On The Internet, If It Looks, Quacks and Walks Like a Duck, Is It REALLY a Duck?

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Final Draft for June 2007 CSI Alert

"A wise man believes only half of what he hears and a genius knows which half to believe." – Unknown origin

Employee privacy is often associated with the use of surveillance cameras, recording conversations, and email monitoring. However, there are growing uses of online sites and technologies related to employee activities and vetting job applicants. Sometimes employees are fired for what is found, and it is more common to make hiring decisions based upon information gleaned from the Internet. Business leaders must judiciously use information they find on the Internet and become savvy about Internet practices and trends.

Just because it appears so doesn't make it so

It is likely that a large percentage of your personnel, especially if you have a comparatively young workforce, have their own websites, blogs, and/or listings on social sites such as MySpace and Facebook. I have spoken to several organizations that monitor the Internet to find out information that may be posted about their organizations; pretty common, eh? And certainly a good idea in today's business environment.

Many companies include within their search practices employee sites, blogs, and entries on these social sites. The information is public, and the employees made the decision to post the information in a public forum, so if a company finds information that concerns them on the employee private sites, they should be able to use that information to make job-related decisions, right? That's the stance that many organizations are taking, anyway.

Consider the following:

- On May 9, 2007 it was widely reported that the general manager of an Olive Garden restaurant in Orange City, California, was fired after working at the restaurant for 18 years because of a photo posted on her daughter's MySpace page. The photo showed the manager with her daughter and her daughter's boyfriend, holding empty beer bottles she said they got from a recycling bin for a "crazy picture" for her daughter's eighteenth birthday at the restaurant. The restaurant indicated that showing a manager with a minor, looking as though they were drinking alcohol, could hurt employees and the company brand. The fired manager is considering legal action, as are her former coworkers who believe she was wrongly dismissed.
- On May 2, 2007 it was widely reported that a student at Ohio State University (OSU) lost both his job as a resident adviser and his dorm room because of photos his friend posted pictures of him on Facebook. The pictures were taken at a New Year's Eve party the student hosted at his parents' house in Dublin during winter break, showing the 20-year-old student, who was not shown

drinking in the photos, with other underage OSU students who were consuming wine and beer.

- On April 28, 2007 it was widely reported that Millersville University in Pennsylvania denied a student a teaching degree the night before her graduation because they found a picture of her, taken at a 2005 Halloween party, wearing a pirate hat while drinking from a plastic cup on her MySpace site. The student received "superior" or "competent" ratings on her final student-teacher evaluation in all areas except for "professionalism," where she was rated as "unsatisfactory" because of the photo, according to the suit she subsequently filed. The student is suing the University.
- In March 2007, it was widely reported that a high school bus driver, who was also a volunteer fireman, in North Carolina lost both jobs after information about his Wiccan religion and his wife's bisexuality was found on the couple's MySpace page. The man is suing in federal court alleging the school system and fire department used his page as an excuse to dismiss him.

These cases occurred just within a matter of a few weeks of each other; there are many more similar types of cases where employment or employment opportunities were terminated because of information found on the Internet. What is interesting is that in two of these four examples other people posted the photos that got the employees terminated.

According to an October 2006 CareerBuilder.com survey, 24% of hiring managers use the Internet to screen potential employees. Of those who do, 51% say they did not hire based on what they found.

It is certainly prudent and wise to do all you can to ensure you are hiring trustworthy people; I endorse background checks of various types as a leading business practice. It is also important to ensure the folks working for you are not doing anything against your company's policy. However, be careful in jumping to conclusions based upon words or a photo found on the Internet. Pictures are worth a thousand words, but sometimes the stories they appear to tell do not really reflect what really happened. Digital cameras and computer software can easily fabricate a situation. You must know the context of the situation, and get the involved person's point of view, to bring the picture into accurate focus.

Even if it is legal to fire someone because of a picture of them partying, it could severely impact the attitude and moral of your other employees, resulting in other employees quitting, filing lawsuits as in the Olive Garden case, and even giving your organization a reputation as a bad employer, making it hard to find good folks willing to work for you. Also, if it turns out the photos were not accurately representing the situation after you fire someone, you do not want the publicity of being duped by bogus information

The OSU publication, The Lantern, reported that Aerotek, a professional staffing agency based in Columbus, uses Facebook and MySpace to find recruits. You may want to check with your HR area to see how the Internet is used for screening potential hires, and for doing checks on current employees. Be sure to include your legal counsel in your discussions.

Beware when others speak on your behalf

Many organizations allow, and in many cases encourage, their personnel to post on Internet sites, to blogs, within Internet communities, and various other locations. It is a growing trend to have a blogging site on the corporate website for employees to make posts. The issues are many, but few organizations have really thought about them all; the implications of employees posting from the corporate network, using their corporate email address within online postings, the time used while at work to post, the possibility of libelous statements being made that the corporation may have to ultimately end up paying for, and many assorted other issues.

