Redmondmag.com
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

**IN-DEPTH**

# Social Networking Compliance: A Guide for IT Teams

*Social media has opened a whole new can of worms for companies, just as they were getting e-mail under control. Despite the challenges, it's possible to get social networking applications under control, too.*

By Paul Korzeniowski • 03/08/2011

The Information Age is in full bloom, and communication is now a 24x7 phenomenon. In companies large and small, individuals spend much of their days answering e-mails, sending co-workers instant messages (IMs), posting blogs and tweeting.

While these developments have helped some companies streamline business processes and increase productivity, they also raise new management issues. Bits of corporate data information are flying around in cyberspace like children darting around an amusement park. In order to be in compliance with various government and industry regulations, companies need to safeguard their data. To do this, IT departments need to track an ever-expanding array of communications options and then block, collect and archive employee exchanges.

So, how well is IT doing this right now? The answer depends on the type of communications vehicles examined. Businesses seem to have a good handle on employees' e-mail usage; however, the level of control available with IM and social media systems is not as well developed.

"Many companies may unknowingly be leaving themselves open to embarrassment and possible lawsuits because they're not properly tracking all of their employee communications," says Ted Ritter, an analyst with The Nemertes Research Group Inc.

## Paying for the Backlash

The issue of compliance became more important at the turn of the millennium when employees started to rely more on e-mail to complete their work. In addition, there was a backlash to how companies reported their financial information. In response, government regulations such as Sarbanes-Oxley emerged to provide more guidance about appropriate and inappropriate business processes. In 2006, the Federal Rules of Civil Procedure established that companies must establish protocols for capturing electronically stored information prior to civil court cases. Violations of such regulations can lead to costly penalties. In 2002, the U.S. Securities and Exchange Commission (SEC) fined five firms a total of $8.25 million for not properly monitoring and capturing their e-mail traffic.

Perhaps fearing potential fines and lawsuits, companies quickly and willingly ponied up the money needed to buy e-mail management and archiving tools.

"Most have put procedures in place so they can monitor their e-mail systems," says Michael Osterman, principal at Osterman Research Inc.

For instance, MobiTV Inc. delivers more than 100 television and video channels from more than 50 content providers -- including NBC, ABC, ESPN Mobile TV, Disney Channel, FOX News, Comedy Central and Bravo -- to mobile subscribers. "We rely on Symantec products to ensure that our e-mail communications are secure and archived," says Chad Kalmes, IT Director at MobiTV. Kalmes says that MobiTV specifically uses Symantec Enterprise Vault and Endpoint Security applications.

Ready for New Challenges?

Now that corporations have management of their e-mail systems under control, new challenges have arisen. "Businesses don't have as good a handle on instant messaging and social networking communications as they do with e-mail," Ritter says.

The results can be damaging. For instance, hedge-fund managers with the Galleon Group were charged with insider trading in 2009. The evidence that cracked the case open? A single text message.

Texting and social media have become quite popular among consumers and have been working their way steadily into businesses. Increasingly, social media communications account for a significant portion of new business opportunities in many organizations.

However, the recent, rapid uptake -- often in violation of companies' written policies -- has left many enterprises inadequately prepared from both a data-leakage and a compliance perspective. In fact, some observers think that companies may have more to fear from accidental data leakage on social media sites than from hackers. The reason is that social networking communications often occur without employees considering the consequences of collaborating in what are, in effect, public places.

A Multimillion-Dollar Joke

In April 2009, two Domino's Pizza employees created a video where they prepared sandwiches for delivery while one employee put cheese up his nose and violated other health-code standards. In a few days, the video had been viewed more than a million times on YouTube and the pizza chain faced a PR nightmare. Quickly, the company fired the two employees, and the local police department brought felony charges against the perpetrators. In addition, the local health department told the company to discard all open containers of food. The prank cost the pizza chain millions of dollars in brand recognition and lost productivity.

In addition to such losses, companies may face fines because regulatory agencies are starting to demand that corporations put checks in place and monitor social networking exchanges. For instance, in January 2010, the Financial Industry Regulatory Authority -- the enforcement arm of the SEC -- issued Regulatory Notice 10-06, which mandated that financial services companies oversee social networking communications in the same manner that they handle e-mail. The Office of Thrift Supervision, a bureau of the U.S. Department of the Treasury that regulates the nation's thrift industry, and the Financial Services Authority, an independent and non-governmental regulatory body for the United Kingdom financial services industry, have issued similar rulings.

As a result, security professionals face a significant challenge. Controlling social networking communications is complex because IT pros need to monitor communications that often occur in a hodgepodge manner and sometimes even outside their systems. Consequently, they're not sure which -- if any -- spots to examine on their enterprise networks. For instance, how does a company monitor Facebook updates that employees do on their cell

phones?

A De Facto Endorsement?

