

TAKING THE BARK OUT OF WHUFFIE

Anria S van Zyl, CA(SA)

Accountancy SA Online CPD Articles, February 2010

"One can survive everything, nowadays, except death and live down everything except a good reputation." Oscar Wilde

The truth of the matter is that we all have whuffie... whether you want one or not. Whether you actively cultivate or nurture it. Whether you choose to build a wall and ignore it. Digital reputation (whether you call it Whuffie, Karma, social currency or goodwill) is an integral part of Social Networking, and you can lose it without even knowing you had it to begin with.

In his book "The future of reputation", Daniel Solove tells horrific tales of how people lost their digital reputation. He tells of a twenty-five year old who got terminated from her position as a senator's assistant after posting unflattering remarks about her relationships with co-workers on her blog named Washingtoniene. According to Jessica she created the blog to keep a few of her friends informed about her escapes. The blog however was not set up so that only invited members could read it. One could argue that her blog, a needle in the electronic haystack of cyberspace, was harmless and that her co-workers anonymity and reputations would be protected unless somebody who knew her, knew where she worked and could therefore identify the co-workers being discussed, accidentally found and read her blog. As misfortune would have it however another very popular blog, Wonkette, decided to link to her blog. Jessica's blog went global. She soon found out that it is virtually impossible to delete something on the web, as thousands of copies of her blog were archived, copied, printed and emailed. She damaged her reputation, her co-workers reputations, and indirectly her employer the senator's reputation who had to endure a backlash after her dismissal.

One is easily tempted to say: "Only in America", a quick search of local South African media will soon change your mind however. As a popular Sunday newspaper stated recently: We have all seen a Reprinted with permission ASA. This article first appeared in the Online CPD articles series of Accountancy SA February 2010, it is also available online at www.accountancysa.org.za

posting on a friend's Facebook profile telling us how fed up they are with their jobs, bosses and clients (Rapport 2009).

Damage to your organisational reputation caused by Social Networking activities can be caused by a number of diverse factors, some of these might include:

- Articles appearing in the press about employees being dismissed by an organisation for inappropriate use of office resources. These employees can quickly become martyrs in cyberspace.
- Staff can post negative comments about their organisation, clients and colleagues online.
- Former and dissatisfied customers can criticise and complain about the organisation using social tools creating a public image of the organisation outside the organisation's control.
- Employers using Social Networking Sites to obtain information about prospective employees could leave the employer open to the accusation of discrimination. It is important to note that only a minority of potential staff will have a public profile on Social Networking Sites, and using it as a source of information can either give certain candidates an unfair advantage or disadvantage.

We can try to deny that our companies are not at risk. The ostrich strategy will however not help you to escape the cold hard reality that your companies' reputation can be damaged from your employees' home, from an internet café, from your employees' own private cell phone, not to mention the legions of customers and other third parties you have absolutely no control over. The irony is that the only way to protect your companies' reputation might be to allow your employees to protect your castle walls.

Clay Starkey writes about the "Tragedy of the Commons". The Tragedy takes place where there is no community members willing to protect an online community from vandalism or misinformation. The community, if properly motivated will act against any other community members or outsiders who make postings that are deemed undesirable. The trick it would seem is to get your own employees to protect your company reputation in cyberspace, because by protecting your reputation they are indirectly protecting their own hard earned reputations.

Reprinted with permission ASA. This article first appeared in the Online CPD articles series of Accountancy SA February 2010, it is also available online at www.accountancysa.org.za

Maintaining staff morale and job satisfaction, while maintaining discipline and productivity is perhaps one of the biggest challenges to today's managers. Advocates of Social Networking and collaboration tools argue that these platforms create a culture of sharing, increase job satisfaction and by doing so it can increase productivity. Dissatisfied, unmotivated staff often complain that they do not feel valued, and that their contributions goes unnoticed, others complain about office politics and that undeserving staff members often get the promotions. In cyber communities everything you do leaves a digital footprint, your contribution whether it is good or bad cannot be overlooked, and somebody else cannot be credited with it.

In order to understand why your staff members would want to take the time and effort to protect your companies' digital reputation through participation in a virtual community, we first need to understand why people are motivated to contribute to digital communities. Why would thousands of individuals contribute to Wikipedia without getting any obvious reward in return? People do not do anything without incentives, but what could the possible incentive be?

The late Peter Kollock, an American sociologist, who studied online communities identified four motivations for people to contribute knowledge, expertise and time without the expectation of receiving a direct benefit (monitory or otherwise) in return. These findings can be summarised as follows:

- **Anticipated reciprocity**

A person can be motivated to contribute valuable information to the group, by expecting to receive useful help and information in return. This can lead to a culture of sharing knowledge and expertise.

- **Reputation and increased recognition**

Social Networking 2.0 reward contributions through ratings, feedback, and the creation of a following (people who link to, and subscribe to your work). This digital reputation serves to

Reprinted with permission ASA. This article first appeared in the Online CPD articles series of Accountancy SA February 2010, it is also available online at www.accountancysa.org.za

recognise a person's contributions to and beyond the immediate group, and places a value on the individual's knowledge and knowledge creation abilities. This increased visibility satisfies most individual's desire for prestige and recognition and increases their job satisfaction.

- **Sense of efficacy**

People can be motivated to share in groups due to a desire to have an effect on their environment by doing good things. Clay Shirky noted that more people are motivated to contribute to bad contributions, which they desire to make better, than by the desire to start a new article from scratch.

- **Need**

Individuals can be motivated to share innovation in the hope that the community will improve it and therefore the innovation would be more useful to themselves. This trend is most often seen in the open source movement, the improvements to Linux being the most notable.

Deciding to build a virtual community around your business is not enough however. It takes time to get employees to buy into the idea, and to start contributing. Depending on your organisational culture it might even be necessary to create other real world incentives, and allocate fixed time slots for employees to contribute to the community.

The risks of data leakage, resource waste, misinformation, defamation etc. is however real and cannot be overlooked. It is necessary to arm your employees with a little more than just good intentions. It is time to dust off the existing Accepted Usage Policies and re-evaluate the security training and education given to staff. Ensure that employees are aware of the organisational culture, social trust issues, proper etiquette, what they need to do when they become aware of a possible threat or vandalism and it is necessary that you have a proper response plan in case your castle wall gets decorated with graffiti.

Sources:

de Lange, R. 2009. Uitlatings kan jou duur kos. *Rapport 7 Junie*.

Shirky, C. 2008. *Here Comes Everybody. The power of organizing without organisations*. USA: Penguin Books.

Smith, M. & Kollock P. 1999. *Communities in Cyberspace*. London: Routledge. (p227-229)

Van Zyl, A.S. 2009. The Impact of Social Networking on Organisations. *The Electronic Library* 27(6).