

Social Media Problems

Those highly popular Web 2.0 technologies that may be transforming business and marketing models are also regulatory, security and risk management minefields.

BY TED KNUTSON AND JEFFREY KUTLER

Facebook and Twitter. LinkedIn and MySpace. Digg and Buzz up. Reddit and any number of Web sites that fall under the category of blogs. Some of these are more trendy or familiar or stodgy than others. Their popularity and populations are fluid. Some help with business or personal organizational tasks; they might exacerbate or help manage information overload, or tend to distract or to disrupt routines. Loyalty and utility alike are pretty much in the eye of the beholder.

Welcome to the wild – and wildly expanding – new world of social networking, with user numbers reaching into hundreds of millions. The business opportunities of “a disruptive technology that has changed the way we communicate,” as consulting firm PricewaterhouseCoopers described it in a report earlier this year, are too enticing to ignore. But then there is the flip side, as PwC’s advisory services group summarized: “Social networking has transformed the way the connected

masses communicate. Now businesses must change the way they secure their networks and data.”

Social media, in short, epitomize business opportunity and risk. They are both a bonanza and a disaster waiting to happen. And they have proliferated so quickly that corporate executives including risk managers, even when grasping the technology’s potential and applying it in ways that supercharge their marketing and bring them closer to their customers, have been hard-pressed to address obvious and nagging concerns ranging from employee productivity to corporate espionage to computer security.

Another PwC study, its joint Global State of Information Security research project with *CIO* magazine, noted that the vulnerability to data loss or cybercrime “gives IT executives heartburn.” Yet in their survey last year of more than 7,000 security and information technology professionals worldwide, only 23% had adopted policies to defend Web 2.0 technologies – the class of highly interactive networked services that include social media – and control what can be posted on the likes of Facebook and Twitter. Thirty-six percent said they

monitored what employees post on external blogs and social network sites.

“It’s no surprise, then, that every IT leader surveyed admitted they fear social-engineering-based attacks,” said the report. “Forty-five percent specifically fear the phishing schemes against Web 2.0 applications,” in which social media subscribers are tricked into opening authentic-looking messages that contain destructive viruses or other malware.

In the two to three years that social networking has come to dominate some forms of interactivity, particularly among people in their 20s and younger, corporate authorities’ initial resistance has turned into acceptance and even enabling, at least up to a point. The progression was not unlike financial institution IT departments’ handling of instant messaging in the early 2000s. At first they simply blocked access from office computers. One fear was vulnerability to malware. Also, IM, unlike e-mail, could not be tracked or archived and therefore could run afoul of certain compliance requirements. But companies could not block the burgeoning popularity of IM and employees’ use of it on home computers and hand-held devices, and as IM-specific compliance and security solutions were developed, the restrictions loosened.

Cultural and Generational Change

Social networking, however, is literally a social phenomenon, and many media and culture experts expect it will be more lasting and transformative than was instant messaging.

There is also the generational element: 25-year-olds grew up in a multi-tasking “mash-up culture” that embraces technology as a set of problem-solving tools, Gillian Hayes, assistant professor of informatics at the University of California, Irvine, said during a panel discussion in March at the information-security-focused RSA Conference in San Francisco.

Older supervisors might consider Facebook updates or tweeting an unproductive use of



Beware of online impersonations of both individuals and businesses, says lawyer Theodore Claypoole.



Wholesale and retail businesses alike face reputational threats, says Ipswitch’s Frank Kenney.



Reveal only the company information found on a business card, says FINRA’s Thomas Pappas.

work time, but the younger workers would contend that being wired and networked in this way not only helps them in the outreach and collaboration aspects of their jobs, but also makes them more productive.

“They are not prepared for the more restrictive sandboxes of the corporate model,” said Hayes, and indeed, empirical studies are beginning to bear that out. Added Kimberly De Vries, assistant professor of English at California State University, Stanislaus, there are indications that “people who access social networks are productive and make better decisions than those who do not.”

The popularity surge is such that a workplace that tries to bar social networking – which is hard to enforce because of easy access to public Web sites with social media links – will be shunned by talented graduates who prefer to work for a more “open” enterprise. Jim Routh, a former chief information security officer at New York-based Depository Trust and Clearing Corp. who was at the RSA Conference as a consultant with Archer Technologies of Overland Park, Kansas, noted that Symantec Corp. liberalized its internal policies when it was persuaded of the benefits of social-network collaboration.

“There are security concerns” that warrant IT experts’ attention, Routh stressed, but brand and reputation concerns are bigger. Privacy invasions and slander are the darker side of the buzz generation and truly targeted, direct marketing that social media make possible.

Publishing Industry Parallel

“Just because you’re not a media company doesn’t mean you won’t face the same kind of legal exposure a media company would face, says Kenneth Goldstein, worldwide media liability manager for the Chubb Group of Insurance Companies. The solution, he says, is to emulate a newsroom operation and be aware of the legal pitfalls in publishing.

