CLEAR SWIFT

WebSpy

Web 2.0 in the Workplace Today

Contents

Foreword

Andrew Wyatt
Chief Operating Officer

More than a decade after the term 'Web 2.0' was coined, many businesses are still nowhere near to taking full advantage of the collaborative technologies the term refers to. Undoubtedly, confidence is growing in relation to using tools such as Facebook, Skype, Twitter, and indeed many more organisations are using such technology now compared to even just a couple of years ago. But the fact remains that a worrying amount of businesses seem to be operating a 'lock-down' approach – an approach that I'm sure many Board-level staff know is simply not good for business in the long-term.

Collaborative web and email technologies offer massive benefits for businesses – cost savings, improved communication with customers and suppliers and better employee morale to name but a few. In addition – and this is something I see on a daily basis – an ever more powerful Generation Y presence within businesses means that many employees are now expecting full access at work to the type of web experience they receive at home.

Clearly, it is vital that any web and email technology is managed in the right way to ensure that mistakes cannot be made and that compliance with industry regulation and workforce productivity is maintained.

As a company with a strong heritage in content inspection, Clearswift's IT security solutions have been developed to ensure peace of mind when it comes to these collaborative technologies. At the same time, we recognise that these solutions need to be flexible enough to cope with the complex demands of today's IT environment, ensuring that businesses can move forward with confidence to successfully innovate and gain competitive advantage.

I hope this report provides a useful insight into how, with the right security in place, Boards and managers can take the bold but rewarding step towards taking full advantage of collaborative technologies.

Employers enthusiastically embracing potential of Web 2.0

'Staff being 'happier and more motivated' as a result of using these tools in the workplace'

Employers are increasingly aware of the benefits of social media in the workplace, and the majority are now embracing the use of such tools. More than half (52%) of managers think web collaboration is critical for the future success of the company. Web 2.0 is seen as feeding into numerous aspects of business success, including increasing brand awareness (91%), generating new business (89%) and even improving employee productivity (88%). The most significant evidence of a shift in social networking mindset at a corporate level is the fact that 28% of office workers are now expected to maintain a social media presence for work.

While many companies are quick to highlight the benefits of social media in terms of external client relations, employers also recognise the benefits Web 2.0 tools can have for improving employee relations (Figure 1). 47% of managers believe staff being 'happier and more motivated' as a result of using these tools in the workplace could have a beneficial impact on their business and 37% believe that employees feeling 'more valued and trusted' could have a similar impact.

Employers are increasingly harnessing the positives of Web 2.0, recognising the benefits to corporate image, client relations and staff morale, but they need to be careful not to let enthusiasm blind them to the risks inherent in the presence of Web 2.0 in the workplace.

Figure 1: Staff Happier And More Motivated

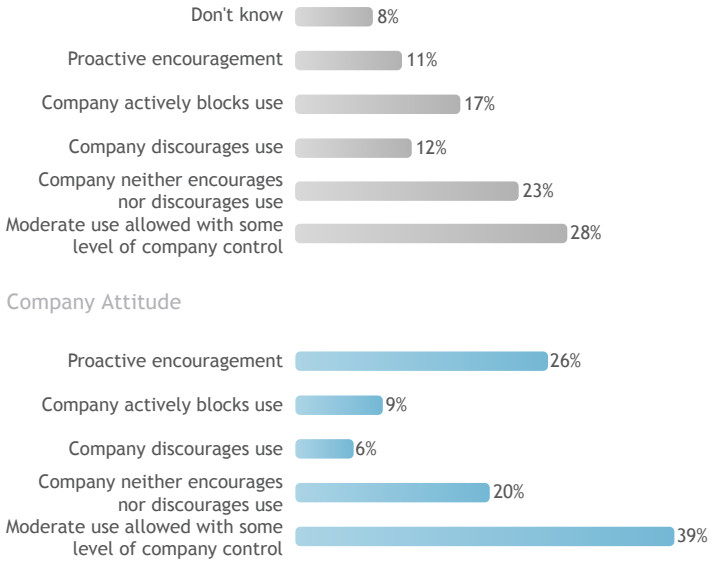
Brave new world

'Liberal approach to web collaboration and social networking'

