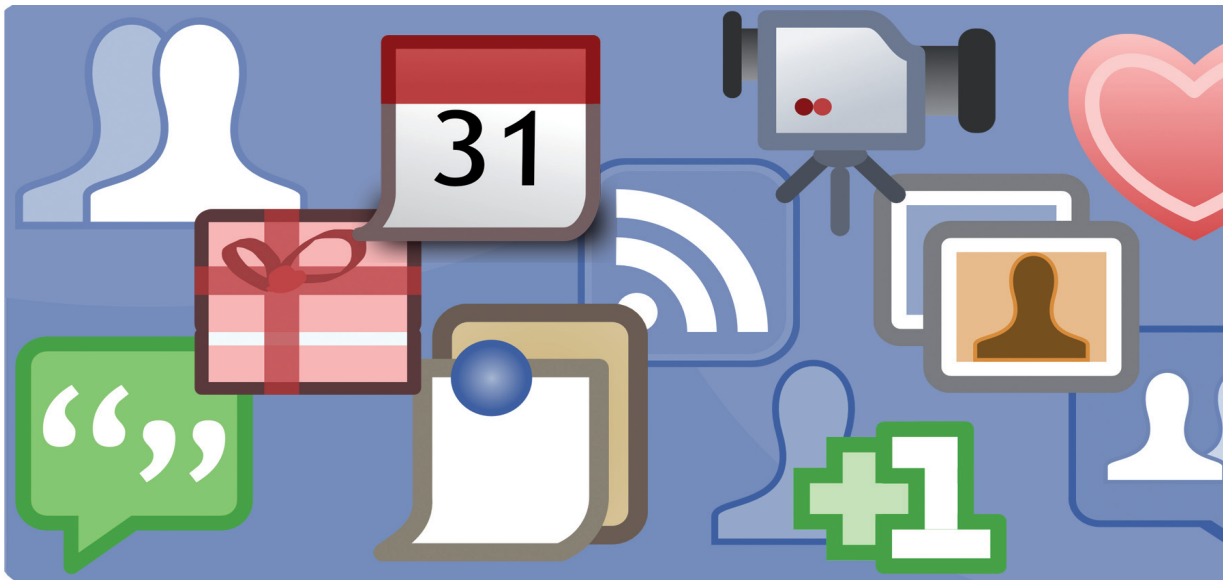

Social Networking in the Business World: A Strategic Approach

ABSTRACT

Is an outright ban on workplace social networking a good idea? Or should companies be more calculated in their points of view and look at how the negative effects social networking has on a company's bottom line can actually turn positive if management adopts a more strategic policy than has been common in the past.

There are certainly good reasons to suppose that unfettered employee access to social network sites can cost your company dearly, and we will discuss some of these reasons in this white paper. But there are also good reasons for thinking that certain types of social networking can benefit many companies a great deal.

Does it have to be all or nothing? We think not, and the purpose of this paper is to explain how employers can manage employee social networking in a way that significantly reduces the negatives and maximises the positives. The strategy combines employee education, well thought out Acceptable Use Policies (AUPs), and—critically—effective, discriminating Web filtering technology.

ALL OR NOTHING?

"Here are some cold numbers," report Professors Matthew Fraser and Soumitra Dutta, authors of highly regarded books and articles on social networking in the workplace:

> *Roughly 65 percent of UK companies deny employee access to social networking sites like Facebook, MySpace and Bebo. In government, figures … revealed that British departments had disciplined hundreds of employees for using Facebook and similar sites at work. In the period from 2005 to 2007, 132 British government bureaucrats had been sacked, 41 had been forced to resign, 868 had received formal warnings, and 686 had been demoted or punished. All for the same crime: logging onto social networking sites at work.* [i]

Is an outright ban on workplace social networking a good idea? It would seem so, given estimates that "have put the negative impact on the UK economy at £132 million a day."[ii] Or should companies be more calculated in their points of view and look at how the negative effects social networking has on a company's bottom line can actually turn positive if management adopts a more strategic policy than has been common in the past. There are certainly good reasons to suppose that unfettered employee access to social network sites can cost your company dearly, and we will discuss some of these reasons in this white paper. But there are also good reasons for thinking that certain types of social networking can benefit many companies a great deal. Does it have to be all or nothing? We think not, and the purpose of this paper is to explain how employers can manage employee social networking in a way that significantly reduces the negatives and maximises the positives. The strategy combines employee education, well thought out Acceptable Use Policies (AUPs), and—critically—effective, discriminating, cutting-edge Web filtering technology of the kind offered by Bloxx.