The Social Becomes Reputational

By Edward Moed

In the aftermath of 9/11, risk managers played key roles in implementing crisis management plans within their businesses. Those who were late to the game accomplished something similar in response to the financial crisis of the last two years. Risk managers' organizational importance has grown accordingly.

That's all well and good. But, from my standpoint, a very real and frightening gap remains where risk managers and their corporate communications colleagues have yet to strategically understand and plan for the risks associated with social media. The threats are all too real, and they are different from many others in that these networks can be both a crisis starter and prolonger and can, in fact, become the crisis itself.

The phenomenon is not all that new anymore. Although corporations have begun to accept it as a way to communicate or to market goods and services, few have taken the time to think through its massive risk implications or to have done scenario planning for what could so easily manifest. Already we have seen horror stories about companies that had not focused on social media risks and suffered the consequences of being unprepared.

Take, for example, the Kevin Smith incident. Smith, a popular filmmaker, was attempting to fly standby on Southwest Airlines when a flight attendant told him to leave the plane because he is overweight and could not fit comfortably into one seat, as per company policy. (Smith had actually purchased two tickets for himself, but when he tried to change his flight, he was assigned only a single seat.) Smith vented his anger on the Internet, using Twitter to describe the experience. The news went viral, first among the thousands who follow

Scott Testa, a business professor at Cabrini College outside Philadelphia who follows corporate social media issues, says businesses are frequently being sued because of Facebook and MySpace postings and practices. But few of these complaints are publicized and many are settled quietly. In one that did make the news, Web 2.0 search provider Yelp is facing class actions alleging that it demanded that businesses advertise with it to avoid having negative reviews posted prominently.

As a widely publicized dispute between Kevin Smith and Southwest Airlines demonstrates (see sidebar), it doesn't have to escalate into a lawsuit to cause reputational damage. In contrast to spoken defamation, Testa notes, social media slurs travel at the speed of light and can do lasting damage.

Even the new-media brands are not immune. Facebook has faced backlashes over its privacy measures. Outages on Twitter make mainstream-media headlines.

Theodore Claypoole, an attorney with Womble Carlyle Sandridge & Rice in Charlotte, North Carolina, and co-chair of the American Bar Association subcommittee on privacy, security and data management, says impersonation has become a particularly insidious social media hazard.

"I can't tell you how many William Gateses from Redmond, Washington, have popped up on LinkedIn," he says, adding that businesses as well as individuals are impersonated, in an online context taking the form of spoofing as well as phishing.

"Punishment by social media can be swift and vicious," adds Claypoole, recalling the case of a couple who toured the country in a recreational vehicle,

parking overnight in Wal-Mart Stores lots and reporting on their travels online – until word got out that they were being

A menace or a productivity aid?

paid a promotional fee by the retailer. It wasn't illegal, but neither was it positive for Wal-Mart's image. If the perceived offense is bad enough, "people will begin a campaign to boycott your goods," says Claypoole.

He believes that the more regulated a company is, the more vulnerable it is to legal actions for social media abuse, and that consumer businesses are more likely to sustain social media attacks than are business-to-business organizations.

On the other hand, Frank Kenney, global strategy vice president of Ipswitch File Transfer, a division of Lexington, Massachusetts network monitoring software company Ipswitch, says that false rumors can just as easily disrupt a B2B company's supply chain and ultimately its reputation.

Controls and Policies

Kenney is also a believer in the productivity-enhancing side of social networking, as in document sharing and collaboration over distances. Still, controls are necessary even to prevent unintended consequences of employees' talking their own companies up. For example, if a lower level worker tweets something as innocent as "my company is doing great" just ahead of a quarterly earnings report, it could trigger an insider-information investigation by the Securities and Exchange Commission.

The PwC-CIO information security

New-Media Security Measures

At companies in PricewaterhouseCoopers' Global State of Information Security survey

Content filtering to keep data behind firewalls	65%
Ensure use of most secure browser versions	62%
Staff monitor employees' online access	57%
Monitor blog and social network posts	36%
Have policies for social media	23%

report pointed to "the ease with which users could share customer data or sensitive company activities while they're telling you what they're having for lunch." It also quoted H. Frank Cervone, vice chancellor of information services at Purdue University Calumet in Indiana: "People are still incredibly naïve about how much they should share with others, and we have to do a better job educating them about what is and isn't appropriate to share."

Bounds of behavior can be codified. A model social media policy drawn up by Dawn Haag-Hatterer, a human resources executive and head of Frederick, Maryland-based Consulting Authority, underscores, for example, that "employees who access social media Web sites during working hours are required to follow the company's Code of Business Conduct and Ethics, as well as all other company policies" (see page 32).

Also on the market is a Social Media Governance Toolkit, including documents and templates for developing and disseminating usage policies, from U.K.-based online compliance marketplace IT Governance.

