

# Towards 'Social' Security



## Towards 'Social' Security

It's common a catch-22 for many business and IT departments: Allow access to social media sites and the business is opened up to malicious content, phishing schemes and other evils. Declare all social media sites off-limits and employees become frustrated, find workarounds or simply elect to work elsewhere. The key is to achieve a safe compromise – through acceptable use policy tailored to each specific organisation's risk profile, and enforced through next-generation technologies.

While IT security professionals may acknowledge the many business benefits of social media use, they're also burdened with the task of shielding organisations from the cyber-threats that lurk within social networking sites. Growing concern regarding this issue is not unfounded. Research indicates that social networking sites and applications are augmenting the criminal toolkit and dramatically increasing user vulnerability. The "Global Survey on Social Media Risks," released in September 2011 by the Ponemon Institute, reveals that a large number of organisations have experienced the danger posed by sites like Facebook and Twitter first-hand. In the survey of more than 4,000 IT and IT security professionals, 52% of respondents said they've experienced an increase in malware as a result of social media.

Identity fraud or corporate espionage through employee profiling are other very real risks propagated through social media. A few minor details garnered from Facebook or Twitter could give a criminal all he needs to pose convincingly as one of your employees and persuade your helpdesk to forgo additional information that could be used to find a back door into your organisation. We're all familiar with the effect that data loss can have on a business. Whether it's a lost laptop or a cybercriminal impersonating an employee to access data, the consequences can be grave. And when you consider the frequency of social media use and the heightened possibility of attacks, businesses that don't heed the potential ramifications of social media are placing themselves at risk.

The relaxed attitude of social media users creates an increased risk of people clicking on links, performing profile updates or generally acting on something of which they would normally be more cautious. This makes malware, spear phishing and other such risks more ominous. Social media sites often operate on recommendations by 'a friend' which naturally will lower users' guards. Social media users place a level of trust in these tools as they believe they're interacting with friends and colleagues and aren't 'on guard' for any malicious activity. On the other hand, when conducting online banking, users take a cautious approach and are vigilant about exposing personal details. While conversations through Twitter and Facebook may feel as if they're happening within a small, intimate group of friends, they're a popular – and potentially lucrative – hunting ground for criminals.

Mobile social networking is on the rise, which further adds to the complexity. According to an October 2011 report by comScore, Facebook was home to the largest mobile audience of all social networking sites, attracting 57 million mobile users, followed by Twitter and LinkedIn with 13 million and 5.5 million users respectively. Moreover, 58% of the mobile social media audience access such sites almost every day. The growing trend for employees to bring their own devices into the workplace further increases organisations' risk. Individuals participating in social media channels typically update their Facebook profiles and post blogs from

their handheld devices throughout the day 'on the fly', in between meetings, while waiting for trains or during their coffee breaks. The security team is tasked with providing a 'virtual lock and key' for these devices, at all times, and irrespective of their location.

## A pressing need

The ever-growing number of social media threats – and victims – is testament to the pressing need for businesses to put this matter firmly on the agenda. Despite the increased risks, the majority of business leaders accept that social media is an important tool for meeting business objectives. If you block social media completely, you do away with its many advantages. If you allow it, you'll likely experience a higher instance of malware. It's a delicate balance to manage. You need to have a strategy for social media and have an acceptable use policy.

Nicholas Arvanitis, a Principal Security Consultant at Dimension Data comments: "Social media platforms have developed so rapidly, with the result that oftentimes IT teams haven't been able to keep up. Many fail to leverage existing defences to address new challenges posed by emerging trends such as social media. But social media is here to stay and its associated threats need to be taken seriously. And those who participate in social media need direction from their employers about the rules, accountabilities and behaviours expected of them."



## Know your risks

Arvanitis believes that there's no one-size-fits-all approach and ensuring that social media doesn't compromise security will depend on the culture of your organisation, the profile of your users and the devices they use, as well as any industry-specific or regulatory requirements by which you are bound. He asserts that to obtain a clear picture of their social media risk profile, organisations should initially conduct a risk assessment to understand what behaviours most threaten the business.

Often these 'new' security threats are old risks in a new form, which calls for you to modify your approach to dealing with

them. By understanding the differences between these risks, you can identify which area of your business is responsible for their management. Furthermore, as many business risks are misconstrued as security risks, understanding the nature of threats, whether they be technological or content-based, is critical. Thereafter, organisations should identify and deploy appropriate strategies, policies, process and, finally, technologies to plug the most troubling gaps.

"Vendors' security tools are maturing rapidly and becoming increasingly granular in their ability to guard against security breaches and attacks related to social media without purely blocking

access to the applications themselves," adds Arvanitis. There's also a great deal of choice in terms of delivery models: organisations can elect to have the solutions delivered on premise, or provided as a hosted service."

Technology, however, can only do so much; its effects will be diluted if it's not backed by a comprehensive policy. So the next, critical step is the development of a comprehensive acceptable use policy that includes guidelines for the use of social media by employees and contractors. Who will write and update the policy? Ideally, setting policy should be a co-ordinated effort between IT and other business stakeholders including marketing, human resources, public relations and the legal team. Whatever your decision, it's important to give thought to who's responsible, accountable, consulted and involved in the policy's creation.

