the balance between the value of their data, value of its loss to the company, and the cost of protecting it.”

The survey showed the most popular Web 2.0 application to be social networking (51 per cent), followed closely by wikis (49 per cent) and blogs (38 per cent).

* * * * *

About Elcom

Founded in 1996 with the vision of developing customisable internet software products and solutions that could be integrated into any organisation, Elcom is today one of Australia's leading and most prolific web application development companies. Elcom develops enterprise content management systems (ECMS) and online commerce applications for secure internet, extranet and intranet sites, enabling customers to take advantage of the internet to build websites, portals, B2B and B2C applications. Elcom's customers include some of the largest blue-chip names in the automotive, retail, property development, healthcare, government and education sectors in Australia. For more information, visit www.elcom.com.au

About Regal IT

Regal IT provides Australia-wide IT consulting services to value-add to your computer network or system. Our consulting services provide IT solutions for access delivery, network integration and system integration. We are committed to delivering personalised service with our service desk and our 24/7 support to assist you with any queries. Explore our site to find out more about us and how our preferred IT solutions can help your business obtain a fully optimised and integrated IT system. For more information, visit www.regal-it.com.au

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, data and email security solutions, provides Essential Information Protection for more than 43 million employees at organisations worldwide. Distributed through its global network of channel partners, Websense software and hosted security solutions help organisations block malicious code, prevent the loss of confidential information and enforce Internet use and security policies. For more information, visit www.websense.com

About Sense of Security

Sense of Security provides a comprehensive range of IT security risk management services centered around IT security assessment, architecture and implementation. Our services have been specifically designed to assist organisations identify and evaluate IT security risks (through security assessments, security audits, and security tests) and to design and implement security solutions which mitigate any exposures through strategic IT security, policy and technology initiatives. For more information, visit www.senseofsecurity.com