



DeCISion



A publication of CIS Pty Ltd

www.cis.com.au

PO Box 1155, Box Hill VIC 3128
 Ph: (03) 9899 4433 Email: info@cis.com.au

Welcome to the March Issue!

Dear Valued Readers,

Welcome to the March edition of DeCISion. We can now say goodbye to Summer and start to welcome some cooler days that lie ahead.

CIS held another successful seminar last month, titled "How Excellent Leaders Lead". If you were unable to attend you can view Russ Wylie's presentation at our website – www.cis.com.au. CIS look forward to seeing more of our readers at our next seminar.

In this month's DeCISion, we focus on the impacts of Social Networking sites. This article discovers the potential benefits and risks these sites have on corporate organizations and looks at what to weigh up when creating policies and procedures in relation to employee usage.

Enjoy this edition of DeCISion – and we look forward to seeing you next month. All the best, Stephanie Olszak & The Team at CIS.

Inside the March Issue:	
Developing Employee Social Networking Policies That Meet Corporate Needs	P 1 & 2

Developing Employee Social Networking Policies That Meet Corporate Needs
 Written by Lana Owens

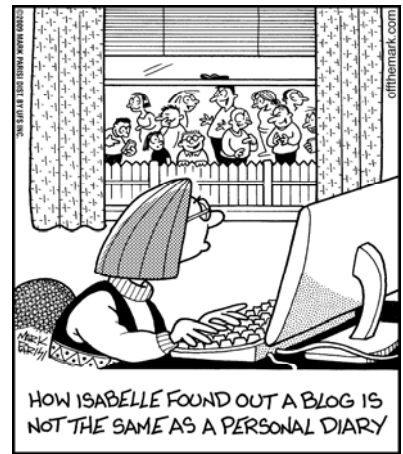
Social networking has become a global phenomenon, and there are no signs its growth will decelerate anytime soon. According to the marketing and media information company Nielsen, two-thirds of the world's internet users engage

in social networking sites; social networks occupy nearly 10% of all Internet time. While social networking was once largely an activity of the younger set, leading social network Facebook reports that this is no longer the case. The website's greatest growth has come from the age 35-49 demographic.¹

Many experts across different academic fields and industries espouse the benefits offered by social networks for businesses; building brand name recognition and consumer trust are a few popular topics. However, the benefits to organisations are weighed against the alarms raised when employees spend time at work social networking. While loss of productivity is an issue, corporate security is a greater perceived threat. A recent survey conducted by an IT security firm of 500 organisations, found that 72% were concerned "that employee behaviour on social networking sites exposes their businesses to danger, and puts corporate infrastructure - and the sensitive data stored upon it - at risk."² They examined the risks and benefits of social networking, and based on their research have identified key factors that IT Managers should consider when composing a practical employee policy.

First, they have uncovered several risks social networks pose to companies. The 2010 "Security Threat Report" released by IT security firm Sophos explains that among the social network users in their survey, 57% reported spamming and 36% admit to having received malware through a social network site. While Linked In – the social network dedicated to career-minded users – may seem less threatening, this is not the case. Linked In offers a unique set of information to hackers targeting organisations.

*"Targeted attacks against companies are in the news at the moment, and the more information a criminal can get about your organisation's structure, the easier for them to send a poisoned attachment to precisely the person whose computer they want to break into. Sites like LinkedIn provide hackers with what is effectively a corporate directory, listing your staff's names and positions. This makes it child's play to reverse-engineer the email addresses of potential victims."*²



Organisations also perceive non-IT threats posed by social networks. A company's brand and reputation could be negatively impacted by an employee that intentionally or unintentionally leaks data or disparages the corporate brand on social networking sites.

However, many corporations recognize the benefits offered by social networking when employees participate. The primary tool social networks share is users' ability to connect with others. Sales and marketing departments can directly communicate with customers. These communications

can vary, from subtle brand promotions to direct messages that target specific consumers. Within the past few years, sophisticated online metric tools have been created that allow sales and marketing departments the chance to measure their social network campaigns. These unique resources often provide invaluable information about how consumers perceive an organisation and its online advertising.

