

# **Curb your enthusiasm: Corporate risk assessment of Web 2.0**



## Curb your enthusiasm: Corporate risk assessment of Web 2.0

The risks and benefits of corporate use of Web 2.0 tools (known as Enterprise 2.0) are rather balanced in the report **Beyond Enthusiasm: making the business case for your organisation's use of Web 2.0**. This article intentionally takes a more negative view, concentrating on some specific risks of Web 2.0, how it affects the behaviour of employees, suppliers and data holders; and how it provides new opportunities for cybercrime. Even if your organisation does not itself make use of Web 2.0 technologies, it may be affected by users among its employees, customers, suppliers, and competitors

### Data loss: the trends

Recent research in the UK has measured the frequency and average cost of information security incidents. It's sobering to realise that very large companies are almost guaranteed to have such an incident every year, at an average cost for the worst incidents of over £1million.

	Small (<50 staff)	Large (>250 staff)	Very Large (>500 staff)
Companies that had a security incident in the last year	45%	72%	96%
Average number of incidents, median (mean)	6 (100)	15 (200)	>400 (>1,300)
Average cost of worst incident in year	£10k to £20k	£90k to £170k	£1m to £2m

Source: Ninth Information Security Breaches Survey, (2008) BERR<sup>1</sup>

<sup>1</sup> UK Government department of Business, Enterprise and Regulatory Reform now BIS (Department for Business Innovation and Skills)

A global view is provided by KPMG's regular **Data Loss Barometer**, which suggests a lower volume of incidents in 2009 than 2008 (down by an estimated third). However, within this trend is a significant increase in malicious insider leaks.

## What are Web 2.0 risks?

Social networking sites offer the potential for hackers and fraudsters to gain personal details about an organisation's employees, which could be used to guess employee's passwords to corporate IT systems. Despite the well-recognised risks, it is still common (unless the organisation's IT department has robust and well observed protocols) for employees to use passwords such as partner or child's name; pet's name or sports team. This problem is exacerbated because many people are poor at managing multiple passwords, and use the same one for many sites.

There is a more indirect risk, which is that personal information might be used to hack into, and gain control of personal email accounts, which are often poorly protected. This has an implication for work-related emails, because there is often traffic between the two accounts, enabling hackers to identify valid work email addresses and use these for 'spear-phishing'.

Spear phishing is a refinement of the speculative mass spamming of emails purporting to come from another source (referred to as phishing), spear-phishing being more targeted. Tailored emails are created which appear to come from a named individual (or team in IT or HR etc.) in a position of authority such that the recipient will comply with their requests to supply information or download files. Cyber criminals often construct their own virtual 'corporate directories' and may target new (and thus more vulnerable) members of staff.

There is also the reputational risk of employees, contractors, suppliers, distributors etc. discussing their work on social networking sites. Many organisations take action where they feel an employee had brought their company into disrepute. **Recent research** suggests that 8% of large US companies surveyed have terminated an employee for violating social networking policies in the past 12 months

With respect to malicious damage to corporate data, the risk is that downloads from social networking sites or blogs often contain viruses. Users tend to be

less suspicious of downloads or messages sent by contacts (because those contacts are 'friends', aren't they?); or instructions purporting to come from such familiar sites.

A recent data security report from Sophos (the IT security company) advised that the primary source of malicious code (responsible for 2% of it worldwide) was Google's blogging tool Blogger. This is because it's easy to set up new pages without requiring identification – as indeed it is for Facebook and most of the social networking sites. Because there is no joining or membership fee, there is not even the requirement to provide credit card details, which would be some kind of identity check. If employees access blogs or social networking sites on the company's server, they can provide a gateway into the organisation.

Specific risks include:

- Downloads sent by contacts often (intentionally or unknowingly) contain viruses. For example, Facebook has thousands of downloadable applications contributed by users – to send each other virtual beers, or cupcakes; to rate each other's attractiveness or turning each other into 'Zombies' – some of which contain viruses.
- Contacts identities can be misappropriated to send malware.
- The site itself can be counterfeited- users log on to what they think is the genuine site, and are advised to download 'the most recent version' of the software used to e.g. upload or view videos. Instead they download malware.

