Web 2.0 Privacy and Security Considerations

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI
Final Draft for October 2008 CSI Alert

Much has been written about “Web 2.0” and how it can be used for business, the risks of employees wasting their time all day using “Web 2.0” and so much more. But, do you really know what “Web 2.0” means?

Web 2.0 is generally a term, made popular after the first O’Reilly Media Web 2.0 conference in 2004, describing the emerging ways in which World Wide Web technology and web designs can be used to enhance and make easier information sharing, creativity, and group collaboration. Web 2.0 services and technologies include such things as social networking sites, wikis, blogs, micro blogs, mashups, crowdsourcing, surveillance sites, and folksonomies. And more are emerging.

There are information security and privacy concerns for all of these Web 2.0 capabilities. Organizations need to think about the threats all these Web 2.0 offerings bring to their organization, determine the risks, create a set of policies to address the use of Web 2.0 services and technologies, and then provide personnel with training and ongoing awareness for how to use them in appropriate ways that safeguard business, customer and employee information.

Here are three popular Web 2.0 activities, along with some of the corresponding privacy and security concerns, to help you with establishing your own Web 2.0 policies and procedures.

What are the information security and privacy concerns for social networking sites?

Social networking sites provide an easy way for individuals to share information about themselves. However, as a large and growing number of social networking site members are discovering, the information shared with site friends can very easily be shared with others, or even posted on Internet websites for the whole world to see. This goes for the people at work, as well. When personnel post information about their work on social networking sites, the risk is great that the information will be shared with others that could misuse the information for criminal purposes, or damage the company's reputation in some other way.

It is also a growing trend for employers to look on the Internet, including social networking sites, to see if they can find information not only about job candidates, but also about current employees. There have been several instances were people lost their jobs because of the information that was originally posted to a social networking site.

Also consider that email harvesting from social networking sites is a widespread practice. If you have folks using their company email addresses on social networking sites, it is likely you will experience an increase in spam coming into your corporate mailservers.

Key information security and privacy issues to address with social networking use from corporate networks and computers used for company business include:

- Determining and documenting the types of business information that must not be posted by personnel and contracted workers onto social networking sites.
- Establishing acceptable social network use policies.
- Documenting the social networking sites that personnel must not use while at work, or while using a work computer.
- Or, perhaps easier to do, documenting the social networking sites that personnel are allowed to use from the corporate network and work computers.
- Making your personnel aware of security and privacy risks involved with using social networking sites. Include such information as:
    - Look for a posted privacy policy and understand the security privacy controls offered to the site participants.
    - Know who can access personal pages. Some sites allow participants to restrict who can access pages, but others do not.
    - Do not use company email accounts on social network sites. If possible, use anonymous e-mail addresses. This can help protect not only PII, but also help keep spam out of the corporate mailservers and employees' personal email accounts.
    - Don't give out personally identifiable information (PII); don't post such things as SSNs, home addresses, bank accounts and other sensitive information on your social network pages.
    - Use strong passwords, consisting of at least eight alpha and numeric characters.
    - Use a good user name. Using a pseudo name helps to protect users' identities.
    - Always use active and up-to-date anti-virus, anti--spyware and firewalls on your computing when visiting the sites.
    - Never post anything to a social network site that should not be shown to anyone in the world.

What are the information security and privacy concerns for blogs?

Increasing numbers of people blogging means increasing concerns of executive management about the information their personnel share within their blogs. These concerns spill over into personnel off-work time when they blog about their work, co-workers, business plans, and so on. In response, growing numbers of organizations are implementing programs to actively review the blogs that their personnel maintain and to which they contribute. Employees have been fired for information found within not only their blogs, but for what has been said in other people’s blogs. Job candidates have also been rejected because of information found within blogs.

Before implementing a blog review procedure, though, organizations need to study the statutes effective in their jurisdictions that impact their legal rights to look through personnel blogs. Organizations cannot legally act on certain types of information they find. For example, organizations often cannot fire or apply sanctions against personnel solely based upon information found within blogs about such topics as sexual orientation, union activities, political actions, and so on.

Many organizations are also establishing blogs as a way to market their company, products or services, or to allow for a communication method between their employees. This is fine if organizations remember that blog posts are generally considered as a form of publication. As such they are typically under the same requirements and subject to the same types of liability risks.

Key information security and privacy issues to address with blog use from corporate networks and computers used for company business, and for employees who maintain their own blogs, include:

- Determining and documenting the types of business information that must not be posted by personnel and contracted workers onto company sponsored blogs, as well as personal blogs.
- Determining and documenting how personal opinions may and may not be provided within company sponsored blogs, and the accompanying notices that must be provided within blog postings.
- If appropriate for your organization, asking personnel who have their own blogs to sign nondisclosure agreements to help keep business information from being discussed.
- Establishing strong security controls around company-sponsored blogs; malware may get into your organization through blogs if you don't.
- Establishing and documenting policies and procedures for how employee blogs may and may not be monitored.

What are the information security and privacy concerns for micro-blogs, such as Twitter?

Twitter is arguably the most famous of the micro-blogs; blogs that allow only up to 140 characters per post, and that people have seemed to become addicted to using to relay their every move and thought. People also use micro-blogs to talk about things beyond what some consider as ethical. A recent example is when, in September 2008, a Rocky Mountain News reporter used a micro-blog to report the play-by-play description of the funeral he attended of a 3-year-old boy who was killed when a pickup truck crashed into a Baskin Robbins ice cream shop in Aurora, Colorado. This was widely viewed as not only being inappropriate, but also being unethical and insensitive.

There are certainly ways in which using micro-blogs can provide some business benefit. For example:

- Publishers are finding some good uses for it using it as a marketing tool
- NASA has used it to keep interested folks up-to-date with satellites
- Conference goers use it to communicate with colleagues at conferences to keep each other informed about sessions
- Travelers coordinate the geographic/physical locations of co-workers while they are traveling

- Coworkers use it to perform disaster recovery, fire, tornado, terrorist, and other types of drills
- Celebrities, sports stars and musicians use it to communicate with their fans and groupies
- And many more possibilities

However, I've also seen many people posting their whereabouts to their micro-blog sites, along with where they plan to go, who they are with, and other juicy information that, if I were a burglar or some other type of criminal, I could really use to commit some huge thefts, frauds and other crimes. I've also seen the same people who micro-blog about their locations minute-by-minute also ironically complain about how their company, parents, whatever-authority-figure, wants to have them use a GPS/RFID/some-other-tracking-system.

I've looked through many online micro-blogs and I'm seeing information posted about business plans (YIKES! although I'm sure competitors like it); customers (YIKES! a civil suit waiting to happen, not to mention a path to privacy breaches); complain about their bosses (YIKES! a career-limiting activity); plus many other types of information that is or could be damaging not only to the business, but also to employees ("...Sue just stole my idea! She'll be sorry...") and customers. Most organization should be able to review and update their "electronic messaging" policies to address these issues.

Key information security and privacy issues to address with micro-blog use from corporate networks and computers used for company business, and for employees who maintain their own micro-blogs, include many of the same issues as for regular blogs, in addition to:

- Establishing the limitations around which micro-blogs may be maintained during work hours.
- Establishing effective, and reasonable, policies that indicate the types of business information that can and cannot be posted to micro-blogs.
- Providing training and awareness communications to indicate inappropriate uses for micro-blogs that would not be allowed under the corporate ethics policies, as well as the security and privacy policies.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, "The Privacy Professor" tm is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She creates learning tools, such as "Protecting Information" and "The Privacy Professor's Security Search #1," and blogs daily at http://www.realtime-itompliance.com. She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.