WHITEPAPER: Social networking, security and your business: a guide for IT managers

Social networking, security and your business: a guide for IT managers

Love it loathe it, social networking is almost ubiquitous. This white paper examines the benefits and risks and it looks at the different ways companies can reconcile them.

Symantec.cloud

Social networking, security and your business: a guide for IT managers

Contents

Introduction

If you are one of the 500m Facebook users or you have a professional profile on LinkedIn or you Tweet, Digg, Stumble or blog then you'll know that social networking is an important communication medium and can be a vital business and personal tool.

If you're not, you don't have to take our word for it. Go look at the traffic stats for your company and see what sites people visit. For example, half the users of Facebook log in on any given day and the average user has 130 friends and creates 90 items of content every month[1].

There's no doubt social networking is becoming almost ubiquitous. Even Google are getting in on the act with Google+. But that doesn't mean that CIOs and IT managers have fallen in love with the idea. Social networking can have business benefits, but it brings with it serious risks too. As more and more people use it, the risks increase and ignoring them becomes impossible.

Social pressure

In fact, 36% of Web Symantec.cloud customers already block access to social networking altogether and another 33% block Instant Messaging and chat. Symantec's 2010 State of Enterprise Security Report[2] reveals a major reason - 84% of CIOs and CISOs consider these sites to be a serious threat to their security.

According to Symantec's 2011 Social Media Protection Flash Poll, these concerns are well-founded. The survey found that social media incidents cost companies an average of more than $4 million over the past 12 months, as a result of stock price, litigation or direct financial costs[3]. These risks are so serious that IT managers cannot afford to ignore social networking or treat it as an HR problem.

Business benefits

Before we investigate these risks and costs, let's consider the benefits of social networking.

- **Marketing and PR -** If Facebook were a country, it would have more inhabitants than the USA. No wonder it's an attractive target for company PR and marketing. But social networking goes beyond traditional 'push' advertising by opening up a two-way channel between customers and companies. It is therefore a great source of ideas, feedback and a viable option for customer service. It can even provide a route to market for some businesses. Gartner estimates that 50% of enterprises will be micro-blogging by 2012[4].
- **Employee motivation and morale -** At the most basic level, for many 'digital natives' now entering the workforce it has replaced email and the telephone as the primary means of communication with friends. Those bright young graduates you want to recruit may not work for your company if you destroy their social lives by banning Facebook. They see access to these services as something close to a basic human right.
- **Recruitment -** Their online relationships can have a business benefit too. For example, a vibrant social network around your company can make it attractive to new recruits and it can help recent hires settle in more quickly. Similarly, it helps HR with recruitment. For many users and companies, LinkedIn is a kind of CV exchange and services such as BranchOut are bringing online recruitment to Facebook too.
- **Networking and support -** Employees use their networks and online connections to get support for their work. It can act like an informal technical support or training system. For example, many IT people turn to online Q&A forums like Quora to solve tricky technical problems. It can also create a strong sense of community and cohesion within a company, providing mutual support and exchange of ideas.
- **Brand enhancement -** Companies like Microsoft encourage their staff to create blogs and interact with customers, informally mixing support, market research, PR and evangelism.

[1] http://www.dailymail.co.uk/news/article-1362413/Facebook-users-UK-surges-HALF-population.html and http://www.guardian.co.uk/technology/2011/jun/13/has-facebook-peaked-drop-uk-users and http://www.facebook.com/press/info.php?statistics

[2] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=sesreport2010

[3] http://www.symantec.com/business/resources/articles/article.jsp?aid=20110204_what_you_need_to_know

[4] Gartner Reveals Five Social Software Predictions for 2010 and Beyond," Gartner Inc., February 2, 2010

The risks and challenges

Online criminals are quick to exploit any popular activity to make money. Social networking is especially attractive because it exploits trust between friends and it is inherently viral by nature. Risks include:

- **Malware -** Social networking is easy and fun, with a variety of apps that enable you to interact with friends and play games. So users are very open to seeing new things on social networking that they need to click on and install in order to participate in some kind of activity. For malware writers, it's a goldmine. Malware distributors are constantly looking for new ways to distribute malware, with their new weapon of choice being malicious apps, which are similar to old-style email worms so that they infect your friends, the Koobface Trojan being a good example.
- **Targeted attacks -** Rarer but more sinister and on the increase. Using social engineering (see below) and custom-written malware, criminals or corporate spies trick people into installing virtually undetectable spyware on their computers. Social networks make it much easier to discover corporate hierarchies, groups of friends and a target's personal and professional interests. All this makes it much easier to craft an irresistible message containing the Trojan and puts companies at serious risk of data theft.
- **Blended attacks -** Social networking teaches users to click on links in emails, making malicious spoof emails even more attractive. For example, in January 2011 65% of email malware contained malicious links (the average in 2010 was just 23.7%)[5].
- **Revealing secrets -** There are plenty of opportunities for indiscretion on social networking sites. One example reveals how thoughtless people can be online, even when their own lives are at stake. In 2010, the Israeli Defence Forces called off a raid after a solder posted the time and destination in advance on Facebook[6].
- **Reputation risk -** Employees, even senior managers, may feel more relaxed about public pronouncements on social networking sites or on their blogs than they would in a press release. Employees don't always think about what they say or do online. In a Deloitte report on the subject, 53 percent of employees thought that their social networking pages were none of their employers' business[7]. Certainly, most companies don't vet people's blog comments before they are published in the way that they check official pronouncements.
- **Hacktivism -** Hacktivists, disgruntled employees and customers can use social networking to create bad publicity for companies. Account hijacking or the use of company pages or sites with similar names (e.g. the the spoof '@BPGlobalPR' Twitter account that activists set up during the 2010 Gulf oil spill[8]) can attract a lot of attention and traffic.
- **Social engineering -** Because people tend to over-share information on social networking sites, criminals and malicious hackers can put together a profile of their victims. They can use this to send targeted spyware attacks. Corporate rivals and other predators can use social networking information to understand the internal workings of your company. For example, you probably wouldn't publish your organisation chart and the contact details of senior management online but a rival could piece this information together from website profiles.
- **Spam -** Just as email spam is costly to filter and time-consuming to deal with manually, social networking spam is increasingly a problem. It can waste people's time and contribute to other problems, such as malware attacks. For example, even though Twitter has improved its internal spam filtering, in 2010, one tweet in a hundred is spam; that's something like 650,000 spam messages a day[9]. If spam rates increase to the levels of email spam (where 90% of all messages are unwanted), then social networking could drown itself and its users.
- **Cyberslacking -** Social networking sites can be addictive and time-consuming (although it is arguable whether employees who fall victim to temptation might find some other way to slack off if these sites were unavailable and that better management rather than censorship is the way to deal with poorly-motivated or unproductive staff).
- **Harassment and cyber-bullying -** Social networking sites are sometimes the forum for workplace bullying and harassment. This creates challenges for HR.

[5] Symantec.cloud Threat Intelligence presentation
[6] http://news.sky.com/skynews/Home/Israeli-Soldier-On-Facebook-Army-Calls-Off-Military-Raid-After-Soldier-Reveals-Details-On-Site/Article/201003115567680
[7] http://www.slideshare.net/opinionwatch/social-networking-and-reputational-risk-in-the-workplace-deloitte-survey-july-09
[8] http://www.telegraph.co.uk/technology/twitter/7782888/Spoof-Twitter-account-that-mocks-BP-over-oil-spill-wins-more-followers-than-real-thing.html

How to deal with social media

Businesses have to take a strong, proactive approach to social media, including monitoring, protecting and deciding how social media information flows through the organisation. This is not a problem that will diminish or go away if you ignore it.

Companies can adopt one of three basic strategies:

Option 1 - outright ban - Where the needs of security outweigh the benefits of social networking and employee's expectation that they would have access to it, you can ban it outright and enforce the ban with technology.

Option 2 - free for all - You can allow unrestricted access to social networking sites but put in place policies, training and technology to prevent malware, minimise the risk of data leaks and encourage responsible use by employees.

Option 3 - user segmentation - You can segment the employee population into different groups, based on their business needs and usage patterns. For example, the marketing department might get full access but other staff might be restricted to lunch times and after work. Or you might give the HR department access to LinkedIn for recruitment but ban it elsewhere. Again, policies, training and technology are required to make this approach work.

Within these three basic approaches, there are a series of sub-options and suggestions that can allow you to harness some of the benefits without accepting all of the risks:

- **Separate network for social networking -** You can set up a 'dirty Wi-Fi network' for employees to use with their smartphones for social access but ban it on the corporate network. If you have users who simply can't live without Facebook, this is a viable option. Similarly, you can set up public-access PCs in a staff room or canteen for employees to use for Facebook.
- **Acceptable Use Policies -** It is essential to review and update your AUP to take account of social networking sites. In particular, an acceptable use policy can help employees understand that they are ambassadors for the company online and explain what is and isn't permissible in terms of speaking for and about the company and what kinds of information they can share publicly. Back this up with technology to notify employees when they try to send confidential data outside of the company.
- **Monitor social networking usage -** Anonymous and aggregated data about the sites employees visit and when they visit them will help you understand the scale of the issue and the impact of any changes. However, the Data Protection Act 1988 says that employees are entitled to a degree of privacy at work. Similarly, the Regulation of Investigatory Powers Act 2000 limits your ability to monitor or record employee communications. Monitoring on an individual basis is therefore more problematic – get proper legal advice before you start.
- **Ensure the mobile and home users are also included -** With more and more people working on laptops, iPads and on home computers, it is important to make sure that any systems you put in place for office-based employees also extends to people who work outside the office so that everyone is treated consistently and that there are no short circuits.
- **Corporate social networking -** Consider corporate alternatives to public social media. For example, you can set up an intranet site with all the attributes of LinkedIn using software like Microsoft SharePoint, Conenza or Socialcast. This kind of technology can harness the benefits for your company while reducing the risks.
- **Educate users -** 'Peopleware', not hardware or software, is often the weakest link. Give new hires a proper briefing as part of their induction and provide recurring training and reminders for existing staff. Update your curriculum to reflect the latest threats from social networking.