THE RISKS OF SOCIAL NETWORKING IN THE WORKPLACE

Why in the world would social networking cost an economy so much? Here are some of the most plausible and accepted explanations:

- ***Lost productivity***—The spectre of lost productivity is the most common reason employers cite for blocking access to social networks.[iii] For example, Portsmouth City Council in the UK has now banned staff access to Facebook, Twitter, Bebo and the like after discovering that employees were spending nearly 400 hours a month on Facebook.[iv] That adds up to a lot of wasted salary, and taxpayer groups were naturally outraged. For national security reasons, the U.S. Marine Corp recently made a similar decision with respect to Facebook. Nucleus Research interviewed "randomly selected office workers" and determined that of the 77 percent of workers who had Facebook accounts, 61 percent visited the site at work for an average of 15 minutes per day, which resulted in a 1.47 percent productivity loss across the entire employee population.[v] Although we can't be certain that the study group was truly representative—it only contained 237 workers—common sense suggests that people can easily get distracted by social networking and waste a lot of company time. Indeed, Nucleus reports that one in every 33 workers built their entire Facebook profile at work, and 87 percent basically said that their time on Facebook had no business-related purpose.

[i] Matthew Fraser and Soumitra Dutta, "Is Web 2.0 creating a staff productivity paradox?" MyCustomer.com, 1/6/2009. Fraser and Dutta are co-authors of Throwing Sheep in the Boardroom: How Online Social Networking Will Change Your Life, Work and World.

[ii] Ibid

[iii] Doug Cornelius, "Online Social Networking: Is It a Productivity Bust or Boon for Law Firms?" Law Practice, American Bar Association, March 2009, Vol 35, Number 2, p. 28

[iv] "Facebook banned for council staff," BBC News, http://news.bbc.co.uk, Tuesday, 1 September 2009

[v] Nucleus Research, "Facebook: Measuring the Cost to Business of Social Notworking", http://www.rb.ru, July 2009

- ***Malware, identity theft and data leakage***—Social networking sites can be the delivery vehicle for malware and spyware that cybercriminals covertly embed onto innocent users' pages. These malicious programs can spread throughout an entire internal corporate network and wreak havoc on the company's bottom line. By destroying or disabling systems and data that employees need to do their jobs, malware can have a tremendous impact on productivity which is quite independent of merely "wasting time". Malware and spyware can also bombard internal networks with spam, target users with phishing attacks, and steal user names and passwords. Criminals can use the latter information to appropriate identities and construct fake Facebook profiles that facilitate access to valuable company secrets. Some "ethical hacking" firms will demonstrate, if you pay their fees, how easily and quickly they can obtain almost any company data by using employee names and gaining access through social networking sites.[vi] Moreover, the time it takes for IT departments to defend against ongoing malware and spyware attacks can be extremely expensive.
- ***Compromised confidentiality***—Cybercriminals often don't need sophisticated spyware to obtain secret company information. For whatever reason, naïve social networkers are often more open with personal or confidential information on social networking sites than they are elsewhere in life. Although Facebook users can restrict their pages to a select number of "friends," many social networkers set profiles as public and befriend strangers or imposters who take on the identity of co-workers within their companies, including unknown "colleagues" who claim to be part of the same organization (this is a special vulnerability of large companies, where no one can possibly know everyone else). Collegial discussions can easily lead to the unintended disclosure of private company information. Moreover, social networkers can inadvertently violate government confidentiality regulations. In the aforementioned study, Nucleus Research cites an example of hospital nurses sharing patient information via Facebook with nurses on other shifts. If any of these nurses' other Facebook friends were not hospital employees, the hospital could have easily found itself in violation the Data Protection Act. Similar vulnerabilities exist for lawyers who can violate client confidentiality in much the same way. Beyond that, if legal professionals give innocent advice to Facebook friends, they can unintentionally establish binding lawyer/client relations. Nucleus also noted a growing trend among social networkers to use Facebook as an alternative email platform. Although many organizations monitor ordinary email accounts, if they can't or don't monitor Facebook, users can circumvent corporate email controls and unintentionally or deliberately violate corporate communication policies.
- ***Bandwidth consumption***—Videos, other streaming media and other downloads from social media sites such as YouTube, MySpace and Flicker can consume an enormous amount of bandwidth. When employees are busy downloading videos for example, business-critical applications may run very slowly. If organizations do not restrict access to these sites, they will either have to accept a reduction in productivity or make expensive investments in more bandwidth.