Some of my information assurance colleagues have found troubling statements their personnel have made, on their own time and from their own home accounts and computers, about their organizations. Some have posted information about competitors and sensitive information about individuals and customers. Some have posted outright lies. The legal counsel within many organizations consider such issues to be covered by the respective organizations' non-disclosure agreements (NDAs).

In a recent case Reunion Industries, Inc. claimed that anonymous defendants posted libelous statements and committed defamation through the Yahoo! Financial Bulletin Board. Reunion Industries tried to force AOL (the ISP for the posters) to provide the identity of the defendants. However, on March 5, 2007, the judge denied the motion until Reunion Industries presented sufficient prima facie evidence (generally enough evidence to establish a fact, and if not denied or proven to be wrong, becomes conclusive of that fact) to meet the defamation standard. The court ruled that to meet the defamation standard for a corporation, Reunion Industries would need to prove actual damages.

Could your organization prove actual damages if someone posted anonymous libelous or defamatory messages? What documentation would you have to demonstrate the damage? What kind of logs do you keep to validate such damages? What would happen if someone anonymously posted a customer database to a website? What if they had good reason to suspect a certain person, but no hard evidence? Have you planned how to request a site to remove incorrect information? Do you know if and when you would post a rebuttal to such libelous statements? These types of incidents are starting to occur more frequently. Now is a good time to consider how to address them for your organization.

Beware of the lies and lying liars

On the flip side, what if you find derogatory remarks written about your employees on the Internet? What would you do? Would you take them at face value, discuss with your employee, or determine the source of the sour statements? Would you take a potential employee out of hiring consideration based upon anonymous remarks about them, even if everything else you found about them was stellar?

According to a December 2006 Ponemon/ArcSight study, around half of U.S. companies use the Internet to vet job applications. Information found in around one-third of the searches resulted in the candidate being turned down for a position.

Earlier this year a Yale Law School Phi Beta Kappa graduate, with articles published in highly respects legal journals and completed internships at leading institutions in her field, sent applications to 16 firms. It seemed to her friends and professors she would be a shoe-in at any of the firms. She received only four call-backs and got zero offers. While it cannot be conclusively proved, she believes this was because she was a victim of harsh and derogatory anonymous remarks on law discussion board run by Anthony Ciolli on AutoAdmit, a widely read college discussion site.

AutoAdmit contains discussions about schools and companies. However, a preponderance of anonymous users also post negative and hateful messages about women, and minorities, and they use actual names and other PII. It is common to see false claims and fabricated information. These postings subsequently get spread throughout the Internet and via search engines, such as Google.

Ciolli, who was a law student at the time of the incident, refused to remove the derogatory statements and misinformation from the site. It is interesting to note that the law firm that had offered Ciolli a position rescinded their offer after the news about this incident was published earlier this year because the actions did not fit with their code of ethics by allowing and facilitating libelous and hate-inciting language, including messages making explicit physical threats to specifically named individuals, to be posted on his board.

Generally website operators are not liable for information posted by others. Anonymous posters can be sued for defamation, and the court can require website hosts to reveal the identity of posters. However, such information is often not available because anonymous posters of such flaming remarks often do not provide accurate information about themselves. There is also a growing tendency of the owners of such discussion sites to not collect PII about posters to begin with not only to encourage posters to be more frank because they will not fear retribution for their comments, but also so the website owner can legitimately say they cannot help with investigations.

Do you have website discussion boards set up on your corporate website? Do you know for sure? I have run across information security officers who were surprised to find discussion sites set up on some of their business unit sites that were being unmoderated and went against corporate website management policies.

"I'm Captain Jack Sparrow....savvy?" ARRRGGGGH!

As we become an increasingly more online society, with more people keeping not only personal blogs but also posting to others' blogs, chat rooms, discussion boards, virtual communities and personal websites, organizations must consider how these areas are used within business and for employment purposes. Be savvy to the fact that all information purported to be fact must not be taken at face value; everything is not always as it seems. Before taking action based upon information posted on the Internet obtain proof to validate claims. Anonymously posted information is a big red flag; be savvy…be skeptical.

Business leaders must be aware of the negative ways that such Internet sources of information can impact their company and/or their employees. They must realize that not only their own company's reputation may be pirated through misinformation, but that potential and current employees may also have rumors spread as fact by numerous cyberspace scallywags. At the same time they must also realize they may have some sharks within their own ship that may try to post mutinous information about the company on the Internet seas if proper procedures and controls are not in place.

Information security, privacy, legal and HR leaders need to go to lunch together and talk about what issues their organizations face with regard to what needs to be done when information from, or about, their organization is posted, and what, if any, logs or other documentation exists that would help them in any subsequent court case. They also need to look closely at how these popular Internet gathering points impact their employees and potential hires.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. Her latest publications are Say What You Do (Shaser-Vartan) and The Privacy Management Toolkit (Information Shield). She can be reached at rebeccaherold@rebeccaherold.com or http://www.rebeccaherold.com.