[9] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf

Here are ten elements that you could include:

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses.
- Be cautious when clicking on URLs in emails or social media programs, even when appearing to come from trusted sources and friends.
- Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins.
- Be suspicious of search engine results and only click through to trusted sources when conducting searches—especially on topics that are hot in the media.
- Deploy Web browser URL reputation plug-in solutions that display the reputation of websites from searches.
- Deploy Web browser URL reputation plug-in solutions that display the reputation of websites from searches.
- If users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (fake antivirus infections), have users close or quit the browser using Alt-F4, CTRL+W or the task manager.
- Use strong passwords to reduce the risk of account hijacking.
- Reduce vulnerabilities by using up to date browser plugins etc. (e.g. PDF readers, Flash).
- Limit the amount of personal information you make publicly available on the Internet (including and especially social networks) as it may be harvested and used in malicious activities such as targeted attacks, phishing scams.

Symantec.cloud and social media

We also recommend that you use security technology to underpin, support and enforce your social networking policy and to make sure that employees can use it safely. Symantec.cloud delivers comprehensive, cost-effective, industry-leading hosted security. It includes several elements that are directly relevant to the issues in this white paper:

- **Web Security.cloud -** lets you set and apply company-wide policies to control internet use in your organisation. You can block access to sites by name or by category and apply the policies on an individual, group or company-wide basis on a permanent or time-restricted basis. Whether you allow free access or block social networking sites completely, this system will help you make the decision effective. Add Email AntiVirus.cloud and Instant Messaging Security.cloud for all-round protection against blended threats.
- **AntiVirus and AntiSpyware -** Web Security.cloud also scans website requests in real time to block viruses and spyware, even if they infect trusted and legitimate sites. Using multiple scanning engines plus our proprietary Skeptic™ technology, this system adds a unique extra level of protection against malware on social networking sites.
- **Roaming user support -** Because Symantec.cloud solutions are internet-hosted, they can be applied to any internet-connected user whether they are in the office, at home or on a laptop with a mobile broadband connection. This ensures that policies and protection apply to all your users.
- **Endpoint Protection.cloud -** provides comprehensive security for individual PCs/Laptops and fileservers, including antivirus, antispyware, firewall and intrusion prevention with centralised management. This provides PC-level protection against malware on social networking sites.

Symantec.cloud technology can help your business use social networking as a business tool without it becoming a security liability.

For more information, visit www.symanteccloud.com or contact us at CLD_Info@symantec.com (and don't forget to visit our Facebook page and follow us on Twitter '@symanteccloud')!

Office locations

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester GL3 4AB
United Kingdom
Main +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone +44(0)800917 7733

DACH
Wappenhalle,
Konrad-Zuse-Platz 2-5,
81829 München,
Deutschland
Tel +49(0)89 94320 120
Support +44(0)870 8503014

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Main +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Freephone +44(0)800 917 7733

NORDICS
Business Center Nord
Lyngbyvej 20
2100 Copenhagen
Denmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +45 88 71 22 22

FRANCE
17 avenue de l'Arche
Tour Egée
92671 Courbevoie
France
Tel +33 (0) 6 8089 8886
Support +44 (0) 870 850 3014

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-Free +1 866 460 0000

CANADA
170 University Avenue
Toronto ON M5H 3B3
Canada
Toll-Free +1 866 460 0000

ASIA PACIFIC

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: +852 6902 1130

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: +800 120 4415

AUSTRALIA
Level 14
207 Kent Street
Sydney NSW 2000
Australia
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1800 088 099

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku
Tokyo 107-0052
Japan
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: +531 121917

About Symantec.cloud

More than 55,000 organisations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud's MessageLabs services to administer, monitor and protect their information resources more effectively. Organisations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on 15 data centers around the globe. A division within Symantec Corporation, Symantec.cloud offers customers the ability to work more productively in a connected world.

For specific country offices and contact numbers, please visit our website:
www.symanteccloud.com

World Headquarters
MessageLabs
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
+44 (0) 1452 627 627