Advisory Services
Security

Security for social networking*

Social networking has transformed the way the connected masses communicate. Now businesses must change the way they secure their networks and data.

*connectedthinking

PricewaterhouseCoopers

Table of contents

In today's socially connected workplace, information flows freely between employees and their online followers. This can pose serious risks to an enterprise's network, data, and reputation.

Social media can enrich employee performance and create a vibrant corporate community. The downsides? A business's network and data could be compromised and its reputation and brand put in serious jeopardy.

Businesses must take extraordinary care to craft an integrated security strategy that balances employee education with sophisticated network monitoring. That requires teamwork between the business and information technology groups.

The heart of the matter

In today’s socially connected workplace, information flows freely between employees and their online followers. This can pose serious risks to an enterprise’s network, data, and reputation.

Today, social networking is as routine as sending an e-mail at home or work. Employees swap updates on Facebook and Twitter, log opinions at blogs, and upload snapshots to photo-sharing sites.

The result for businesses? A digitally connected social world in which the line between personal and corporate lives is increasingly blurred.

As this digital conversation swells, potential risks to businesses also rise. Simply said, not all data being shared is as innocent as weekend plans.

In 2009, for instance, an employee of a Hawaii hospital illegally accessed a patient's electronic medical records, then posted the patient's name and confidential medical details on her MySpace page. This violation of Health Insurance Portability and Accountability Act policy did not deter the employee, who was later sentenced to one year in prison.

It's clear that businesses need a proactive— and powerfully persuasive—communications plan to educate their user community about social media risks, personal and company impacts, and expected behaviors. Companies should support the communications plan with targeted protections to mitigate the risks of social networking, a phenomenon that will only continue to gain force. Social networks including MySpace and Facebook; microblogging services such as Twitter; and blogs, wikis, and photo-and video-sharing services are among the Web's fastest-growing sites. In fact, social networks are more popular than personal e-mail and are visited by 67 percent of the global online population, according to Nielsen Online.[1]

This skyrocketing popularity makes social media a very real threat to network and data security. The risks are not limited to data sharing by employees, however. A treacherous new breed of hackers can use social media to infect a corporate network with malware and viruses, exploit vulnerable networks, steal intellectual property, and harm a company's reputation.

It's not just the hackers businesses must worry about. In addition to leaking sensitive information, individual users of social networks can distort information about a company (or its employees) to create public relations disasters .

Despite the risks, many companies are ill-prepared. To safeguard critical data, mitigate data leakage, and control intellectual property, chief information security officers (CISOs) must adopt a two-pronged strategy that leverages the experience and leadership of the business and technology sides of their companies.

With the proper security, social networking can be a powerful enabler for change. However, businesses will stand to benefit only if policies and technologies work in concert to safeguard data and the network.

[1] Nielsen Online, *Global Faces and Networked Places,* March 2009

An in-depth discussion

Social media can enrich employee performance and create a vibrant corporate community. The downsides? A business's network and data could be compromised, and its reputation and brand could be put in serious jeopardy.

Social networking is a disruptive technology that has changed the way we communicate.

Consumers now broadcast their thoughts and actions to an ever-widening audience of friends, family, and followers. As the user base of social networks increases—Facebook alone has more than 300 million members—the scope of the networks is also expanding. Consumers use social networking to make buying decisions, corporations promote new products and services with tweets, and customer service takes on a life of its own. All of this is going on outside traditional company walls and firewalls.

Beyond Facebook and Twitter, social networking comprises a wide range of Web 2.0 tools. Public social networking media also include blogs, wikis, map-based mashups, and social news sites such as Digg.com. Anyone can access these networks from work, home, or on the road. Users can disseminate any type of information, be it public or private, fact or fiction.

However, only 40 percent of respondents to PricewaterhouseCoopers' 2010 Global State of Information Security Survey reported that their organization has security technologies that support Web 2.0 exchanges. In addition, a little more than one-third (36%) audit and monitor postings to external blogs or social networking sites, and only 23 percent have security policies that address employee access and postings to social networking sites.[2]

Not all social media are public. Businesses are creating proprietary social platforms that include user communities, mashups, blogs, wikis, and internal microblogging sites. These media create a human connection for the workforce that can greatly enhance communications, collaboration, and teamwork. Employees can easily update one another on the status of projects, documents, and other work-related actions; they can customize and contextualize information in ways that boost performance.

