



2011 saw some significant growth in social media usage generally:

- **Twitter** had 75 million user accounts in January 2010, but only 15 million used the site regularly. This resulted in 27 million Tweets per day. In March 2011, this had grown to more than 95 million Tweets per day and 175 million registered Twitter users.
- **LinkedIn** has grown by an impressive 100 percent from 2010 to 2011 with over 100 million users across the globe.
- **Facebook** had 350 million active users across the globe in January 2010, and in November 2011 it now has in excess of 800 million – half of which login daily. Users accessing Facebook via their mobile device has grown by over 200 percent. In early 2010 the figure was around 65 million, it now stands upwards of 200 million. This figure evidently reflects the rise in mobile device usage around the globe.



## Social media and NFPs: a perfect match

Social media has expanded beyond a point where it can be considered a flash-in-the-pan or a fad with many global NFPs, such as Greenpeace, the Red Cross and World Vision using social media to promote themselves and their causes. Moreover, the use of social media applications can level the playing field for small and medium-size NFPs.

The emergence of social media has produced the “perfect storm” for NFPs. It has the potential to deliver significant benefits in terms of building relationships, marketing, communicating with donors, fundraising and reducing costs. Social media applications enable the following

**BUILDING RELATIONSHIPS** - social media is all about relationships, making connections and sharing ideas, thoughts and experiences with like-minded people. It provides NFPs with an opportunity to connect with donors, to hear what they think and feel, in a way that was not possible previously.

**FUNDRAISING** - online donations are increasing and this is a trend that is likely to continue. In fact, research indicates that people who donate more than \$1000 to a single cause in a year prefer to make online donations as it is quick, efficient and immediate.

**TWO-WAY COMMUNICATION** - unlike advertising, social media enables effective two-way communication. NFPs can reach their market by joining with them in conversations that are important and relevant to them, making them more aware and more active with the organization.

**REDUCING COSTS** - social media is free. This enables NFPs to re-allocate limited funds from traditional, more expensive media advertising.

**PROMOTION** - social media is akin to word-of-mouth marketing, enabling organisations to promote their cause and access large numbers of potential donors at little or no cost. Moreover, research on donors indicates that they are generally baby-boomers, are experienced internet users and they spend approximately 18 hours a week online. In short, they pay bills, bank, get news and make frequent online purchases.

**SOCIAL MEDIA SAVVY** - NFPs attract Gen X and Y to their causes. They see the internet as the only real place to advertise and promote their cause. They do not understand or actively participate in the old world of advertising.

## The anti-social side of social networking

It is clear that social networking, just as in the case of the telephone and the internet, is the way of the future. It is equally clear that NFPs will need to proceed with caution as there are risks that could seriously impact the organisation.

When Warren Buffet coined the expression “It takes 20 years to build a reputation and only 5 minutes to ruin it!,” he must have been thinking of social networking. Inappropriate comments, pictures and videos posted on social networking sites by corporations, politicians, the military, actors and sporting celebrities make the point as their reputation and public image have taken a battering as a result.

However, the reality in today’s ultra-connected world is that it may take significantly less than 5 minutes. The speed with which inappropriate comments and content can spread around the world is a genuine concern and NFPs are right to be wary. Take Hollywood actor Charlie Sheen as an example. He joined Twitter on March 1 and within minutes had 60,000 followers without even a tweet.

Social media bring huge benefits to NFPs, but it also brings some huge challenges that need to be recognised and managed if they are to avoid HR, legal and compliance issues that could lead to irreparable damage to their organisation. NFPs need to consider the following:

**PRODUCTIVITY LOSS** - if employees or volunteers are on social networking sites for prolonged periods of time doing non-work related business or downloading unauthorised applications, there is a cost to the organisation in terms of lost productivity.

**REPUTATION** - an organisation’s reputation and brand can be seriously damaged as a result of inappropriate, offensive or confidential information published on a social network site. Publishing such content to the internet or to social media networks can result in lost donors, volunteers, revenue and destruction of stakeholder confidence in the organisation. With many NFPs relying heavily on donations for their funding, their reputation must be protected.

