



Social Networking: The Pros, the Cons and the Solution

Introduction

Social Networking sites such as Facebook, MySpace, LinkedIn and Bebo have permeated society and the workplace over recent years. In April 2009, Facebook reported that it had over 200 million active users worldwide, up from 50 million in October 2007. Neilsen/Net Ratings reports that in April 2009 there were over 18 million unique Facebook visitors from the UK alone, each spending on average over five hours on the social networking site during the month. The same report shows over 30 million people logging on to Facebook from the work place in the United States. Some sites are focused on letting friends and family stay in touch (MySpace, Facebook) while others, such as LinkedIn and Plaxo serve to network the business community. The most recent phenomenon is Twitter, which experienced a 1382% growth in the number of users over the period of February 2008 (475,000) to February 2009 (7,038,000) according to Neilsen/Net Ratings. With media giants such as ITV, News Corporation and Google buying up social networking sites - and other sites arriving on the scene constantly - there is little doubt that they are here to stay. Some sites are focused on letting friends stay in touch (MySpace, Facebook) while others, such as LinkedIn and Plaxo serve to network the business community.

Organizations are right to embrace these sites as an extra weapon in their sales and marketing armory. However, they need to do so secure in the knowledge that organizational and employee security is not being compromised. Unfortunately, the extremely rapid growth in popularity of these sites risks catching many IT departments unprepared. Complacency is not an option for organizations faced with such a powerful, yet potentially problematic, communications channel, which is why more and more organizations are turning to advanced content security technologies to mitigate the risks associated with social networks.

Getting the Balance Right

Social and business networking sites are changing the way people communicate with each other, both for business and pleasure. Some might think it makes sense for organizations to simply block employees' access to these sites while at work, citing cyber-slacking as the reason, but it isn't that straight forward. These sites provide employees and the organizations they work for with a very real business advantage. Some of the

benefits of allowing employees to access social and business networking sites while at work are outlined below.

Networking, collaboration and information sharing

Social networking sites can be very effective for business networking. Almost like an informal CRM system, people can use social networking sites such as LinkedIn to maintain business contacts and to introduce colleagues or contacts to one another in an informal manner. There are also some less well known social networking sites that have been set up specifically to encourage information sharing and collaboration between professionals operating in a particular industry. Sermo, for example, is a site exclusively for US physicians. It has teamed up with the pharmaceutical giant Pfizer to allow doctors direct online access to employees from the drug company, which encourages feedback and ongoing communication.

These specialized social networking sites offer much more than just an unmoderated free-for-all. Given a few restrictions in terms of membership and content, a social network can provide a valuable, easy-to-use forum for academic debate or business discussion. The use of restricted groups in Facebook is another good example of this: companies can set up a private area and use it to share ideas in an informal environment that encourages creativity.

Marketing

Social networking sites have also opened up new marketing and promotional opportunities for businesses. Companies can pay for banner ads on the sites themselves and can also create their own home pages. Appealing to the tech-savvy, less formal, Web 2.0 generation who have become used to hearing about the latest bands on MySpace, social networking sites have become a valuable, low cost marketing tool, particularly for consumer-facing organizations. Publishing corporate blogs on social networking sites can also be a very effective way of sharing information and strengthening brand image.

The MySpace generation

But it goes further than that. They also play a very important part in the lifestyle of anyone under 30: accessing social networking sites is as important to these younger employees as using their mobile phone. Preventing these

employees from using all the technology tools they take for granted will only lead to disgruntled, unhappy workers. By contrast, giving them the freedom – albeit regulated - to use these social networking sites in the workplace can help both employees, and the organizations they work for, to flourish.

Approach with caution

It is therefore important to get the balance right: allow employees to use these sites, but ensure that they do so without subjecting themselves or the organization to undue risk. Most employees will have the common sense to use these networks to socialize and do business without compromising security, but it only needs one employee to use a social networking site unwisely for the repercussions to be significant.

Threats

From a purely technical perspective, social networking is simply another example of employees accessing websites while at work. However, social networks do present specific challenges for employers due to the type of content published on these sites. Some of the key threats that organizations need to guard against are discussed below.

Viruses/Malware

The MySpace trojan (2006), the Orkut worm (2007), the Secret Crush Facebook widget (2008) and Koobface (2008 and 2009) which affected MySpace, Facebook and Bebo are examples of how criminal gangs can use Social Networking sites to their advantage. For the 'bot-herders', who can charge based on the size of their botnets, social networking sites provide an easy way to play a percentage game: with so many users, they know they can rely on some of them to become victims. And if the user is accessing the social networking site from a work PC, then the organization's whole network risks being compromised. This is especially the case when people believe they are receiving something from a friend and hence their defences are automatically lowered.