Making the most of connected human capital

The benefits of social media are many.

Businesses are embracing social networking to cultivate an internal culture of collaboration. Additionally, it is easy to see how this free flow of information can boost productivity and autonomy. Employees working on a project will have relevant, current, and customized knowledge at their fingertips, and they can tap into a ready-built group of team players at all levels of the organization.

Outside the organization, social networking can help a business reach and engage customers, improve the customer experience, and manage its brand image.

Many businesses today patrol sites such as Twitter and Facebook, for instance, to listen in on the chatter about their products and services. Their online brand ambassadors can promote new products or, if a business's reputation is threatened, use social media to move the discussion in the right direction.

Businesses also take advantage of online customer voices to create a more effective advertising campaign. Successful brands leverage customer experiences as an integral part of a product campaign and life cycle. Consider, for instance, the success of Apple. Apple customers have a tight emotional bond to the brand and track the company and its products on blogs, Twitter feeds, and Facebook. How deep is the connection? Apple retail stores in some cities have now become tourist attractions. Anyone can read about them on Twitter.

[2] PricewaterhouseCoopers, *Global State of Information Security, 2010*, October 2009

Why social media may be hazardous to the corporate network

As the adoption of social networking grows exponentially, CISOs have begun to understand that they must change the way they safeguard their networks and sensitive data.

They are concerned about the risks of social networking, and rightly so.

As we have seen, employees may easily leak critical (and regulated) information via social media. And ambitious cybercriminals can gain access to sensitive data by infecting networks with malicious code that connects to Web 2.0 platforms, such as Facebook and Twitter.

These threats are abetted by the very nature of social media, which is built on flexible Web architecture that enables exploitation and compromise. As cybercriminals know, Web 2.0 platforms are increasingly powerful and open and enable more sharing of rich data. Such an extraordinarily dangerous combination leaves the enterprise vulnerable to hacking, viruses, and malware. It has become alarmingly commonplace for hackers to unleash malicious code on social media sites to attack networks with viruses, spam, phishing expeditions, and Trojan horses. During the first half of 2009, 19 percent of all Internet attacks targeted social networking sites. This represented a dramatic increase over previous years, according to a study by Breach Security Inc.[3]

Cyber attacks are dangerously effective on social media because they often generate seductive messages that appear to come from trusted friends. The subject lines—such as “You look just awesome in this new video”—direct unsuspecting users to sites that employ phishing schemes or malware to obtain sensitive personal information.

Sometimes, however, employees voluntarily disclose critical business information and intellectual property without being manipulated by malware. Recently, an employee of a cell phone handset maker, which was covertly developing a much-anticipated new model, posted revealing details about the phone on his LinkedIn profile page. A blogger discovered the confidential product data in a matter of days, and soon the news spread to blogs and trade press around the world.

In addition to personal and proprietary information considerations, data leakage can violate confidentiality mandates. A recent study published in the Journal of the American Medical Association found that 13 percent of medical school deans surveyed reported student violations of patient confidentiality via social media.

Another threat comes from anything-goes commentary—by employees or the public—that can cause serious reputational damage when opinion becomes negative or untruthful. Thanks to the instant flow of information and opinions, a public relations blip can quickly become disastrous as it ricochets among consumers and customers. These malicious comments can be very difficult to remove or address effectively.

Meanwhile, legal ownership of information on social sites remains uncharted territory. Content created on a social network might become the property of the network; yet if the data is posted using corporate equipment (a personal computer or smart phone), the business might be held legally accountable. In the event of legal disputes and e-discovery, companies might be required to disclose information posted on social networking sites.

[3] Breach Security Inc., *Web Hacking Incidents Database 2009: Bi-Annual Report,* August 2009

How businesses can balance security and social networking

Let's face it: There is no stopping the two-way flow of information. Instead, PricewaterhouseCoopers believes, businesses should embrace social media and adopt a proactive strategy to safeguard corporate networks and data.