**LEGAL** - organisations can be held liable for any compliance, legal or OH&S breaches such as bullying, sexual harassment, defamation, downloading and viewing inappropriate content or illegal applications. These legal implications mostly apply to volunteers as well as employees and can cost significant HR time managing expectations and potential breaches of policy.

**COSTS** - viewing and publishing content to social media sites consumes a huge amount of bandwidth, which can impact the performance of business-critical applications and systems as well as drive up the cost of internet connections. Unauthorised software can cause conflict and stability problems if not properly tested.

**MALWARE** - malware, short for “malicious software,” includes viruses and spyware to steal personal information, send spam and commit fraud. The web is the primary source of spreading malware. Cybercriminals exploit new technologies like social networking sites by luring individuals to a website in the hope they will click and download malware. If downloaded, malware can embed itself in computers and spread to users’ contact lists, thereby infecting the systems of associates, friends and family members. These viruses are often programmed to steal personal information.

The cost of a malware attack to a NFP organisation can be significant and can be measured in lost productivity, revenue and possible fines for violating confidentiality and privacy agreements by allowing the disclosure of sensitive information. If subjected to an attack, employees may be unable to continue working due to a laptop failure or shutdown. The IT staff will need to spend time rebuilding and reconfiguring all machines and systems that are compromised. Microsoft reports that phishing using social media networks such as Facebook has risen 1200% over the last year (2010-11).

**DATA LEAKAGE** - across industries, compliance has become an increasingly important corporate initiative. Regulations including the Privacy Act, Sarbanes-Oxley, HIPAA and similar legislation and regulations make it a priority to maintain and protect data. With an increase in cyber threats and targeted attacks, organisations need to ensure system and data integrity as well as demonstrate compliance.

With the increased threat to sensitive data, there is an increased risk of damaging an organisation’s reputation with its stakeholders. Adhering to compliance standards not only saves untold costs from fines and data loss, but also provides an extra level of confidence for donors.

**CYBER BULLYING** - is often defined as bullying that uses e-technology as a means of victimising others. It is the use of an internet service or mobile technologies - such as e-mail,

chat room discussion groups, instant messaging, web pages or SMS (text messaging) - with the intention of harming another.

Cyber-bullying has been widely reported in connection with children and schools however workplace cyber bullying is an increasing issue. The Victorian government in Australia as an example has introduced new legislation to make workplaces safe, secure and free of harassment and bullying. Bullies could receive up to 10 years in jail if convicted under the new "Brodie's Law."

Workplace bullying is also covered under most Occupational Health & Safety (OH&S) legislation and the responsibility to provide a safe workplace is still with the employer. Management may be held personally liable if bullying is found to have occurred and they have turned a blind eye.

## 5 steps to making social networking work

It is understandable that the natural inclination, given the risk level, would be to block access to social media sites. In fact, it is estimated that more than 60% of organisations believe this is the way to go.

However, it is not a matter of opening the floodgates to give employees and volunteers uncontrolled and unfettered access to social media sites. The sensible approach for organisations is to identify and understand the risks, and to develop a social media strategy that might incorporate the following:

**1. LINKING WEB 2.0 TO BUSINESS STRATEGY** - the foundation of a Web 2.0 strategy should be the same as every other marketing strategy: a link to the overall business strategy, a specific target audience, and clear, measurable goals. This must be followed up with a clear plan assigning responsibilities and goals to the activities.

**2. LEGAL AND HR FRAMEWORK** - with social media has come new legal issues. It is important that all staff and volunteers are educated on such issues as copyright infringement, downloading music or videos, posting inappropriate or offensive content on blogs, using sites to discriminate against or to harass fellow employees and not to make negative comments about the organisation on social networking sites.

Review all employment contracts and volunteer engagement agreements and include terms obliging them not to disparage their employer, both during and after their connection with

the organisation. Make sure any changes to contracts and agreements are well communicated. Make sure that all current and future employees and volunteers understand them and the obligations they impose.

**3. EDUCATION AND COMMUNICATION** - Organisations will need a social networking policy that explicitly lays out what is and isn't permissible, both on the organisation's network and outside of it if they're presenting themselves as representatives of the organisation. However, 75% of organisations have no formal social media policy or guidelines.