Privacy

It is very easy for people to get carried away and post too much information about themselves on social networking sites. This can lead to identity theft or phishing attacks and helps to promote cybercrime. There have also been several instances where employers or prospective employers have used information posted on these sites in evaluating employees. Many sites, such as Facebook, recommend that users do not post sensitive information on these sites and that they apply the necessary security measures to prevent their personal home pages from being viewed illicitly. That said, there have also been

some concerns over what social networks do with the information that they are privy to. Towards the end of 2007, social networking site Quechup came under a lot of fire for using its members' address books to send out spam to try and swell its ranks.

Cyberbullying/Cyberstalking

Similarly, employees using these sites are putting themselves at risk of becoming victims of cyberbullying or cyberstalking. A survey carried out by the trade union Amicus, reported that one fifth of employees in the UK were being bullied electronically. Whilst cyberbullying includes emails, it also extends to social networking sites; the overall effect can be seriously detrimental to morale within an organisation. Amicus estimates that bullying costs the UK economy over £2 billion per annum in sick pay, staff turnover and productivity. Often, a cybervictim's only recourse is to secure or remove his profile from the offending site.

Data Leakage

It is very easy for an employee to post confidential information about their company – be it unwittingly or deliberately – in a blog or on a social networking site. Whether it is the product road map, confidential financial information or even just derogatory comments about management, data leakage can lead to internal reprimands or worse: litigation, fines or even imprisonment of company officials may occur as the result of poor data control.

There are other considerations too: whilst LinkedIn and other such sites can be used advantageously as a cheap and simple CRM system, they are usually attached to an individual rather than a company, so the data becomes very portable. It would not be difficult for an employee to take the entire sales database with him to a rival after having built up an extended network of friends/business colleagues through a social networking site.

Brand Credibility

Warren Buffett said that it takes twenty years to build a reputation and five minutes to ruin it. When an organisation tries to use a social networking site to its advantage, it needs to be careful. Six major companies seeking to benefit from advertising through Facebook found their banner ads appearing on the neo-fascist British National Party's pages. They all pulled their advertisements, one of them publicly declaring that it was doing so to "protect its brand."

Lost productivity

Social networking sites can become addictive, so much so that it is relatively easy to spend two or three hours of the working day socialising online instead of working. Recent surveys indicate that 43 percent of organizations in the UK have banned the use of social networking sites at work completely, for productivity and security reasons. Indeed, in August 2007, Kent County Council banned all of its 32,000 employees from using Facebook, citing 'time-wasting' as the principle reason. This was shortly after the 'I have dossed around on Facebook all day and consequently have done no work' group had been set up.

To Ban or Not to Ban?

So where does all this leave organizations that are concerned about the use of social networking sites in the workplace? The answer is that it doesn't have to be that black and white. The technology is available – in the form of secure Web gateways – to allow employees to use social networking sites safely and securely. A secure Web gateway, such as WebMarshal, combines advanced Web access controls, data leakage prevention and inbound threat controls in one centrally managed solution or service that makes accessing social networking sites a low-risk, high-reward option for organizations.

There are both technical challenges and personal use issues that to be addressed: organizations have to determine their own modus operandi, identify and deploy the appropriate underlying technology solution and then communicate to employees how social networks can be used in accordance with their Acceptable Use Policy.

How a Secure Web Gateway Can Help

A secure Web gateway sits between the Internet and the edge of the corporate network and keeps the bad things on the outside of the organization while ensuring that the good things remain within. From a social networking perspective, a secure Web gateway enables employees to collaborate safely with business partners and friends/colleagues on approved, malware-free social networking sites, while also controlling what content can be downloaded or uploaded onto such sites. A secure Web gateway can also be used to provide bandwidth and time of day quotas to employees, to ensure that they do not waste valuable work hours, or use up valuable network bandwidth, on social networking sites.

Securing social networks with WebMarshal

WebMarshal is one of a new breed of content security solutions dubbed secure Web gateways by analysts and market commentators. It is a three-in-one solution that combines technologies for Web access control, data leakage prevention and Web threat security, all of which have a role in making social networks safe for employees. WebMarshal enables organizations to apply policies for Web security, compliance and acceptable use at the Web gateway, providing safer Web use and a more productive working environment.