Another significant information issue is how to protect information no longer within the organisation's own firewalls, but shared with third parties.

Another risk is that information might be disclosed which is commercially sensitive or price sensitive; which gives away intellectual property or which damages the organisation's reputation. Information disclosed on line is searchable; easily shared or linked to; persistent and impossible to eradicate. The BERR Information Security survey previously mentioned gave the following example in relation to the risks posed by the use of social networking

**'The IT staff at an insurance company used an Internet chat room to help them solve technical issues. However, this resulted in them inadvertently disclosing the company's security set-up and configuration in a public forum.'**

The disclosure of sensitive financial information is a specific concern; and an evolving issue. Boards are increasingly regarding company blogs as an acceptable and convenient channel for formal shareholder information. In the

USA last year, the SEC provided guidance on company website postings as a form of public disclosure. The position of the UK regulator, the Financial Services Authority (FSA) is **'price sensitive information which could significantly affect a company's share price must be announced to the market as a whole without delay.'** The FSA has not updated its guidance from 1996 to take into account social media, so the position remains that **'Information must always be given to the market as a whole, by an announcement to the Company Announcements Office. Companies are free to use additional media, but selective disclosure of price sensitive information, without an announcement, is never acceptable.'** The problem is where the disclosures are less formal, an unintentional release of price-sensitive information.

Finally, there are other regulatory risks relating to advertising law. The regulator in the UK, the Advertising Standards Authority (ASA) seems not to have issued specific guidance about the use of social media so I have made reference to the position in the USA as a guide. Readers should consult specialist advisers for detailed information.

Suppose an organisation sends out free samples of its product, to its target market (say, young mothers; or keen cyclists) asking only that they blog about their experiences using said product. In the USA, this practice would contravene fair trade practices – the organisation would have to ensure that bloggers disclosed they had received the product as a free sample, in any review they wrote about it.

The organisation might feel it's easier to write its own reviews, posing as a customer. That could constitute false advertising. And what about seeding reviews of its product on retailing or price comparison sites? In the USA, the Federal Trade Commission has advised that it is illegal for employees to endorse their company's products on such sites, without disclosing that they work for that company. The risks are not just that an organisation's marketing staff might try such initiatives but enthusiastic staff elsewhere in the organisation who are less familiar with the relevant requirements might mistakenly take the initiative.

There is not just the reaction from regulators, but the reaction from the internet's own 'police' – thousands of social media enthusiasts – who will react against any inauthentic posts or disguised selling and will mete out their own form of justice – flaming, naming and shaming.

## Web 2.0 risks not on organisation's radar

A recent EIU/KPMG survey suggests only a minority (28%) of organisations have included Web 2.0 risks in their risk management process.

Yet it's important to keep a sense of proportion. In many cases Web 2.0 is not creating an entirely new risk, but a new twist, or a refinement to exploit an existing vulnerability. It may be helpful to remind ourselves that the underlying issues are mostly about human behaviour. **'People remain the weakest link'** was one of the key findings of the recent global information security survey conducted by Ernst & Young<sup>2</sup>. This survey advised that half of respondents felt organisational awareness of such risks was the biggest challenge - more so even than limited financial or other resources to prepare defences against information security threats.

Ernst & Young comments **'Hackers have long known the easiest way to circumvent an information security system is to exploit the people. Simple techniques – such as impersonating IT or company personnel – can be used to gain access to information from unsuspecting employees. A large percentage of respondents (85%) confirm they regularly perform internet testing, but only 19% of respondents conduct social engineering attempts to test their employees.'**

## The corporate fight back

Detailed technical solutions to these risks are not within the CEO's purview – CEO's have IT departments for this. But it is the responsibility of the CEO to be aware of significant risks, and to create the culture and tone to address the human issues. Since Web 2.0's impact on organisations is still relatively new, organisations will simultaneously experience some enthusiasts trying new practices and triggering unforeseen risks alongside colleagues who are to various degrees ignorant or suspicious of Web 2.0 applications or otherwise reluctant to engage. Both groups will benefit from training, and guidance from management about what the organisation expects. Specific defences against Web 2.0 risks include:

**Good password protocols.** Passwords should contain some non-alphabetic characters and be changed frequently; and preferably not be any word

<sup>2</sup> Moving Beyond Compliance, Ernst & Young's 2008 Global Information Security survey downloadable from [www.ey.com](http://www.ey.com)

contained in a dictionary, since common password-cracking tools are based on dictionaries.