Two-thirds (65%, Figure 2) of companies claim that the use of Web 2.0 is encouraged or allowed within their organisation, although interestingly only 39% of office workers consider that their companies promote or support the use of Web 2.0 to the same extent. Whilst companies appear to be taking a somewhat liberal approach to web collaboration and social networking, there is an evident disconnect between employer and employee perceptions of moderate or acceptable use and some confusion around what levels of company control are being exercised and communicated.

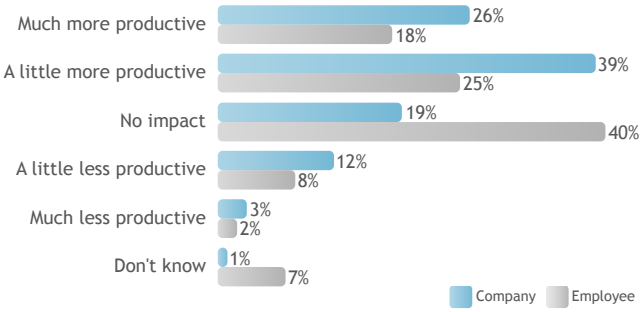
There are signs that employers' eagerness to be seen to be adopting an open or progressive attitude towards social media could, in fact, be obscuring their view of some of the potential risks. 65% of managers believe that use of web collaboration and social media tools at work makes employees more productive (Figure. 3), but only 43% of office workers say the same, suggesting that employer trust may be somewhat misplaced and that social notworking is still an issue in some corners of industry. The productivity pendulum seems to sway in both directions, however, with 66% of office workers saying that they make up the time they spend doing personal email and social networking at work by working later or through lunch. 33% of office workers are happy to use their own private social networks to the advantage of the business suggesting a new give-and-take dimension to employment in 2010.

Figure 2: Employee Perception Of Company Attitude



'44% are happy to discuss work-related issues on social networking sites'

Figure 3: Impact Of Web Based Collaboration And Social Media Tools On Productivity



Although 60% of managers say that they trust employees to use the internet or social networking sites responsibly, there is some evidence that this trust may be a little misguided as a significant proportion of office workers admit to behaviour that might not be quite as welcome within their organisation. 44% say that they are happy to discuss work-related issues on social networking sites, and 25% have sent content via email or social networking sites that they later regretted. Somewhat incongruously, more than half (54%) of office workers would be uncomfortable with people from work seeing their private social networking information suggesting a need for more education amongst in the workplace about the risks associated with social networking sites.

Web 2.0 and security: new approach needed?

'Security breaches are taking place as a result of increased internet usage at work'

While only 39% of employers state that their company has voiced concerns about social media having a negative impact on productivity (Figure 4), they are much more aware of the security threats posed by the presence of vulnerable applications on their network. Security is the biggest Web 2.0 concern, with 61% of companies having voiced concerns about security as a result of social media.

Even though employers may be over-confident in their employees' behaviour on social networks, most are all too aware that their security-savvy is somewhat lacking.

More than half (51%) of managers think employees are oblivious to security concerns when it comes to IT.

Security breaches are taking place as a result of increased internet usage at work, and not all firms are equipped to deal with the new threats presented by the latest technologies. 47% of companies have had at least one security incident as a result of internet application usage (Figure 5) and only 64% have specific tools in place to secure Web 2.0 exchanges. Current popular approaches to Web 2.0 security issues typically involve "big brother" style monitoring and locking down social networking sites. Such approaches may serve to erode employment relationships and diminish business value to be gained from web collaboration. It is a positive sign, therefore, that 64% of companies recognise that a new approach to security is needed in this era of web collaboration.

