Social Networking Policies and Training: Essential Elements in Protecting Your Trade Secrets

Insights
7.15.10

Any business that does not have a social networking policy or does not train its employees on the do's and don'ts of social networking may have a critical security gap in the protection of its trade secrets, and its confidential and proprietary information and may be exposing itself unduly to harassment, hostile work environment, defamation and numerous other legal claims. Chances are that one-quarter to perhaps as much as one-half of your workforce (or more if your workforce is younger) are regular users of social networking websites. And that number is likely to increase.

Social Networking -- the New Security Threat
The term "social networking" refers to the regular communication and publication on the internet of thoughts, ideas, activities, opinions and myriad other content on social networking sites, such as Facebook, MySpace, LinkedIn, Twitter, and YouTube, to name a few.Most of these sites allow their users to post a personal profile which can contain a listing of the user's education and work history, family, social and business relationships, activities and likes and dislikes.LinkedIn is designed with the networking professional in mind and is tailored to business networking; whereas, Facebook, MySpace and Twitter are designed with a broader, more open freewheeling architecture that invites disclosure (and therein lies another part of the problem). These sites allow users to post status updates (in other words, whatever is on their mind) at anytime day or night from any computer with internet access or even from a cell phone, iPhone or Blackberry."Anytime" is a key word here.A recent survey of 1,000 Americans by Retrevo, Inc. revealed that 48% of those polled admitted that they update Facebook or Twitter during the night or as soon as they wake up. In addition, 19% of people under the age of 25 say they update Facebook or Twitter anytime they happen to wake up during the night compared to 11% over the age of 25.Social networking also includes both personal and professional blogs, which now are so simple to use that a blog can be set up in a matter of a few minutes.

Careless employees can be just as damaging and just as dangerous as malicious ones.In social settings, like social networks, people naturally gravitate to discussions about work.The people who tweet about their haircut, the movie they just saw or what they had for dinner are also likely to tweet about coworkers, customers and the work they did that day.Stories abound of inappropriate posts about coworkers and customers.How often are employees observed "texting" below the table at a meeting?One recent mobile Facebook post from a meeting tersely criticized a subordinate's failure to comprehend and concluded that the employee "forgot to take her medication." An employee's

“friends” or followers are also likely to extend well-beyond a small social circle. In addition to former high school and college friends, the list likely includes former colleagues, maybe ones who now work for competitors, or customers or other business relationships. It is not surprising then, according to a recent survey, that over 50% of employers believe they have a right to monitor employee postings on social networking websites.On the other hand, 60% of employees surveyed believe their online activities are none of their employer’s business.The inherent tension on this issue is obvious, but equally obvious is the need for a clear set of rules and expectations, particularly where your employees are regularly exposed or have access to confidential business information.

Social Networking Policies and Employee Training

The first two steps essential to reducing the security risks posed by employees engaged insocial networking are (1) having a detailed social networking policy, and (2) carefully training your employees.It is essential to have a social networking policy that clearly establishes permitted and prohibited conduct at work and expected behavior online, regardless of whether the online conduct is for business or personal purposes.Routine email, computer and confidentiality policies do not adequately address the risks presented.Despite the dramatic increase in the use of social networking websites, in a survey done by the Wall Street Journal only 26% of employees said their employer had a policy regarding social networking.An August 2009 study done of one industry found that 50% of employers reported not having a policy for employees’ online activity outside of work and only 10% reported having “a policy specifically addressing these types of social networking sites.”

Employee training is also essential if you want to meaningfully reduce your risks.For many employees social networking online is a new phenomenon.Many employees are not likely to instinctively appreciate the risks or intuitively understand the full scope of what is necessary to police their behavior in relation to their job.For example a manager “friending” an employee is fraught with problems.The employee may feel he or she has to say “yes” because to say “no” risks insulting the manager.There is a risk that the casual “friendly” atmosphere cultivated by social networking sites may lead to inappropriately personal messages or what may be perceived as inappropriate, which could in turn create a hostile environment or otherwise encourage a harassment claim. It also gives the manager access to information that could provide the basis for a discrimination claim.

By the same token, an employer cannot issue a blanket decree prohibiting employees from using social networking sites on their own time without potentially running afoul of federal and state law.Thus, proper training is imperative to protect the company and, in large part, to protect the employees from themselves.Remember in almost all instances, the only online editor is the employee, who could be posting from the office or from any street corner or from any Starbucks at anytime.Employees who understand the personal and professional risks of inappropriate activity will be much more likely to self-regulate their online behavior in an appropriate fashion.

A topic for another day are the myriad reasons for companies to take full advantage of social networking.Many companies are already actively involved in most facets of online social media.They recognize that social networking presents substantial opportunities for marketing, customer service, protecting brand name, keeping in frequent touch with customers, raising the company's public and community profile and performing competitive research.These opportunities simply underscore the need for a well thought out social networking strategy that incorporates policies and training that allow the company to reduce its risks and reap the rewards.

Related People

David W. Erb
Partner
410.857.1399
Email