

The term Web 2.0 was coined in 2004 by Tim O'Reilly, the computer book publisher, for a seminal conference which was intended to re-inflate the internet industry after the burst of the dotcom bubble in 2001. The term suggests an updated technical specification, such as the release of a new generation of software, but actually refers to the concept of the second-

generation internet and how users interface with it. Some, including internet pioneer Tim Berners-Lee, argue that the worldwide web was always intended to be about people communicating and sharing.

Rather than offering a concrete definition, O'Reilly describes Web 2.0 in terms of relationships and even a 'meme map',

more on which can be found in his essay referenced at the end of this article. But he does say that the most important principle is that 'Web 2.0 is about systems that harness collective intelligence'. Web 2.0 concerns various technologies that enable collaboration, such as web-based communities, wikis, blogs and other social networking applications.

# Look to the future

**Louise Ross** plugs into the online business community to take a close look at the risks and opportunities presented by the social networking revolution enabled by Web 2.0 technology.



**Risky business**

Even if an organisation does not make use of Web 2.0 technologies, it will be affected by users among its employees, customers, suppliers and competitors. Although a recent survey suggested that only 28% of organisations have included Web 2.0 in their risk management process, awareness of the risks of these technologies should register on every organisation’s radar. It is important to keep a sense of proportion. In many cases Web 2.0 is not creating an entirely new risk, but a new twist that exploits an existing vulnerability. It may be helpful to remind ourselves that the underlying issues are mostly related to human behaviour. ‘People remain the weakest link’ was one of the key findings of the recent global information security survey conducted by Ernst & Young (E&Y).

The survey found that half of respondents felt organisational awareness of such risks was the biggest challenge for business – more so even than limited financial or other resources to prepare defences against information security threats. ‘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%) confirmed they regularly perform internet testing, but only 19% of respondents conduct social engineering attempts to test their employees,’ the survey said.

Many organisations also ignore another significant information issue, which is how to protect data no longer within firewalls but shared with third parties. It’s sobering to realise that large companies are almost guaranteed to have such an incident every year, at an average cost of over £1 million.

**Issue: misuse of personal information.** Users reveal a lot of personal information on social networking sites, which is often inadequately protected and therefore vulnerable to misuse by cyber criminals. Some specific risks are listed below.

- Personal information might be used to guess employee’s passwords for corporate IT systems. A 2004 survey showed that the most commonly used passwords in offices in the UK were a partner or child’s name (15%), football team (11%) and pet’s name (8%). Many people are poor at managing multiple passwords, and use the same one for many sites.

- Personal information might be used to hack into and gain control of poorly protected personal email accounts. Recent high profile victims include Sarah Palin and Paris Hilton. This practice is known as a Tinkerbella hack, in honour of the latter’s Chihuahua, whose name was her password. If there is traffic between personal and work email accounts, hackers can identify valid work email addresses and use these for spear-phishing. This is a refinement of the speculative mass spamming of emails purporting to come from another source, known as phishing. Spear-phishing is more targeted; tailored emails are created that appear to come from a named individual or team, possibly IT or HR, in a position of authority such that the recipient will comply with requests to supply information or download files. Cyber criminals construct their own virtual corporate directories and can target new and more vulnerable members of staff.

**Issue: people discuss their work on social networking sites**

According to a recent YouGov survey quoted on the Personnel Today website, 42% of users in the UK discuss work online. Organisations cannot and should not dictate whether or

how people can use social networking sites in their private life, so inevitably there are risks:

- Users might post misinformed, malicious or otherwise damaging content about their employer (or its customers or suppliers). Many organisations take action where they feel an employee has brought their company into disrepute. Research quoted on the Management Issues website indicated that over one in five companies had disciplined an employee for violating blog or message board policies in 2005, with 7% of US companies and 4% of UK companies dismissing the individual concerned. One of the most famous European examples is that of the UK accountancy firm Dixon Wilson, employers of the Paris-based secretary who blogged as ‘La Petite Anglaise’. Despite her care not to identify herself or her employers by name or nature of business, Dixon Wilson argued that she had made herself, and therefore the firm, identifiable by including her own photograph on her blog. The firm dismissed her for gross misconduct, but she subsequently won her unfair dismissal case.
- Information might be disclosed that is commercially sensitive or price sensitive,

**‘Hackers have long known the easiest way to circumvent an information security system is to exploit the people.’ Ernst & Young**

Popular social networking applications		
Web 2.0 tool	Description	Examples
Social networking sites	Websites that allow users to meet people with similar interests and link up with contacts, friends and family	Facebook, MySpace, Bebo
Blogs	Short for web log, blogs are online journals containing whatever the user wishes – images, thoughts, news, links etc.	Beehive (Steve Bee, cartoonist and head of pensions strategy at the Royal London Group), Freakonomics authors continuing where their book left off, and millions of others.
Wikis	Web pages, the content of which can be added, removed or modified by a group	Wikipedia, Wikileaks, WikiTravel
Virtual worlds	Simulated environments that offer an alternate existence or “avatar” in hyperspace, with virtual landscapes, buildings, vehicles and more, creating another world.	Second Life, Nicktropolis, The Sims Online