Given these concerns, you might wonder why any manager in his or her right mind would ever permit employees to access social network sites at work. Why not use readily available Web filtering technology to completely block the sites? Yet, managers ought to think twice regarding an absolute ban on social networking. Some moderate and managed uses of social networks can genuinely benefit a company, and discriminating Web filtering tools can help organizations take advantage of these benefits while significantly reducing the risks.

[vi] Ed Sperling, "Social Networks' Security Risk", Forbes.com, http://www.forbes.com/2009/03/13/social-network-security-technology-cio-network-social-network.html, March 3, 2009

THE ARGUMENT FOR WORKPLACE SOCIAL NETWORKING

It is safe to say that most of the top management of today's businesses are not members of the "Y Generation" who are rapidly entering the workplace, and they are obviously not "Millennials," who will follow the Y Generation in short order. Yet this generation is the first to have grown up totally immersed in not only the Internet, but in interactive, often completely mobile technologies such as texting, instant messaging, blogging, media sharing and the now ubiquitous social networking. Indeed, according to the NCC Group IT security firm, UK intelligence agencies are worried that Facebook, et al, are "ruining" the spy industry because they find it virtually impossible to recruit young people who do not have an extensive online trail.[vii]

While many managers are gradually mastering the new forms of communication, the impulse may not come naturally and so they may not fully appreciate how deeply engrained these habits are in the younger workforce. Yet as the younger generation grows older, they will take over global business, become both corporate executives themselves and customers, and they will bring their habits with them.

So a draconian ban on Web 2.0 technology may cut off a primary means of communication that is deeply entrenched in the younger lifestyle. A ban will likely cause frustration and resentment among younger employees, and it might also deprive them of the venues where they can most comfortably and skillfully deal with important business contacts and customers, develop prospects, market their company's products, etc.—in other words, successfully do their jobs. Talented job candidates are beginning to consider such restrictions when deciding on their employment options. The Deacons' Social Networking Survey 2008 reports that 16 percent of respondents said an organization's social Internet policy would influence their decision to join one employer over another, and this percentage is bound to increase as more young people flood the recruiting pool. If executives want to attract the best talent, they should definitely be considered.[viii] They should also remember that by completely blocking staff from their favourite social networking sites, they may prompt tech-savvy employees to devise ways around the ban—e.g. through anonymous proxies—which could potentially damage corporate defences.

Some research suggests that a moderate use of social networking sites actually increases productivity. Dynamic Markets conducted a European-wide survey of 2,000 people, and 65 percent claimed that workplace social networking had made them more productive, and 45 percent said it had sparked creativeness.[ix] An oft-cited reason for this is that discussions on social networks enable workers to brainstorm with both company colleagues and interested friends, and this process prompts innovative approaches to seemingly intractable problems. Social networking allows employees to leverage the collective knowledge of contacts with expertise and similar interests.

Moreover, social networking helps employees stay connected with college and university friends who now have careers in a variety of industries and may turn into valuable partners or customers. These sites also provide access to otherwise inaccessible people and opportunities. Connections count in business, and given there are over 300 million active users on Facebook alone and growing numbers of members of business-oriented sites such as LinkedIn, social networks provide unprecedented opportunity to make and sustain worthwhile connections. Indeed, a Massachusetts Institute of Technology study found the workers with the largest networks were 7 percent more productive than colleagues with fewer Facebook or Twitter friends. Social networks can be a tremendous resource for critical information about customers, employees, job candidates, competitors, the current state of your industry and what others are saying about your organization.

Companies are also discovering that corporate social network accounts, blogs, etc. can be valuable marketing tools, providing more exposure and even increasing Google rankings. Corporate social network sites enable sales and marketing professionals to engage in more intimate and interactive dialog with potential customers, two-way communication that is not possible when companies rely exclusively on ordinary Websites and advertisements. An Australian study indicates that even non-business-related social networking can increase productivity because small breaks allow employees to "reset" their

[vii] Daniel Emery, "Security Risks of Social Networks", BBC News, Tuesday, 7 July 2009 http://news.bbc.co.uk/2/hi/technology/8138777.stm

[viii] Cornelius, March 2009

[iv] "European Study Reveals Social Networking Increases Productivity", Geek with Laptop, http://www.geekwithlaptop.com, Dec.11, 20089

[x] Sarah Perez, "Facebook at Work: Helpful or Hazard", ReadWriteWeb, http://www.readwriteWeb.com, July 14, 2009.

concentration.[x]

If a company can successfully manage the other issues associated with social networks—data leakage, confidentiality, malware, bandwidth—why not allow employees to take the breaks they most enjoy, which often includes Facebook, MySpace, etc? Morale matters in an organization. Beyond that, people who waste time on such sites are likely to find other ways to waste time if the sites are banned. Time wasting in the workplace did not begin with Facebook. Regardless, even if workers do waste time, what does it matter if they are meeting or exceeding their numbers or otherwise performing their jobs well? Performance is ultimately what counts and has the largest affect on a company's revenues.

