bank five nine

Navigating The Social Media Minefield

Social networks are growing in popularity and corporate usefulness, but there’s a fine line between personal and professional networking on the Web, and missteps can be treacherous. As a result, some companies simply ban social sites in the workplace. A wiser approach might be to come up with a strong policy to regulate them. Here are some issues for businesses to consider in terms of monitoring online activities.

A Balance Between Performance And Risk

Social media sites such as Twitter, Facebook, LinkedIn, YouTube, and blogs can be powerful business tools. But they also carry risks, including inadvertently disclosing corporate trade secrets or engaging in behavior that can harm your company’s reputation.

These concerns, combined with obligations to maintain confidentiality and concerns about employee productivity, have prompted some businesses to block or severely limit access to social networks on the job. Other companies, however, are embracing the new technology and urging employees to use it to its fullest.

At the same time, employees need to understand that their employers are increasing their social network presence and that workplace rules of conduct apply online.

If your organization is grappling with this issue, here are some recommendations to help develop a policy that can leverage the power of social networking while limiting the risks:

Assess the benefits and threats. Determine how employee online networking can help or hinder your company's brand, reputation and growth. This will help you decide what activities, language and behaviors you want to allow or prohibit.

Weigh boundaries. Imposing a total lock-out could do more harm than good. It could prompt technically savvy employees to come up with workarounds that could open holes and threaten the security of your computer network. Just as damaging, it could suggest to staff members they aren't trusted, which could damage morale, lower productivity and prompt some employees to post derogatory remarks about your organization.

Consider a compromise. Put reasonable limits on the frequency or duration of social networking during the workday. Some IT departments have installed software that blocks access after certain thresholds have been reached, such as visiting 20 sites in one day or networking for 45 minutes. Also, consider blocking social media sites that contain inappropriate or potentially inflammatory content. There is also software that will search publicly accessible areas of social sites for mentions of your company so that you can monitor what employees or others are saying.

Get legal advice. Staff members may view limiting and monitoring of social networking as a violation of privacy rights, but courts have generally ruled that employees have no expectation of privacy when using workplace computers. Nevertheless, it's a good idea to get legal advice to answer questions such as:

- How does social networking affect corporate policies on confidentiality, trade secrets, proprietary information, product or service introductions, discrimination, harassment and other issues?
- What are the legal implications of imposing controls on social networking while employees are at home and off work?

Have employees agree to the policy in writing. Once your business crafts an actual policy, be sure each employee reads, agrees to and signs off on it. The policy should:

- Explain clearly what is and is not acceptable.
- Inform employees to follow all corporate policies when they are identifiable as being affiliated with your organization.
- Outline the consequences for violations.

When it comes to social networking, the lines between personal and professional activities are often unclear. Should a manager "friend" an employee on Facebook? What about employees becoming online friends with customers? Engaging in online discussions in which they mention your company's name and become aggressive or insulting? These are just some of the questions facing businesses today. Having a policy in place can help your organization balance the benefits of social networking with the risks.

Crossing The Line

When it comes to social networking, unexpected situations come up for employers. For example:

- A police officer resigned after writing on his Facebook page that there should be a law allowing police to arrest people for being "stupid." The man apologized, noting that the comment didn't "reflect the attitude or atmosphere" in the local police department.
- An employee of an airline, who participated in travel-related online forums, violated a passenger's privacy by posting the individual's travel history. The employee said the information was disclosed to show the passenger lied in a previous post.
- In another situation, an employee posted information about a company's internal policies -- specifically a loophole that customers could take advantage of - that the business did not want revealed.

Private Means Private

Generally, courts have found that employers can discipline employees based on online comments made about the company or its staff. However, a recent New Jersey jury verdict suggests that the comments must be publicly accessible.

The jury found against the Houston's Restaurant chain in a case in which managers fired two employees based on comments they found after accessing a private social webpage without proper authorization.

Two New Jersey employees started a private MySpace page where colleagues could sign in with a password and rant about the employer, sometimes using profane language. A manager heard about it and asked an employee for the password. Fearing repercussions, the individual complied. Once managers saw the postings, they fired the employees who set up the page on grounds of violating the company's "core values of professionalism and a positive mental attitude."

The employees sued, charging invasion of privacy and violations of state law and the federal *Stored Communications Act*. That law bans unauthorized access to electronic communications, such as Internet postings, stored by electronic providers, such as social network sites.

The jury found for the employees on both counts, saying Houston's managers entered the MySpace page without authorization and acted maliciously. (*Pietrylo v. Hillstone Restaurant Group,* U.S. District Court 06-5754)

As social networking grows, so do the number of cybercriminals using the sites to spread viruses and engage in phishing attacks. Keep your company's IT team current on emerging threats and how to fight them.