Information security breaches			
	Small (<50 staff)	Large (<250 staff)	Large (<500 staff)
Companies that had a security incident in the last year	<b>45%</b>	<b>45%</b>	<b>96%</b>
Average number of incidents, median (mean)	<b>6</b> (100)	<b>15</b> (200)	<b>&gt;400</b> (>1,300)
Average cost of worst incident in year	<b>£10,000 to £20,000</b>	<b>£90,000 to £170,000</b>	<b>£1 million to £2 million</b>

Source: "Ninth information security breaches survey, (2008)", BERR.

which gives away intellectual property or damages the organisation's reputation. Information disclosed online is searchable, easily shared, persistent and impossible to eradicate. BERR's "Ninth information security breaches survey, (2008)" used the following example when discussing 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 setup and configuration in a public forum.'

#### Issue: downloads from social networking sites or blogs can contain viruses

Users tend to be less suspicious of downloads, messages or instructions purporting to come from friends, colleagues or familiar websites. A recent report from IT security company Sophos 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 on Facebook and other social networking sites. If employees are accessing 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. Facebook, for instance, has thousands of downloadable applications contributed by users – for example to send each other virtual beers or cupcakes, to rate each other's attractiveness or turn each other into virtual zombies. Some of these applications can contain harmful code.

- Contacts' identities can be misappropriated to send malware (software designed to infiltrate or damage a computer system without the owner's informed consent).
- A site can be counterfeited – users log-on to what they think is the genuine site and are advised to download supposedly the most recent version of the software used, for example to upload or view videos. What they actually download is malware.

Technical solutions to these risks are not necessarily within a business leader's purview – they have an IT department for that. But it is their responsibility to be alert to the possibility that there are major gaps in a firm's defences and to create a culture that addresses the human issues. Specific defences include:

- **Good password protocols.** Hopefully your IT department has specified that passwords should contain some non-alphabetic characters and be changed frequently etc. It will help to create the necessary co-operative and responsible culture if it also explains why certain practices are risky. For example, the reason that employees should not use any word contained in a dictionary as a password is that common password-cracking tools are based on dictionaries.
- **Reinforced training about password protection.** Remind employees to be suspicious of anyone asking for passwords – whether your own IT team or HR department, 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.

- **Requirements for information security in contracts with third parties.**

- **Setting up a virtual private network (VPN).** There should be little need for employees to forward mail between their personal and work email accounts, if you provide a VPN to enable employees to work flexibly wherever they have access to the Internet.

- **A policy for online conduct.** Remind employees that bringing the organisation into disrepute or disclosing commercially sensitive information is a disciplinary offence, whether it takes place online or not. Advise them that information disclosed online is searchable, easily shared or linked to, persistent and impossible to eradicate. Therefore, it has more serious consequences than venting about a bad day to friends in the pub. In this area, you might find the TUC's work useful (please see the resources at the end of this article). Advise employees about the risks to the organisation of work-related details posted on social networking sites. Ask them not to post details about their jobs. Consider whether to carry out social engineering testing (please see Wall Street Journal article in resources).

- **Business-oriented sites for work-related networking.** If you allow/encourage employees to use networking sites for business purposes, advise them to use business-oriented sites, such as LinkedIn, which do not include personal information on family or hobbies.

#### Web 2.0 opportunities

Enthusiasts argue that one of the biggest risks posed by Web 2.0 is to not exploit its opportunities. 'Web 2.0 is a game changer – it holds the potential to turbo-charge back office functions, foster collaboration and transform every business unit in the enterprise,' says O'Reilly.

Hard data to measure benefits is hard to come by, partly because it is quite early in the lifespan of these technologies, but also because it is hard to measure those. In lieu of hard data, I can contribute cases that I have come across, which illustrate the potential benefits.

#### Issue: harnessing expertise outside the organisation

Innovative organisations have recognised that they can tap into talent and ideas outside their own product development teams. There

is a parallel between this sort of web-based collaboration, and the open source software development model. The principle upon which the latter is based is that allowing free access to source code for anyone to use or modify as they see fit accelerates the development of new applications. Instead of the traditional proprietary model in which developers seek to ensure that users cannot use, modify or share the product unless specifically allowed to.

Open source development is the most effective approach in many circumstances, for example, where there is a need to quickly build a critical mass of users (or suppliers); or where it is necessary because of short product life cycles, to get products to market quickly; or to avoid a costly battle of rival technologies. And these reasons also apply to the kinds of Web 2.0 collaborations I discuss below. Note the new role of the originator in these cases – no longer the sole developer,

but providing the protocols, objectives, framework and channels for users or others to provide content or solutions.