The strategy must be two-pronged: It must set forth policies and procedures that govern the use of social networks and corporate information, and it must use technology that helps protect the safety and integrity of data and the corporate network. This multilayered approach requires that the business and technology sides of the company unite and fully commit to the initiative. The two must analyze content and policies in detail, as well as determine the right mix of enterprise technologies available to monitor, classify, and manage data.

The policies and processes for social success

As with any policy implementation, the first step concerning social media is to form a business strategy that includes a long-term adoption plan for policies, procedures, and solutions.

It is essential that the business classify data so that employees understand precisely what is—and is not—sensitive information. This process also should define who is authorized to access and share corporate content, and it should lay out procedures that delineate how employees may use sensitive data. As part of data classification, the business should also establish a data-retention policy for information created on social media.

Data classification is commonplace but far from universal. The 2010 PricewaterhouseCoopers Global State of Information Security Survey found that 22 percent of global firms do not classify data and information assets.

Policy also must delineate the types of social networking accounts that the company sponsors. For instance, the business should take steps so that employees understand the difference between a company-sponsored Twitter or Facebook account and individual company accounts run by a person or team. Everyone must know that company accounts are separate and very different from an employee's personal account.

What's more, the business must clearly specify who is responsible for particular types of communications; these operational roles typically fall within the marketing and customer service departments. The company also should establish management oversight for social media—both a chief strategist and a community manager, for instance.

When developing roles and policies, the business should include a strategy for employee separation to maintain ownership of intellectual property and social identities. For example, if an employee is assigned to monitor Twitter feeds for customer service complaints and opportunities, he must understand that the company owns this online identity and he must relinquish it upon potential termination.

No strategy is complete without a remediation plan. The business should know how it will manage reputational damage and respond to critical online commentary. Social networking can instantly create buzz as well as negative publicity, so the strategy should include methods to evaluate the situation quickly, then act appropriately and swiftly.

Establishing these policies is only the beginning, however. The real work lies in behavioral changes of employees. The business must fully educate and train its workforce on its social networking policies and the risks of social media. This is an ongoing initiative that requires an unwavering commitment.

The business should decide whether employees may access social networking sites from corporate devices (including mobile phones). Increasingly, businesses are blocking the use of social media on the corporate network. PricewaterhouseCoopers believes, however, this is a false security. If a business does not establish policies and platforms for social networking sites, its employees will find them and use them as they like.

Businesses must educate employees on the need to protect intellectual property and sensitive information, and they should fully detail the consequences of noncompliance for both the company and the individual. Policies should state that employee use of social media might violate the corporate code of conduct for privacy, client confidentiality, and intellectual property. Be clear: Jobs are at risk.

The boundaries of proper use of social media can be ambiguous as the line blurs between work and private life. But policy must not be. Staff members must be aware that if they identify themselves as an employee of the business, they are representing the company. Anything they say online about the company becomes part of the public discussion and can have a potentially harmful impact on the business.

Why technology is essential to an effective security strategy

All the policies and processes in the world won't effectively protect an organization without the right technology in place. To that end, the organization must use security solutions that scan traffic for malware, data leakage, and other suspicious activity. And it must actively monitor the environment.

Possible strategies include multilayered security at the gateway and end point, content classification, content filtering, and data loss prevention (DLP). Yet identifying the right combination of these security tools can be a daunting challenge because the Web 2.0 technology is new and evolving.

PricewaterhouseCoopers believes that effective security for social networking must leverage both decentralized and centralized modes of IT security. In other words, the business must protect both the network and the user at the end point.

Start with centralized security, which holds the key to safeguarding the enterprise's data and network resources. As hackers become more aggressive in their attacks on social media, businesses must continue to step up the use of traditional protection tools such as scanning to verify incoming content and traffic. Indeed, many companies have taken the first step and implemented a Web security tool and configured their Internet gateway to block malicious inbound traffic such as cross-site scripting exploits and phishing. Another option is inbound content filtering, which employs spam blockers and anti-virus applications to block or allow a communication based on analysis of its content.