A MANAGEMENT STRATEGY

An effective corporate policy toward corporate networking will include at least three key components: comprehensive employee education, well-designed Acceptable Use Policies (AUPs), and deploying discriminating Web filtering technology.

- ***Education***—Every employee who sends email, texts, instant messages or accesses any Internet site—not just social networking sites—should be well versed on the dangers of malware, viruses, identity theft, data leakage and compromised corporate confidentiality. A course on these issues should be a required part of new-hire orientation and should also be taken by existing employees. Since social networking is so popular and second nature to many workers, special attention should be paid to corporate vulnerabilities exposed on these sites. When relevant, the instruction should include counselling on confidentiality and data protection laws such as HIPAA, Sarbanes-Oxley, UK Data Protection Act or other relevant local legislation.
- ***Acceptable Use Policies***—Organizations should articulate unambiguous AUPs that state clearly what kind of corporate information can be shared on social networking sites, what is confidential, what can be said about the company, which of these sites workers can visit, and when they can visit (e.g. during lunch or other official break periods). The policies can be designed to make exceptions for certain personnel, such as marketing staff, who may have valid business reasons to access social networking sites more frequently, but this exceptional use should always be justified by businesses purposes. Restricting social networking to specific times and groups automatically addresses the bandwidth issue by reducing the time spent on and number of people accessing the sites. What is just as important as the policies themselves, however, is management's commitment to enforce them. In extreme cases, this can sometimes mean termination of employment, especially if workers have been previously warned, have broken the law on the Internet, or have used devious means to evade AUPs, say through anonymous proxies. If employees are not disciplined for violating AUPs, the employee population will not treat the policies seriously.
- ***Web filtering*** —Finally, organizations should invest in advanced Web filtering systems that will help to implement the rules as effectively as possible, as well as protect internal corporate networks from malware. Bloxx's Web filtering solution is excellent for these purposes. The system can block any existing site either completely or during particular times, and it can make exceptions for specific employee groups or even individuals. Bloxx's Web content filtering solution is powered by its patented Tru-View Technology, an intelligent real-time contextual analysis engine that rapidly categorizes requested Web pages in real-time. Tru-View Technology can go beyond blocking sites already listed in the URL database to identify and block previously unlisted sites. This is important because new social network sites appear quite frequently. Tru-View Technology also has the capacity to detect completely new and unknown anonymous proxy sites and block those in real-time as well. The solution will identify malware or spyware embedded in the pages of Facebook and other sites and minimize the risk of malware entering the internal corporate network. In addition, a company can enforce rules for email and instant messaging by blocking use of those clients using the Bloxx Web filtering appliance.

By combining education, AUPs and Web filtering into an enlightened management strategy, an organisation can reap the benefits of social networking while protecting itself against lost productivity, malware, identity theft, data leakage and compromised confidentiality. Employees will be happier, more productive and effective, and talented young people more willing to join the organisation. It's a win-win for employers and employees alike.

ABOUT BLOXX

Bloxx is a privately held company with offices in the U.S., U.K., The Netherlands, and Australia and offers Web filtering appliance-based solutions for medium and large organizations in both the business and public sectors. In 2007, it was recognized by Deloitte as one of the U.K.'s Top 50 Fastest Growing Technology Companies in its prestigious "Fast 50." For more information please visit: **www.bloxx.com.**

ABOUT BLOXX TRU-VIEW TECHNOLOGY

Bloxx Tru-View Technology uses internationally patent pending technology to analyze and block Web sites quicker and more accurately than other Web filters, which use manual classification and keyword scoring. Tru-View Technology uses intelligent identification and analysis providing instant classification of Web content as soon as it is accessed even if the content has not been seen by anyone before.

Bloxx Tru-View Technology helps organizations proactively manage users' access to Web content which might lower productivity, expose the organization to risk and liability or pose a network security threat.

An estimated 1 million + users already benefit from enhanced security and performance with low administration and no cost per user charges. Additional protection is provided via anti-virus, anti-spyware and anti-phishing functionality, alongside onboard cache.

To learn more about Bloxx Web filtering technology, book in for an online demonstration at bloxx.com/demo, call +44 (0)1506 426 976 or email info@bloxx.com.

Deloitte. Technology Fast500 EMEA 2008

Deloitte. Technology Fast50