#### Case: Goldcorp

Goldcorp was a mining company in terminal danger if it didn't find new gold deposits. Its chief executive took the radical step of publishing the company's geological data, previously considered proprietary and strictly confidential information, on the web and threw out an open challenge to suggest which areas should be prospected at its Red Lake mine in Ontario. Goldcorp offered nearly \$600 000 in prize money for the best ideas (methods and sites) and was staggered by the quality of the applications. It had tapped a wealth of expertise it didn't even know existed. Of the targets identified by these new collaborators, more than 80% yielded substantial quantities of gold, totaling \$3 billion. The success of this project kick-started a wave of innovation in drilling techniques,

data collection procedures and geological modeling that transformed the company.

#### Issue: collaboration and team working

Web 2.0 tools enable better collaboration, but some organisations are specifically considering how to use them to improve team working or to harness communities of volunteers. IBM is one of the most enthusiastic proponents of Web 2.0 technology, which represents a significant business opportunity for the company as well as some methodologies for managing its own community of developers, suppliers and users. For example, IBM is currently developing technology to enable users to create virtual meeting places, with the facility to make them secure so you can discuss legal, patent or other commercially sensitive issues. IBM believes that this technology brings participants together in a more natural and effective way than teleconferencing or emailing.

**'Web 2.0 is a game changer – it holds the potential to turbo-charge back office functions, foster collaboration and transform every business unit in the enterprise.'**

## MSc in Managing Organisational Performance



Develop your performance management skills and be recognised for the value you can add to your organisation.

The MSc, brought to you by the Cranfield University School of Management with CIMA, will give you the knowledge, skills, confidence and experience needed for performance management roles.

- Develop strategic understanding of organisational performance including the strategies, processes and challenges involved in managing organisations.
- Reflect on performance and use skills to plan, manage, measure and review it.
- Acquire the confidence to use your skills in an organisational context to drive measurable results.

CIMA members receive exemptions from entry requirements and discounts from fees.

For more information visit: [www.cimaglobal.com/cranfieldmsc](http://www.cimaglobal.com/cranfieldmsc)



**Case: IBM**

IBM is also the most enthusiastic corporate presence on Second Life. Irvine Wladawsky-Berger, vice-president of technical strategy and innovation at IBM, believes that 'highly visual and collaborative interfaces will become very important in the way we interact with all IT applications in the future'. IBM uses Second Life as an important tool for testing new ideas and models. It has twelve islands, some public and some private, where its engineers, consultants and designers can brainstorm and collaborate on projects such as the 3D internet.

**Case: The RSA**

The 250 year old Royal Society for the Encouragement of Arts, Manufactures and Commerce is considering using a social networking tool such as Facebook to communicate with its fellows. In common with many membership organisations, the thousands of fellows

are geographically dispersed and run local groups, stage events and undertake various projects. There is evidence of a bottom-up call from the fellows to use this technology to reinvent, or at least reinvigorate the society.

**Conclusions**

The key word running throughout this article, and one to keep in mind when Web 2.0 is ever mentioned, is collaboration. Web 2.0 technologies bring people together to comment, innovate, suggest or complain. There is a sense that these are levelling technologies, enabling individuals to have a platform for their opinion or ideas nearly equal to an organisation's.

As well as equality, collaboration implies trust. There is a need to trust that partners in an industry consortium will protect data with as much care as its owners do and not exploit what they learn for competition. It is also important to recognise that customers

might have insights about how a product might be used that may not have occurred to a company itself. Trusting that employees will act responsibly when discussing their work lives on social networking sites is also crucial. Work and personal life will always intermingle – we are not machines. But we all – not just the "IT guys" – should be alert to the new risks that Web 2.0 poses.

Web 2.0 is not just a concept for companies to worry about though; it is also a powerful tool to be made use of. The implementation of Web 2.0 applications has energised the user – accelerating innovation, creating new market for product development, turbo-charging the efficiency of a supply chain and motivating dispersed teams. ■

**'Web 2.0 is not just a concept for companies to worry about; it is also a powerful tool to be made use of.'**

**Web 2.0 resources**

- Tim O'Reilly's article 'What Is Web 2.0' can be found on his website, <http://oreilly.com/>
- EIU/KPMG's survey is downloadable at [www.us.kpmg.com/news/index.asp?cid=2587](http://www.us.kpmg.com/news/index.asp?cid=2587)
- The "Information Security Breaches Survey" is available at [www.security-survey.gov.uk](http://www.security-survey.gov.uk)
- The Wall Street Journal's article "Spear Phishing Tests Educate People About Online Scams", Technology Section, can be found at <http://online.wsj.com/public/us>
- The TUC briefing for employers on use of social networking at work is available at [www.tuc.org.uk/extras/facinguptofacebook.pdf](http://www.tuc.org.uk/extras/facinguptofacebook.pdf)
- The Financial Times' article 'Fraudsters target social networkers' can be found on the newspaper's website, [www.ft.com](http://www.ft.com)

**Louise Ross**

Louise Ross is a technical specialist at CIMA. Her special interests are narrative reporting, the changing role of the management accountant and the impact of collaborative web-based technologies. Formerly, she was CIMA's Director of Research and retains her interest in bringing academic research findings to practitioners.