Organisations have also discovered that social networks provide invaluable opportunities for human resources recruiters. Many companies screen applicants' social network profiles to reveal any negative personal or professional information – a potential sign an applicant would contribute to disharmony. New recruiting tools for social networks also help employers locate applicants that are “a perfect fit.” According to the May 30, 2009 New York Times article “Finding New Employees, via Social Networks”, several social networking products now innovate hiring. For example, online resources provider Appirio offers a tool that asks an organisation's employees to add an application to their Facebook profile. The app notifies employees about internal job openings and specifies which of their Facebook friends may be an ideal fit.³

Companies are provided several other benefits through their employees' social network participation. First, employees are able to build personal ties with their co-workers and managers, strengthening their company's group psychology. These improved employee relations may directly relate to increased productivity. Secondly, when social networking communication occurs between employees, opportunities arise for collaboration and innovative group brainstorming. Social networks present unique chances for employees to bond on personal and professional levels, and in turn directly stimulates organisational work product.

IT managers clearly have to weigh the risks and benefits of social networking when they develop a solid set of policies and procedures for employees. Some

organisations have opted to issue strict social network prohibition, even dictating employees' social networking behaviour outside of work. However, a number of companies have not chosen this rigid approach. In fact, many organisations still have not implemented their employee social networking policy, according to Joan Goodchild, Senior Editor of CSO Security and Risk, an IT security and risk management firm.⁴ There are several reasons many companies have not issued their employees a policy on social networking activity. Executives are concerned that a prohibitive social networking policy will be ignored, or employees will develop negative attitudes about the company. Other leaders are unsure about the future benefits social networking could offer, and do not want to hastily limit the practice before more information is uncovered.

Every organisation is culturally different, so policies and procedures will vary. However, due to IT security risks, along with potential harm employees could cause the company through their social networking behaviour, IT Managers must establish an appropriate employee social networking policy. Policy definitions must address work-time spent on social networks; admissible behaviour online; and illustrate how employees may discuss work, their co-workers or supervisors, and the company.

The following factors should be considered when creating corporate social networking policies:

- Protocols may need to be individually tailored for different work groups. Sales and marketing employees may require work-time spent on social networks while other department managers determine the activity is unnecessary.
- Company leaders may have strong opinions. Some managers feel they offer employees a necessary outlet by allowing time on social networking sites during the work day.
- IT Managers must clearly comprehend the stability of

corporate IT systems. Some businesses may lack the IT infrastructure to handle potential security threats or increased bandwidth usages related to employee social network activity.

IT Managers can create corporate social networking policies that meet specific company needs. Understanding the risks and benefits allows IT Managers to gain a greater perception of social networking outside of IT security concerns. Through careful consideration of the policy-development factors we provided, IT leaders can successfully assess their organisation's needs and build a functioning social networking policy framework.

While developing a corporate social networking policy does present challenges to the IT leader, if executed well the IT group may benefit as a result. We were intrigued by a possibility offered by Jack Phillips, Co-Founder and CEO of IANS, a research company devoted to IT security and compliance issues. IT Managers can use a social networking policy to raise security awareness among employees, who may not be aware of the risks imposed by their activities on the internet. Further, the increase in awareness could positively develop IT security's profile throughout the organisation.⁵

References:

1. <http://blog.nielsen.com/nielsenwire/global/social-networking-new-global-footprint/>.
2. <http://www.sophos.com/pressoffice/news/articles/2010/02/security-report-2010.html>
3. <http://www.nytimes.com/2009/05/31/jobs/31recruit.html>
4. http://www.csoonline.com/article/529764/Social_Media_Risks_The_Basics?page=3
5. http://www.csoonline.com/article/505593/4_Tips_for_Writing_a_Great_Social_Media_Security_Policy

If you care at all, you'll get some results. If you care enough, you'll get incredible results.
Jim Rohn