'...new approach to security is needed in this era of web collaboration'

Figure 4: Impact Of Web Based Collaboration & Social Media Tools On Productivity

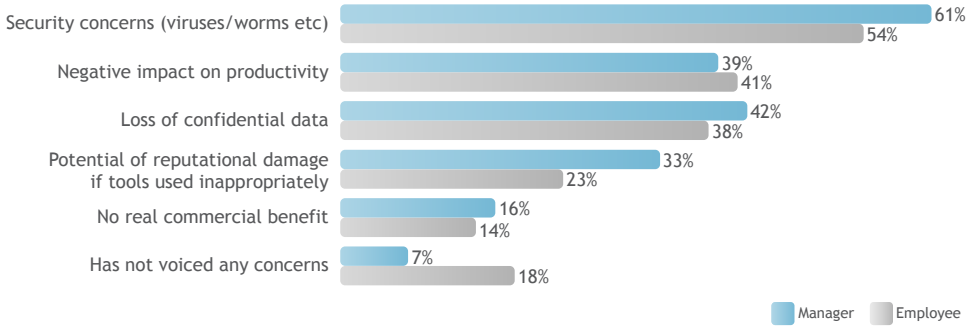
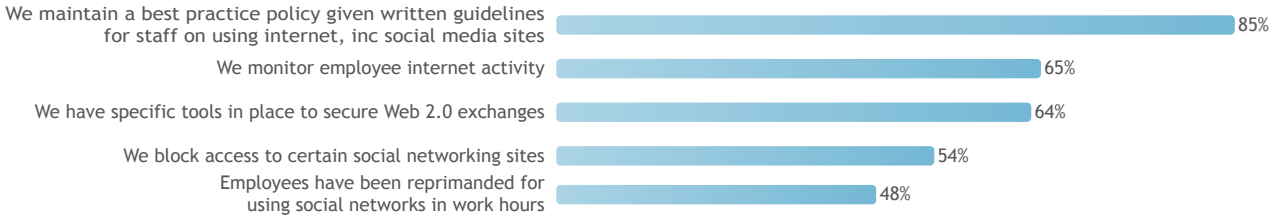


Figure 5: Statements About Information Security Within Organisation



Clearswift SECURE Gateways

Confidence opens doors, paranoia slams them shut

Just as the internet has changed to empower Web 2.0 companies and individuals to become publishers as well as recipients of information, it follows that IT security is evolving.

Today, because information is a two-way flow in and out of the company network, it is logical that a new approach to security is needed to deal with this, and that content needs to be scanned and filtered on the way in as well as the way out.

Unfortunately, for some companies this may be interpreted as the need for draconian 'lock down' measures which could risk them missing out on the myriad of commercial opportunities afforded by developments.

Clearswift SECURE Web Gateway and Clearswift SECURE Email Gateway are trusted by organisations globally to deliver internet security for business. They maintain productivity by enabling information to flow safely into and out of the workplace.

Both SECURE Web and Email Gateways exploit Clearswift SECURE the policy-based content-inspection and filtering platform. Template policies can be tailored at user level to enable the safe exchange of information. For example, collaborative website use can be allowed but file uploads and display of inappropriate content prevented.

This, in turn, engenders the confidence required for companies to fully embrace collaborative web and email technologies and conquer the fears of 'lock down' measures which could risk them missing out on the myriad of commercial opportunities afforded by developments.

WebSpy Reporting

'...rest assured Internet resources & social media is used as intended'

