HelpSource Q&A

We invite you to send your information
systems audit, control and security
questions to:
HelpSource Q&A
bgansub@yahoo.com

Fax to: +1.847.253.1443
Or mail to:
ISACA Journal
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Gan Subramaniam, CISA, CISM, CIA, CISSP, SSCP, CCNA, CCSA, ISO 27001 LA, is the global IT security lead for a management consulting, technology services and outsourcing company's global delivery network. Previously, he served as head of IT security group compliance and monitoring at a Big Four professional services firm. With more than 16 years of experience in IT development, IS audit and information security, Subramaniam's previous work includes heading the information security and risk functions at a top UK-based business process owner (BPO). His previous employers include Ernst & Young, UK; Thomas Cook (India); and Hindustan Petroleum Corp., India. As an international conference speaker, he has chaired and spoken at a number of conferences around the world.

Q Internet access given to employees is mostly restricted using either commercial packaged software or by some other means. What kind of restrictions must be put in place regarding the use of social networking sites and blogs? Blogging has become part of everyone's life and even leading employers have started making their presence felt in social networking sites such as Facebook and Twitter.

What are your thoughts in terms of policies and controls that must be put in place for these?

A Blogs have become an integral part of our personal and professional lives. Many times nonmalicious acts may land employees and employers in trouble. Equally, an employee with malicious intent can post the most sensitive and confidential information with an aim to embarrass the company.

There is an argument that blogs may not be suitable for all organisations. While there is no doubt that it is an emergent and widely used technology, the lack of sufficient maturity of the organisation may lead to the conclusion that blogs may be counterproductive.

The informal style or the conversation-like information on blogs makes them attractive to the authors and to their readers who flock to read them. Equally, the same informal style makes it dangerous from an organisation point of view.

Lack of policies governing the use of blogs and social networking sites open up a number of risks to the organisation such as:

- Loss of confidential information including proprietary trade secrets and patentable intellectual property (IP)
- Reputation loss due to malicious posts on the web
- Legal suits and claims relating to potential sexual harassments, defamation, etc.
- Regulatory or legal noncompliance
- Impact on employee productivity

There should be a clearly defined policy outlining the responsibilities of employees when they indulge in blogs. Putting a blanket ban on the use of blogs is not possible; however, the rules of the game must be clearly set.

Such rules must include the following:

- The language, content and usage must align to preset standards, and employees cannot be liberal based on their whims, publishing whatever they want however they want.
- The content posted by employees, in particular, must be in complete alignment with other existing policies of the organisation on topics such as sexual harassment, discrimination, diversity, ethics and compliance, and, above all, confidentiality rules and regulations. Employees may knowingly or unknowingly violate policies while writing on their blogs and land themselves and their employer in trouble.
- No opinion, whether personal or professional, must be allowed to be posted on blogs be it overtly positive, leading to some potential stock market fluctuations, or negative or critical of the employer's products, services, co-employees, senior management, competitors, clients or customers, business partners, or vendors. The issue is the employer may end up facing the consequences on such occasions.
- Employers can be held accountable and responsible for the acts of employees, which is called in legal parlance 'vicarious liability'. For example, in the UK when an e-mail was exchanged internally between two employees of a financial institution potentially defaming a competitor, the competitor got wind of the e-mails and sued the other institution for damages and the court upheld the claim. Whether it is an act of stupidity or a deed of malice by the employees, it can still harm the employer.
- Policies and procedures of the employer must and shall apply consistently irrespective of whether employees post information on their personal or official company blogs. Assuming that personal blogging is allowed using the

computers supplied by the employers and given that such computers are company assets, any information created using them also belongs to the company. The question of privacy does not arise here.

- Employees must not use the corporate logo or symbol, trademarks or advertisement taglines, or other patented or IP-protected materials on their personal blogs.
- Posting information on blogs anonymously or using pseudonyms must be discouraged or, better, banned. Allowing such practices may lead to an indirect encouragement of employees posting whatever information they want, because they are confident that their identities are hidden. Various courts have taken different standards on the 'lifting of the veil' in terms of allowing or disallowing Internet service providers (ISPs) to identify the names of individuals who have posted the information. For example, India had a classic case in which an ISP disclosed the IP address and the name of an individual incorrectly, wrongly assuming that he had posted the information and leading to the arrest of an individual who was completely unrelated to the blog.
- All those who post information on blogs must clearly use a disclaimer stating that the views and opinions expressed therein are completely their own and do not necessarily represent the views and opinions of their employers. I am not a legal expert to comment on the sufficiency of such disclaimers' ability to protect the organisation, but perhaps it is better to have something rather nothing.
- The company's media management policy must be linked to the blogging policy. Any media frenzy or inquiry must be handled by the employees working in conjunction with their public relations department and not on their own volition.
- If the organisation chooses to put processes in place to monitor the blogging-related activities of employees, such monitoring must not be undertaken covertly. There must be explicit communication to the employees on the monitoring mechanisms put in place.
- Employees who blog—internally or externally—must be aware of the retention policies of blogged information; the information posted on the blogs may end up as evidence in the court should any litigation arise involving the blog posts.

Social networking sites equally carry the same risks as blogs. Given the way people connect and network with each other, there is every possibility that information can be shared inappropriately.

There is no simple, straightforward solution to the problems noted here; creating risk awareness is the best possible option.

As always, the content here must not be construed as legal advice and, equally, the points I have discussed are only indicative and not exhaustive.

Q&A