



Networking or not working?

Protecting against social networking threats is a priority.

– Mark Padginton, Information Safe, Channel Development Manager.

From file sharing and public instant messaging through to Unified Communications and collaboration, the soaring popularity of social networking has made today's internet an even more complex environment for organisations to manage. Worldwide over 200 million people use Facebook; 45 million people connect to each other through LinkedIn and 44 million micro blog on Twitter. In New Zealand, iconic businesses such as Air New Zealand, Telecom and Vodafone, as well as a number of government organisations, already use social networks to “connect and share” business information.

However, the increased popularity of social networking has also created new concerns around network security. Inbound threats are becoming increasingly complex to manage, with viruses, malware, SPIM (spam over IM) and inappropriate content being propagated over social networking channels. Outbound threats can include organisational information leaks of intellectual property and corporate or personal financial information, which could lead to identity theft.

IT administrators and security managers who try to block these social networking environments will soon discover that many social networking applications are highly evasive and difficult to manage through traditional security technology. The goal of many social networking applications is to provide ubiquitous access to create a positive end-user experience, so simply blocking specific native ports will cause the application to find another route to connect with its intended recipient. Many of these applications will apply Port/Protocol Tunnelling, P2P/Onion Routing or Random Session Behaviour to ensure connectivity.

Over May and June this year, FaceTime Communications, whose technology enables the safe and productive use of instant messaging, web usage and Unified Communications platforms, conducted a survey on web 2.0 with an emphasis on social networking. The results of the survey highlighted that IT administration is vastly underestimating the use of social networking by its employees.

In the survey, which consisted of 1199 participants (43% representing organisations with greater than 1000 employees), less than 15% said they do not use social networking at all. Most employees use it once to twice a week, with 39% logging into social networking sites at least once a day. This led to nearly 40% of administrators surveyed saying they believe that employees are using social networking sites for between one and five hours per week.

The survey results showed that information leakage is of primary concern for administrators, followed by staff productivity (too much social activity), security (backdoor attacks) and brand awareness.

Despite these concerns, almost 50% of the IT professionals said that social networking has some business value. However, the vast majority (73%) said virtual worlds (such as Second Life) have “no business value”, while 58% felt the same about IPTV and 45% about iTunes.

The real question for key administrators, however, is how best to control social networking to reap the benefits and escape the traps. Forty-three percent believe it should be allowed as long as it is controlled, because its benefits include better employee communications, faster decision times due to collaboration, improved marketing communications and an environment for sales

lead generation. However, the security issues remain. The question then is: Is the new ‘social generation’ networking or not working?

Any organisation wishing to enable the use of social networking should consider a number of factors:

- The control of information across a myriad of channels such as IM, P2P and web 2.0, and enforcing ethical communication boundaries.
- An organisation's regulatory compliance, covering regulations and mandates for archiving.
- eDiscovery of any content and the ability to present the information for either internal reviews or courts of law.
- How to manage and control malware and SPIM across multiple channels and federation boundaries.

Organisations should also consider granular application control including policy-based control of applications, such as IM, P2P, public voice over IP (VoIP), blogs, data-sharing portals, web conferencing, chat, etc.

Corporate and organisational use of social networking is fast becoming adopted as a powerful business communication tool. Social networking and web 2.0 are connecting customers, suppliers and partners, and providing measurable and sustained business value. Social networking is changing the way an organisation conducts business both today and tomorrow, and as such, its security measures must grow and evolve to meet these needs. **IT**