Enhanced Web access control

WebMarshal's enhanced Website classification system is fundamentally different to the more standard URL filtering products on the market. WebMarshal enhances and extends URL filtering, to provide a content-based approach that automatically identifies and classifies unclassified websites based on analysis of the page content. This real-time classification, when combined with URL filtering, delivers an integrated solution that achieves the best of both approaches. It obviates the need for URL filters to scan every Website, focusing instead on scanning, checking and classifying only those Websites that a user actually attempts to visit. This means that policies can be set up quickly and easily to block employee access to any social networking site known to be a time-wasting site, for example.

WebMarshal also enables organizations to define and enforce policies concerning: the control of file downloads by file type, file size, user permissions and domain; Web application controls (e.g. restricting access to streaming video or instant messaging on social networks); and flexible employee management policies, including bandwidth and time of day quotas. Quota Management controls define how much time users can spend on particular sites and how much bandwidth users can consume over a given time frame. The result is a much more efficient and effective protection system.

Comprehensive data leakage prevention

Preventing confidential/sensitive internal information, or derogatory comments about the company or its staff, from leaving the organization via the Web gateway is another IT headache that can be removed with an effective secure Web gateway solution like WebMarshal. Intellectual property and confidential information are more than just business assets: in today's world, the security of private information such as healthcare records, financial history or revenue data is often a compliance obligation for which organizations - and sometimes also individual executives - are held accountable.

With WebMarshal, data leakage is prevented by the ability to control any content that is uploaded to the Web (e.g. files, text, etc.) and ensure, through user authentication, that unauthorized uploads do not occur. Organizations can set policies to control or block employee access to social networking sites, as well as to analyse and block text containing specific key words from being uploaded to these sites. By controlling what textual content and files are uploaded by employees, organizations can protect corporate reputation as well as confidential data.

Unparalleled inbound threat control

Building a virtual fortress to prevent attacks from the outside is another key weapon in WebMarshal's Secure Web Gateway arsenal. The solution provides real-time anti-virus and anti-spyware scanning, designed to keep out viruses, spyware, phishing and other malware found on social networking sites and other Websites. The anti-spyware integration is a particularly powerful solution that detects malicious code in the downloaded data stream and blocks it before it gets to the corporate network or user's desktop.

By adopting this level of inbound threat control, organizations are also able to provide a duty of care to their employees and prevent them from ending up as unwitting victims of phishing attacks or other fraudulent Internet activity.

Policy enforcement

Once the technology is in place, organizations should negotiate, communicate and adopt an Acceptable Use Policy (AUP) that allows enough flexibility for employees to feel as though they are trusted, but is robust enough to provide a secure environment. The most effective AUPs are usually created with input from many different areas within a corporate body, often with the help of the IT team. Part of the AUP should be that employees acknowledge that their actions are being monitored. If they know that their actions are likely to be uncovered, they will think twice about doing anything wrong. WebMarshal can play an important part in monitoring and enforcing compliance with an Acceptable Use Policy.

It is important, however, to remember that legal restrictions differ from country-to-country, and that users may have some rights to privacy while at work. In the UK, for example, the

Data Protection Act and the Employment Practices Data Protection Code, spells out that employers should only monitor employee's use of the Internet in a proportionate way.

Extending control

Managing disparate, complex networks and remote users has started to pose some problems. As network boundaries start to dissolve in favor of cloud-computing, managing users' Internet access is becoming increasingly complex.

Marshal8e6's Web security appliances, such as the R3000, allow organizations to extend their control over Social Networking sites beyond the standard network perimeter. The R3000's pass-by technology means that it can identify and block URLs transparently without having to change proxy settings on machines across the network. It is also able to analyze network traffic and identify application protocols, allowing it to block attempts by users to access anonymous proxies as well as online games, such as World of Warcraft and P2P traffic.

Used in conjunction with the Marshal8e6 'Mobile Client' software, it enables administrators to control what access remote users have to websites and they can collate that information centrally for reporting purposes.

Conclusion

While social networking sites are currently enjoying a high profile, the challenges that they pose do not differ significantly from other forms of Web-based threats. Today's employees expect to be allowed to access these sites while at work - albeit with some restrictions. Although some organizations are preventing employees from accessing such sites, the smart ones are deploying secure Web gateway technology combined with Acceptable Use Policies to keep the organization and their employees safe, while also providing a flexible working environment. Not only will this powerful combination protect against the current threats posed by social networking sites, it will also protect organizations from many, as yet unknown, Web-based threats.



Corporate Headquarters
Marshal8e6

828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Marshal8e6

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Marshal8e6

Suite 1, Level 1, Building C
Millennium Center
600 Great South Road
Auckland, New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720