**Regular training/reminders about password protection.** Employees should be reminded to be suspicious about anyone asking for passwords – whether this purports to be from their own IT team or HR department; and whether this is by phone or electronically. Most attacks can be deflected if suspicious users enter the full (legitimate) URL of established corporate pages in browsers, rather than clicking on links provided by the phisher. Provide a VPN (Virtual Private Network) to enable employees to work flexibly wherever they have access to the Internet to minimise traffic between work and personal email accounts.

Include **requirements for information security** in their contracts with third parties such as partners, or contractors who have access to this. Organisations should also conduct periodic assessments of those parties' ability to protect this information.

**Properly vet employees.** This can be difficult when functions are off-shored or otherwise multinational, and the staff responsible for vetting are not familiar with identification documents or how to undertake criminal records checks. The Centre for the Protection of National Infrastructure (CPNI) in the UK provides **practical advice** on the latter, for forty-eight different countries.

**Advise employees about the risks** to the organisations of work-related details posted on social networking sites, and ask them not to post details about their jobs. Consider whether to carry out social engineering<sup>3</sup> testing. Note employers cannot *prevent* their staff disclosing where they work, and in fact many social networking sites are built on the premise that users disclose this sort of information to help make connections. If organisations wish to allow/encourage employees to use networking sites for business purposes, they should advise staff to use business-oriented sites (such as LinkedIn) which do not include personal information on family or hobbies.

**Have a policy for on-line conduct**, in which employees should be reminded that bringing the organisation into disrepute; or disclosing commercially sensitive information is a disciplinary offence whether it takes place on-line or not. Organisations should advise employees that online disclosures differ from other discussions, in that they are searchable; easily shared or linked to; persistent and impossible to eradicate. Thus online disclosures have more serious consequences than for example venting about a bad day to one's

---

<sup>3</sup> Social engineering is manipulating people into carry out certain actions, or disclosing certain information. Social engineering testing is therefore creating scenarios to test how staff would react to a social engineering attack such as a fraudulent request for one's password.

friends in the pub.

Organisations should also **use software to monitor blogs or social networking sites** for mention of their name, brands, key products or personnel. Organisations should consider replying if appropriate, to repair or sustain its brand image. The harshest or most organised criticism may be found on 'I hate (name of company)' or '(name of product) sucks' groups or discussion threads. It represents a needle in a very large haystack if no-one is looking for it ('security through obscurity'); but might become an issue when a partner, supplier or acquirer is undertaking research or due diligence.

## Conclusion

It is important to keep a keep a sense of proportion. Negative comments by customers or suppliers, or even a campaign organised using social media tools, can come as a shock to the organisation coming across this unawares. Any organisation affected by this should remember it had as many unhappy customers previously, but they were diluted, even invisible. The old saying used to be that every happy customer tells one friend, every unhappy customer ten. Well, social media tools have recalibrated those proportions. An unhappy customer will reach thousands, possibly millions if (s)he is an articulate and amusing blogger or if readers are actively searching for mentions of a brand or a company.

Copyright ©CIMA 2009

First published in 2009 by:

The Chartered Institute of  
Management Accountants  
26 Chapter Street  
London  
SW1P 4NP  
United Kingdom

Printed in Great Britain

No responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication can be accepted by the authors or the publishers.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means method or device, electronic (whether now or hereafter known or developed), mechanical, photocopying, recorded or otherwise, without the prior permission of the publishers.

Permission requests should be submitted to CIMA at  
[cima.contact@cimaglobal.com](mailto:cima.contact@cimaglobal.com)