

Social Democracy With a Guiding Hand

By Clive Longbottom, Service Director, Quocirca Ltd

Social networking, in whatever form it finally decides to adopt, is here to stay. Whether you believe in the blog as a means for an individual to publish their undiluted thoughts on a subject or see the blog morphing to becoming something that is more formally reviewed and published, the idea has stuck with us. The idea of a Wiki has also stuck with us – not as another attempt to top Wikipedia, but as a means of bringing together thoughts from a disparate group of people in a meaningful way. Instant messaging has been around for a while now and is the preferred means of communication for many younger workers in companies. VoIP has taken up a noticeable degree of many organisations' data bandwidth, both at the LAN and WAN levels. Then, we have the external networking sites – the likes of LinkedIn and Plaxo, being replaced in the individual's favorites by FaceBook and MySpace, which in turn address new entrants on a daily basis.

The stated aim from many vendors in communication and collaboration market, along with the perception from the users has been that technology will make everything far simpler – at least eventually. The problem for the moment seems to be technology is just making things worse. New technologies don't replace old ones; they just increase the number of possible tools, while increasing the volume and type of information that needs capturing and storing.

For an organisation, the issue rapidly becomes how to control the situation. There are two main constituents to this. One is what tools are to be allowed, and the second is around what can be done with the resulting output from such tools?

At the control level, should an organisation decide to go it alone, an expensive, overly complex and manual approach will be required. For example, proscription – setting up a company policy that says that no instant messaging (IM) shall be used, that external social networking sites are banned from any level of access and so on - is very easy to do, but almost impossible to police. The majority of today's social networking systems use a very simple approach to information transport. They use TCP/IP, generally over Port 80. Cutting off access to Port 80 means no one can access the Internet at all – not a very good overall solution. Sites can be blacklisted, but keeping the list up to date is pretty hard if you are going to try to manage it in house.

What happens when access to these nominally defined rogue sites is needed? For example, let's say that you are a pharmaceutical company. You obviously don't want your top scientists sharing all the chemical research on the latest drug on these sites, so you blacklist them. But then, a competitor, or a concerned consumer group puts up some information on such sites that could change the direction for the company and its competitors.

You're at a disadvantage, as access to the site can only be carried out by individuals from their private machine. Your competitor's scientists are already working away at it. Sure, group policies can be set up. But, they need to be maintained and changed rapidly as the need dictates, leaving holes where the unhappy employee can walk through.

Or another example, you're a financial services company, and a customer has just complained that they have been sold the wrong product. You look at your audit trail and everything was done correctly as far as you can tell. The customer then says that they had an IM session with the sales person during which everything was agreed. You may have a policy that forbids the use of IM, but it has already happened. Unfortunately, the content of the IM session doesn't show in your audit log – but the fact that the IM session happened possibly does.

There are vendor solutions out there that identify rogue device applications and shut them down, or maintain dynamic blacklists at a granular level. These should be investigated rather than any homegrown approach.

What Else Can Be Done?

Firstly, the correct types of collaborative and social networking tools need to be utilised wherever possible. When it comes to IM, don't just go for publically available, consumer focused systems. Take a solid enterprise back end system from the likes of Microsoft or IBM/Lotus.

These can support the main consumer clients in areas such as IM, while providing tracking, content management and audit of content of blogs and wikis. Other systems, such as Witness Systems, can record the voice output from voice over internet protocol (VoIP) and standard telephone calls. Each also provides integration into existing applications and full logging of the content of sessions, so that an audit trail can show exactly what happened during any transaction.

For external systems, don't be afraid to use them when they are appropriate. Such sites have reach that the majority of brand names would kill for. For example, FaceBook will have more visitors in any one time period than any standard single corporate brand can hope to get to its own site. Therefore, a marketing campaign carefully crafted and aimed at the right geo-demographic, can be very successful on such sites.

But, how do we ensure that the content here is as legally correct as any information that is held on our sites? At the basic level, the answer is to regard the outside site as an extension of the main site. Still use the content creation tools that you already use. Use the same workflows that are already in place, looking for content reviews and legal sign off before publication. Quocirca recommends that content filtering technology from the likes of Clearswift, Symantec, Bluecoat or others be put in place to ensure that only information that should be leaving the organisation does leave, blocking the transfer of information that may be accidentally or purposefully leaked.

Beyond this, you will have to assign a group of content moderators, particularly if you are using such external sites as a means of encouraging interaction with the target audience. Once your content has gone live on the outside site, events are down to that site. Few social networking sites will allow for events such as inappropriate language or rogue content to fire off an external trigger or message to your own site.

Therefore, organisations will have to ensure that a regular watch is kept on incoming content on these sites taking action as appropriate. Bear in mind that here you are not just looking for the content that may be negative about the organisation – in fact, a lot of this should be left up there and responses posted against it – but for content that may be illegal and which if left on the site could result in a court case and/or heavy brand damage.

Controlling social networking is probably the wrong way to look at the issue. What is required is a guiding hand to ensure that everything remains coherent, consistent and correct - not a command and control approach, more one of a request and guidance.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at

<http://www.quocirca.com>