

opinion piece

dimension
data 

Securing Social Media



With the exponential growth in social media usage by private individuals and organisations, how do you effectively assess and manage the associated risks?

There is no denying it: social media is forcing businesses to change their behaviour. With the lines between business and personal use of technology blurring, employees are demanding that the tools they use in their personal life also be made available at work. For this reason, social media is fast becoming a key challenge for not only security and IT, but also HR and management teams. With growing concerns around productivity

and acceptable individual behaviour, social media and its use within business, is a key area of focus.

So what are the implications for the security and IT professional? How different are the risks posed by social media compared to traditional vehicles? How can these risks be mitigated? And crucially, is there a way to exploit the potential of social media without sacrificing security levels?

Social media today: what are the risks?

The first step in gaining a thorough understanding of the risks posed by social media, is identifying all the potential

threats to which your organisation is exposed. Often these 'new' security threats are old risks in a new form factor, which calls for you to modify your approach to dealing with them. Furthermore, as many business risks are misconstrued as security risks, understanding the nature of threats, whether they be technological or content-based, is critical.

By understanding the differences between these risks, you can identify which area of your business is responsible for their management.

A recent report from Gartner provides a comprehensive view on the various social media risks:

risk	description	security	type
Malware	Infection of desktops, propagation of malware through staff or corporate profiles on social-media services	Yes	Technology
Chain of providers	Mashups of applications within a social-media service enable the untraceable movement of data	Yes	Technology
Interface weaknesses	Public application interfaces are not sufficiently secured, exposing users to cross-site scripting and other exploits	Yes	Technology
Reputation damage	Degradation of personal and corporate reputations through posting of inappropriate content	No	Content
Exposure of confidential information	"Loose lips sink ships," breach of IP or other trade secrets, breach of copyright, public posting or downloading of private or sensitive personal information	Yes	Content
Legal exposure	Legal liabilities resulting from posted content and online conversations or failure to meet a regulatory requirement to record and archive particular conversations	Yes	Content
Revenue loss	For organisations in the information business, making content freely available may undercut fee-based information services	Yes	Content
Staff productivity	Workers failing to perform due to the distraction of social media	No	Behaviour
Hierarchy subversion	Informal social networks erode authority of formal corporate hierarchy and defined work processes	No	Behaviour
Social engineering	Phishing attacks, misrepresentation of identity and/or authority to obtain information illicitly or to stimulate damaging behaviours by staff	Yes	Behaviour
Identity fraud	Profiles and postings that are erroneously attributed to a staff member or corporate office	Yes	Behaviour

Social media in the workplace: does it really matter?

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. According to McAfee's 2010 Threat Predictions report, social networking sites and applications are rapidly changing the criminal toolkit and dramatically increasing user vulnerability.

The challenge is heightened by the fact that social media, by definition, is very public. We all remember the recent embarrassing security incident involving John Sawyers, the head of the Secret Intelligence Service for Britain last year. Sawyers' wife infamously posted photos of her husband, his colleagues and close family and friends on Facebook. By virtue of low privacy profile settings, updates were made to the world, effectively leaking information on the family's home address and location abroad! Ultimately, social media is forcing individuals and businesses alike to think differently about security. The reputational damage an incident like this can cause should not be underestimated.

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 backdoor into your organisation. We are all familiar with the effect that data loss and downtime 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 think about 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 frequency of communication and the relaxed attitude of social media users create 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 are 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 are a popular – and potentially lucrative – hunting ground for criminals.

Of course, businesses need to protect against malicious data being shared or downloaded through links, but it's also important to consider the underlying threat of applications existing on laptops and other devices for prolonged periods of time. These applications collect data without the user's knowledge and can potentially pose serious risks for businesses.

Responsibility

Social media undeniably exposes users to an increased risk of cybercrime. Yet organisations need to adapt to these tools and applications as undeniably, there are here to stay. Many organisations lack clarity as to who is responsible for ensuring their protection. Vendors have only recently begun to realise the need to protect users: the landmark McAfee and Facebook partnership announced recently indicates that providers are moving towards sharing security responsibility with their users. Although developments in this area look set to grow, businesses and users of social media cannot afford to become complacent. Security threats still need to be taken seriously.



How far can IT really protect you from social media threats?

Technology can only do so much. People, while an organisation's greatest asset, can also represent a potential threat. We've all seen examples in the media of employees losing unencrypted laptops or USB sticks and the potential damage these incidents can cause. Social media has only served to exacerbate the human data related risk with the frequency and speed of communication.

When it comes to managing risk, employers need to take a practical approach. For this reason, a corporate policy on social media, defined by HR, is fundamental in ensuring its acceptable use. The HR department needs to define acceptable use and implement a corporate policy aligned with the existing 'personality' of the organisation. The policy will also need to consider the business's appetite for risk. Through this evaluation, the HR department can prescribe the official level of presence or absence of social media and its acceptable use.

Some businesses may choose to lock down social media whilst others acknowledge the requirement to allow Web 2.0 tools in some form. Regardless of which approach your organisation adopts, social media exists and you should expect the demand for it to grow. If your employees want access to social media, the chances are good that they will find a way to circumvent technologies which prohibit their use. Employees may bring in their own 3G USB modems and connect directly to the corporate network and bypass security systems, or if working from home they may simply turn off their VPN. Employees will find a way to access social media, so businesses cannot afford to ignore the issue.

When it comes to managing risk, **employers need to take a practical approach**. For this reason, a corporate policy on social media, defined by HR, is fundamental in ensuring its acceptable use.

Business culture

How can you achieve this complementary balance? A key first step is assessing your business's culture and appetite for risk. While some organisations simply aren't able to take advantage of social media in any form because the risk far outweighs the benefits, others are. For example, Dimension Data realises the productivity that can be gained from instant messaging (IM) and has implemented our own enterprise-grade corporate IM network based on Microsoft Office Communication Server which resides within our perimeter security. This allows our employees to use social media tools without the compromising its security posture.

Dimension Data's Vulnerability Assessment Services

Dimension Data's Vulnerability Assessment Services enable you to understand your vulnerabilities in order to manage your threats. Effective threat management is only possible once you have a clear and comprehensive understanding of your existing security posture, vulnerabilities and risk tolerance. Once the intricacies of your organisation's individual threat landscape have been mapped out, the most suitable technologies can be implemented to provide multiple layers of defence – provided of course, that the threat landscape is updated regularly to identify new vulnerabilities.

Change in approach

As with any new technology or trend, social media and its management in the workplace until now has largely been driven by trial and error. Yet with this new highly public wave of security threats, will come a change in the approach businesses take to manage these threats. The demand for access and use of social media will continue to drive new technology and policy. Ten years ago no one had an acceptable usage policy for online activity and now this is standard. Just as the 'I Love You' virus forced businesses to address network perimeter security, social media is forcing businesses to define their business culture and define their social media and security strategy.

MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • GHANA • KENYA
MOROCCO • NAMIBIA • NIGERIA
SAUDI ARABIA • SOUTH AFRICA
TANZANIA • UGANDA
UNITED ARAB EMIRATES

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