**4. MEDIA MONITORING** - utilise alerting and monitoring applications and services such as Google Alerts to monitor blogs, forums, Twitter and other social networking sites. This will enable individual organisations to respond to positive and negative comments quickly and decisively as well as to take any legal action required. Have a prior agreed plan in place to manage the escalation and response to reputation damaging posts.

**5. TECHNOLOGY REVIEW** - organisations should review the current technology infrastructure to ensure that it works with Web 2.0 technology as many traditional IT security and control technologies simply do not address the risks associated with accessing content in real time via social networking sites. For example:

- Network firewalls provide little protection as Web 2.0 relies primarily on standard HTTP and HTTPS protocols that simply can't be blocked without cutting off Web access. Applications such as gaming, instant messaging or peer-to-peer services can be launched from a USB 'thumb drive' and are applications as opposed to websites. These need controlling at the application level as opposed to by traditional outdated web filtering technologies.
- Traditional anti-virus systems are limited to inspecting file transfers, however many of the greatest "drive by" threats encountered today are contained in browser scripts that are invisible to anti-malware filters.
- Web reputation services alone are ineffective as some of the most valuable sites on the Web, such as Google or Yahoo, have fallen victim to hosting malicious code, and simply blocking access to these sites is not an acceptable answer for most businesses.
- Simple URL filtering that blocks objectionable or time-wasting content based on the home page address of the Web site no longer works when sites now commonly aggregate information from multiple sources.

## Summary

In order to take advantage of social networking, NFPs of all sizes need to create policies and guidelines to regulate social media usage and to educate employees about defamation, sexual harassment and copyright infringement. They also need to explain the ramifications for uploading offensive comments, downloading inappropriate content or using social networks as a vehicle for bullying, discriminating or intimidating others.

New and innovative technologies will go a long way to reducing the risks and concerns many organisations have with social media. These new technologies need to protect NFPs from growing cyber criminal attacks, malware, identify theft, intentional and unintentional data leakage. NFPs need to audit their technology solution to ensure that it addresses the new threats that Web 2.0 technology poses.

The technology landscape has changed dramatically within the last few years; staff are no longer tied to the office and the desktop computer - they are mobile; the office is anywhere there is a 3G or Wi-Fi connection; they connect to the internet and download content to mobile phones, laptops and iPads; they communicate using email, instant messaging, text and any number of social media applications. Here are some technology must haves:

**ONLINE/OFFLINE MONITORING** - it is important that your technology solution should extend the ability to monitor and control any device on or off the network on any company-owned Windows and Mac OS X devices. It should have device-level protection for all internet use.

**BEYOND-THE-PERIMETER CONTROL** - with the emergence of mobile technology, the network perimeter is not as clearly defined as it once was. It is therefore critical that your solution provides for endpoint AV protection. This will ensure that each company laptop and device in use by a mobile worker or remote computer accessing the network is protected and can be easily updated for new threats.

**WEB AND SOCIAL MEDIA ENFORCEMENT** - research from IDC shows that organisations that monitor web use reduce the incidence of viruses by a factor of five. It is therefore important that in addition to your customary anti-spam, anti-virus and malware protection, you need to be able to monitor social media usage. Social media security generally needs to cover Web 2.0 communications such as webmail, search queries and posting content to common social media sites.

### **REAL-TIME ALERTING AND BLOCKING CAPABILITY**

- if prevention is the cure, real-time alerting and blocking are essential. Inappropriate uploads and downloads need to be blocked immediately to prevent harm to the company and the individual. You should be able to set up real-time alerts to inform administrators or managers when rules or policies have been breached.

Also, monitoring of web searches and use can provide early warnings of potential health or personal issues that might be impacting productivity or performance. Managers should be able to access reports via browser or have them emailed to them automatically.

### **MULTIPLE DEVICE PROTECTION**

- laptops and mobile devices are easily lost or stolen, putting any data they contain at risk. A technology solution must have the following capability: password protection, remote-wipe capability and physical device tracking.



### *More info...*

- **Cerebral Palsy League of QLD**
- **Surf Life Saving QLD**
- **netboxblue.com**