Thomas Pappas, vice president and director of advertising regulation at the Financial Industry Regulatory Authority (FINRA), the Washington, D.C.-based securities self-regulator, recommends that businesses ask their employees to limit the amount of company information on a private Facebook or LinkedIn page to what would be shown on a business card.

In January, FINRA published Regulatory Notice 10-06 on Social Media Web Sites. The guidance points out that the SEC requires brokerages to keep records of customer complaints. The issue gets a bit murky on the no-holds-barred frontier of social media. Pappas says broadly speaking, the more specific an allegation of wrongdoing, the more likely it is that a firm will be required to retain it and respond as it would in other channels.

A complaint via Facebook that a broker is stealing money from a client is specific. Saying that a company sucks is not. Claypoole says that when the rage is more virulent than it is legitimate, the best course may be to ignore it. Making a public show of defensiveness might only bring more unwelcome attention.

Smith's tweets and eventually generating headlines in mainstream media outlets.

Within hours, Southwest was facing a customer service disaster. Overweight people were vowing to boycott the airline. Even though the company apologized profusely to Smith and the world, it had a big black eye that wasn't going away for weeks. As good as Southwest typically is in leveraging the technology with its core audiences, it wasn't ready to deal with this crisis, however bizarre, caused by the immediacy of social media. The result was lost business, a tarnished reputation and the need to divert time and resources to deal with the issues.

Companies need to understand and learn from cases like this that they cannot control what is being said about them on the Internet. No one can ever predict what exactly will happen via a Twitter or Facebook account or just some random blog post. But it is possible to be prepared.

As with other crisis management steps, risk managers need to work in tandem with communicators and social media experts to assess what types of vulnerabilities they face and, where feasible, to lower the risk levels involved and/or plan accordingly for the worst case.

As a starting point, internal social media policies need to be tailored to fit the specific needs of the organization. Resources should be allocated to deal with any need to communicate accurate information immediately through the right digital channels. And managers and employees need to go through social media training to be sensitive to how their actions could set off a chain of potentially negative events, and to learn what to look out for in the course of their day-to-day jobs.

Social media is just the latest wake-up call to the risk management function. There is no turning back now. Being prepared is the only logical choice.

Edward Moed is co-founder and managing partner of Peppercom, a New York-based strategic communications firm that specializes in crisis management.

A Model Social Media Policy

The following is a template drafted by Dawn Haag-Hatterer, a human resources executive and CEO of Consulting Authority LLC, www.consultingauthority.com

As part of <Company's> communication standards, we recognize that the use of social media outlets affords <Company> with unique opportunities to generate industry recognition and establish ourselves as industry experts or leaders. Accordingly, we also recognize that many of our employees utilize these same social media outlets for personal reasons unrelated to <Company> business. This policy addresses <Company's> stance on the use of social media outlets in the course of business during regular work hours or while on paid status with the Company.

responsibilities;

- Employees who access social media Web sites during working hours are required to follow the Company's Code of Business Conduct and Ethics, as well as all other Company policies;
- Employees who post Company proprietary or confidential information, or any information, opinion, or commentary about any former, current or future employee or affiliated business partner of the Company on social media Web sites, during work hours or on their own time, will be subject to discipline in accordance with <Company's> disciplinary program;
- Employees should use their best judgment in posting to social media Web sites when required to do so as part of their

Information posted on the Web can be easily taken out of context.

A. SOCIAL MEDIA OWNERSHIP

In order to ensure that the Company's use of social media outlets is leveraged appropriately, <Company> has assigned accountability for corporate use with the Vice President of Marketing. As such, s/he will be accountable for the following:

- Identifying, establishing and communicating the Company's plan on the use of social media;
- Serving as main decision-maker for defining who has access to social media outlets; and
- Ensuring only Company sanctioned or approved content is posted to such outlets.

B. EMPLOYEE USE OF SOCIAL MEDIA

<Company> provides all employees with access to social media outlets during working hours, in accordance with the following guidelines:

- Employees are not permitted to access social media Web sites, including reading or posting to same, during regular working hours unless they are conducting bona fide research or using the outlets as part of their normal Company business

normal duties, as well as during their own time.

- o When in doubt, do not post;
- o Give credit to original authors as necessary;
- o Do not violate the law or the rights of other individuals or companies;
- o Do not denigrate or chastise others in postings; and
- o Remember that information posted on the World Wide Web can be easily disseminated and taken out of context.

C. DISCIPLINARY PROCESS FOR MISUSE OR UN-APPROVED ACCESS

<Company's> disciplinary process governs the misuse or unapproved access to social media websites and posting of inappropriate, illicit and illegal content, up to and including discharge from employment. The Company also reserves the right to pursue civil and criminal charges against employees posting Company confidential or proprietary information, as well as any business harm resulting from an employee's inappropriate, negligent, malicious or otherwise illegal postings to social media outlets relevant to <Company>.