Compounding the challenge is the type of communications typically done on these sites: The sites themselves encourage personal opinions and endorsements. If an employee becomes a fan of a company and notes that on Facebook, does it become a de facto corporate endorsement? Some would say yes. Another example comes from LinkedIn, which provides the ability to send a message to as many as 50 recipients. Would these communications then be classified as sales materials that need to be reviewed by the firm beforehand? Again, some would answer that question in the affirmative.

So, what's a company to do? Around the turn of the century, IT departments were becoming overwhelmed with e-mail traffic. As this electronic medium became popular, a pattern emerged among businesses: Many firms simply blocked all external electronic communications. The same scenario occurred with IM and is now unfolding with social networking applications.

In business since 1948, Graubard Miller is a 40-person law firm that focuses on financial exchanges, real estate and commercial disputes. "We block social-networking connections because we need to be sure that we're in compliance with government regulations," explains Steve Heller, CTO at the firm, which has been using an e-mail archiving service from Proofpoint Inc. to monitor its Microsoft Exchange messages. In other cases, companies discourage such communications because they don't see a fit between their businesses and the social-networking sites. Midwood Financial

Services Inc. has 20 employees and distributes $1.2 billion in financial products and services to 400 U.S. banks, regional brokerage firms and independent broker dealers. "Because we operate mainly in a business-to-business market, social-networking sites, such as Facebook and Twitter, don't have much of an impact on our business," says IT director Tom Przybylak. The financial services company uses AppRiver tools to secure its Microsoft Exchange e-mail communications.

Finding a Way to Skirt Security Checks

But blocking sites like Twitter or Facebook with techniques such as URL filtering may not be effective. Tunneling applications can get around such controls. In fact, Lifehacker.com, The Wall Street Journal and other sites have published items such as the "Top 10 Ways to Bypass Social Networking Security Controls," which outline the process. For example, employees could simply install proxies on their home computers and connect them to the Internet. While at work, they can use the company computer to access the home IP address, circumvent the corporate filter and visit social networking sites.

Another problem is that most valuable employees are often the ones trolling the social networking sites. Rather than discourage such activities, many firms view their use as valuable and productive. Consequently, organizations need to strike a balance. They want employees to use the sites but don't want such access to create new problems. In effect, companies need tools that can scan all traffic, both inbound and outbound, for confidential or restricted content and ensure that the use of social media in the workplace doesn't create a backdoor where confidential and business critical data can leak out. They need to make sure that if employees talk about engineering glitches, they share enough information to solve the problem but don't tell outsiders what the company plans to come out with next year.

A number of vendors are trying to address the issue with software that limits what users can do on social networking sites. For instance, the products may allow users to view Twitter messages but not post them, update a Facebook status but not play games, or post to LinkedIn but not recommend anyone or anything. These products are coming from vendors in a variety of industries, such as Astaro GmbH & Co. KG, an e-mail archiving supplier; Palo Alto Networks, a firewall provider; Dexrex LLC, a mobile text message archiving firm; and ZL Technologies Inc., a supplier of archiving and e-discovery software.

Leaders Start to Emerge

A few products have been gaining some market traction. Actiance incorporated social network compliance features into its software, so it controls Facebook, Linkedin and Twitter communications. Designed to help organizations meet regulatory compliance demands, the controls allow posts to be pre-approved, logged and archived. Its moderator controls allow organizations to examine communications and hold them for evaluation prior to posting. If communications don't meet company policy, the application blocks them.

Cloud services provider Socialware Inc. is also trying to help companies bridge the gap between enterprise and social network functions. With the company's Compass software, customers are able to outline and implement social media policies. IT professionals can manage user access in a granular fashion, and the system will keep an archive of each individual's social-networking activities.

Such features appealed to Cambridge Investment Research Inc., which has 350 employees who provide services to more than 1,800 financial planners nationwide. The organization's New Century Council brings together advisors under the age of 45. Council members asked Cambridge Investment Research to help them develop social media outlets for their services.

"Many of our customers want to use social media sites to market their services," explains Julie Gebert, assistant vice president of compliance for Cambridge Investment Research.

In the fall of 2009, the organization searched for a tool to help monitor those connections and eventually opted for Socialware. One reason was the ability to pre-review information before advisers post it to social networking sites, such as Facebook, Twitter or LinkedIn.

"We're seeing movement toward managing social-networking transactions in industries where protecting confidential information is paramount, such as financial services and health care," Osterman, of Osterman Research, notes. These organizations will vet the new tools so, eventually, they'll become easier to deploy, more functional and maybe even as common as e-mail monitoring tools.

The tools are there to harness social networking. With good policies and the right software, you can control social networking and not be controlled by it.

---

**About the Author**

*Paul Korzeniowski is a freelance writer based in Sudbury, Mass. He has been writing about networking issues for two decades, and his work has appeared in Business 2.0, Entrepreneur, Investors Business Daily, Newsweek and Information Week.*