If you already have a communications policy in place, update it to include social media matters. Prescribe the official level of presence or absence of social media and its acceptable use, in line with the existing culture of the organisation and its appetite for risk. For example, some organisations elect to allow full access to Facebook but only for a limited number of hours during the day, some choose to disallow the site's video functionality while permitting chat and e-mail. Once you've created your policy, don't forget it: You need to consistently remind your employees of the policy and keep it relevant and up to date.

It's unlikely that the policy alone will provide a 'silver bullet' to change social media behaviour in the workplace. A well-designed communication plan, backed up by a training programme, will help make your policy come to life. In addition, there may be value in involving users in the policy creation and enforcement. You might also make the process interactive, for example, by creating a pop-up alert that warns users that the e-mail they're about to send includes an unsafe attachment and that in sending the message they'll contravene the organisation's security policy. Remember that most security violations are unintentional; this approach gives users the opportunity to learn and correct their behaviour.



## Building as foundation for secure social media

Social media communications are interactive, difficult to retract and occur in real time. If they aren't monitored or managed, they can increase your business' liability or damage its reputation. Now that social media rules the day, acceptable use policies should be more the rule than the exception. Clearly documenting ground rules, expectations and repercussions for out-of-policy behaviour will ensure that end users are aware of what's considered acceptable use of social vehicles.

### Success story: Dimension Data Australia

As a forward-looking player in the technology sector, it's not surprising that Dimension Data has an established and active social media presence. The organisation's Australian business provides an example of how appropriate application of acceptable use policy can introduce an element of control over social media use, without stifling innovation and creativity.

Dimension Data's Australian business is an active participant in a host of social media vehicles. The organisation updates its Facebook page on a daily basis and it issues three new Tweets every day. While Dimension Data is a business-to-business provider of services, it recognised the remarkable value inherent in social media tools to enhance its communications with the media, industry analysts and partners, as well as foster a greater sense of community among its employees.

One of the critical first steps in charting the organisation's social media journey was to establish a comprehensive social media acceptable use policy. The aim in setting the policy was ensuring that all employees understood that social media means that everyone is a potential company spokesperson. The organisation needed

“Vendors' security tools are **maturing rapidly** and **becoming increasingly granular** in their ability to **guard against security breaches and attacks** related to social media without purely blocking access to the applications themselves.”

to ensure employees were informed and aware of what their responsibilities are and where the boundaries lay, while at the same time encouraging engagement and participation in these channels. It adopted the Dimension Data's global social media policy, and the objective is to review and update the policy at regular intervals, ensuring that any region-specific issues are included.

The organisation has adopted a rigorous and on-going employee awareness drive around its acceptable use policy for social media. “Education never ends,” explains Ian Jansen, CIO for Dimension Data in Australia.

“There's no question that putting a policy in place is essential, but it's only the first step. Policy creation, maintenance and awareness all need to work in concert.”

Corporate policy for acceptable use of social media is explained to all new employees during the induction process and they're given direct access to the online policy document on the organisation's intranet. The communications team also maintains a regular flow of e-mail reminders to employees regarding the contents of the policy and it's currently also investigating the possible development of an interactive e-learning module. Monitoring compliance

with the acceptable use policy is made easy through the functionality embedded in Radian 6, the software tool that Dimension Data has deployed enterprise-wide. The tool monitors all mentions of Dimension Data in social forums, and provides automatic alerts regarding strongly negative – or positive – commentary. This enables the organisation to capitalise on and further promote positive commentary (e.g. through retweets), and address/mediate potential problems.

“We consider social media a positive tool for encouraging collaboration and building internal and external relationships,” says Jansen.

“However, the blending of the social and work environment does create risk because the exchange of content among employees cannot be controlled and because devices the organisation doesn't own are on the network. For these reasons, we ensure our social media policy aligns closely with our mobility and 'bring your own device' strategy. The rapid proliferation in the use of social media has caught many organisations off guard. It's possible, however, to strike a balance, as Dimension Data has done, through a comprehensive acceptable use policy backed by the appropriate technologies and tools.”

**MIDDLE EAST & AFRICA**

ALGERIA • ANGOLA  
BOTSWANA • CONGO • BURUNDI  
DEMOCRATIC REPUBLIC OF THE CONGO  
GABON • GHANA • KENYA  
MALAWI • MAURITIUS • MOROCCO  
MOZAMBIQUE • NAMIBIA • NIGERIA  
RWANDA • SAUDI ARABIA  
SOUTH AFRICA  
TANZANIA • UGANDA  
UNITED ARAB EMIRATES • ZAMBIA

**ASIA**

CHINA • HONG KONG  
INDIA • INDONESIA • JAPAN  
KOREA • MALAYSIA  
NEW ZEALAND • PHILIPPINES  
SINGAPORE • TAIWAN  
THAILAND • VIETNAM

**AUSTRALIA**

AUSTRALIAN CAPITAL TERRITORY  
NEW SOUTH WALES • QUEENSLAND  
SOUTH AUSTRALIA • VICTORIA  
WESTERN AUSTRALIA

**EUROPE**

BELGIUM • CZECH REPUBLIC  
FRANCE • GERMANY  
ITALY • LUXEMBOURG  
NETHERLANDS • SPAIN  
SWITZERLAND • UNITED KINGDOM

**AMERICAS**

BRAZIL • CANADA • CHILE  
MEXICO • UNITED STATES