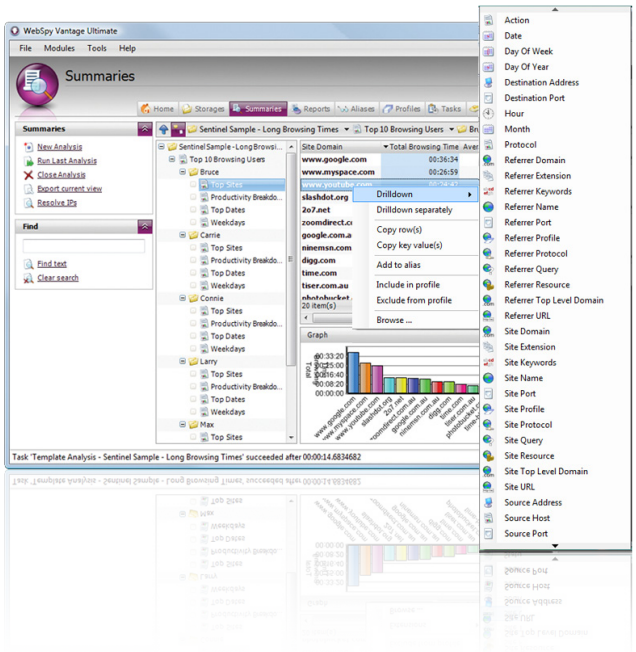
Blocking is clearly not the answer to combat productivity issues and security vulnerabilities in relation to Internet and social media usage.

Using security solutions, such as Clearswift SECURE Web Gateway and Clearswift SECURE Email Gateway, to manage threats and block traffic to illegal or malicious sites, is as imperative as providing unrestricted access to the rest of the web.

Adding WebSpy reporting to the equation enables managers to provide employees with the Internet resources they need, while resting assured the resources are used as intended.

The first step towards ensuring resources are used as intended is establishing and communicating acceptable Internet and social media usage policies. The second step is reporting on usage in order to ensure policy adherence. Unfortunately, taking the employees being reported on into consideration is an important aspect often neglected in the second step. Overly intrusive practices can easily create the negative perception that Big Brother is watching, making employees feel frustrated and uncomfortable.

Effective Internet reporting requires a two-pronged approach; intuitive reporting software AND workforce consideration.



WebSpy

5 Tips for Effective Reporting while taking Workforce into Consideration

1. Allow employees to view their own Internet usage
More often than not, employees tend to underestimate the time they spend browsing non-work related sites. Allowing employees to view, for example, their productive and non-productive activity can help foster and drive responsible Internet usage behaviour.

2. Help employees sticking to the rules
If you have set a limit of, for example, no more than 10 hours of recreational surfing per month, then ensure you alert employees when they are approaching that limit.

3. Distribute reports – distribute responsibility
Frequently IT managers and administrators are given the ultimate responsibility of managing, enforcing and communicating acceptable Internet usage for an entire organisation. Take some of the pressure off the IT department and distribute organisational Internet activity reports to responsible managers or department heads. This will enable them to see how Internet usage affects the security and performance of their own department and distributes the responsibility of enforcing acceptable usage with the managers themselves.

4. Protect employee privacy
If distributing Internet usage reports across your organisation it is important to protect employees' personal data. Make sure you use reporting software designed to protect privacy rights by only allowing authorised users to see the employee's identity. For instance, Network Administrators may need to investigate all traffic going to a particular site but should not need to know the user names – in this case user names should be anonymous for them but available for HR.

5. Automation
Use a reporting solution that easily lets you customise and automate these guidelines for you.

Conclusion

'...risks posed by threats to security, productivity and employee relationships'

While companies are aware of the threats to security posed by the use of Web 2.0 tools in the workplace, not enough of them currently have facilities in place to combat them. Simultaneously, employees appear to be blissfully ignorant.

It is undoubtedly to the credit of the employers surveyed that their approach to the use of Web 2.0 tools in the workplace is now largely open and enthusiastic. However, this enthusiasm must be tempered with a measured approach that takes into consideration the risks posed by threats to security, productivity and employee relationships. As web collaboration further matures, the companies that fully appreciate and manage the good, the bad and the ugly of Web 2.0 will be in the strongest position to optimise the value such tools can bring.

Methodology

Approximately 250 online interviews with office workers and 150 with managers were conducted in the UK, US, Australia and Germany during January 2010. The survey was conducted by Loudhouse Research, an independent market research consultancy based in the UK, on behalf of Clearswift.