For outgoing traffic, a DLP solution enables the business to screen content before it leaves the corporate network. It monitors outbound traffic to detect and potentially stop the communication of sensitive information by underprotected means. DLP can identify sensitive data at rest, control its usage at user end points, and monitor or block its egress from network perimeters. In practical terms, that means DLP can quarantine an unauthorized or underprotected messaging that contains unencrypted personal information before it leaves the network.

Identity and access management (IAM) solutions are essential to help stop authentication hacking. In this increasingly popular attack vector, a hacker obtains user names and passwords via social networking scams. In fact, nearly one-fifth of security hacks on Web 2.0 and social media sites are achieved by authentication hacking, according to a study by the Secure Enterprise 2.0 Forum. [4] We believe the use of strong IAM controls and multifactor authentication will help organizations mitigate this threat.

At the end point, businesses should lock down users' Web browsers to block JavaScript and plug-in capabilities (assuming that does not impact work applications). This step is critical because many social media sites push much of the application logic to the Web browser. JavaScript and plug-ins deliver much better end-user experiences, but they may also introduce additional vulnerabilities that open the network and data to attack.

Finally, remember that mobile devices including smart phones run robust Web 2.0 apps and are likely to become the next frontier for hackers. Any thorough security policy must protect the integrity of the device and the sensitive data stored on it.

[4] Secure Enterprise 2.0 Forum, *Q1 2009 Web 2.0 Hacking Security Report,* May 2009

What this means for your business

Businesses must take extraordinary care to craft an integrated security strategy that balances employee education with sophisticated network monitoring and data protection practices. That requires teamwork between the business and information technology groups.

Social networking can bring competitive advantages to a business, including real-time sharing of information and analysis, better collaboration, and an enriched relationship with customers. It can also make employees feel valued, connected, and an important part of the community.

Yet the hazards are simply too dangerous to ignore. Network attacks, data leakage and theft, reputational damage, and compliance issues are risks that a business must address before it adopts social networking or allows wholesale access to social media sites through its network.

PricewaterhouseCoopers believes businesses must approach social networking with an equal measure of caution and careful planning for today and tomorrow. The activities, risks, and technologies associated with social networking are emergent and constantly evolving. It is essential, therefore, that the business use a life cycle strategy that can address current needs and quickly adapt to changes in the social networking landscape.

Effective security for social networking requires a two-pronged strategy that fuses education and the behavioral change of employees with implementation of a robust technology ecosystem that constantly monitors for risks. This approach demands experience in behavioral change and deep knowledge of data classification, Web applications, and enterprise security.

We believe this type of undertaking should be done with the help of a team of specialists in social networking and enterprise security. PricewaterhouseCoopers is a recognized, trusted leader in security consulting with global experience in the scope of solutions for data protection, data classification, and compliance. Our team assesses security and privacy risks and helps to implement solutions to mitigate these risks.

Social networking is more about following knowledge than people. We believe, however, that effective security requires that businesses lead—not follow—with knowledge. We can help.

Contacts

To have a deeper conversation on the industry or on any of the topics mentioned, please contact:

Gary Loveland
Principal, National Security Leader
gary.loveland@us.pwc.com

Brad Bauch
Principal, Houston
brad.bauch@us.pwc.com

Rik Boren
Partner, St. Louis
rik.boren@us.pwc.com

Kevin Campbell
Partner, Atlanta
kevin.campbell@us.pwc.com

Thomas J. Carver
Partner, Pittsburgh
thomas.j.carver@us.pwc.com

Michael Compton
Principal, Detroit
michael.d.compton@us.pwc.com

Shawn Connors
Principal, New York
shawn.joseph.connors@us.pwc.com

Scott Evoy
Principal, Boston
scott.evoy@us.pwc.com

Kurt Gilman
Principal, New York
kurt.gilman@us.pwc.com

Joe Greene
Principal, Minneapolis
joe.greene@us.pwc.com

John Hunt
Principal, Washington
john.d.hunt@us.pwc.com

Jerry Lewis
Principal, Dallas
jerry.w.lewis@us.pwc.com

Mark Lobel
Principal, New York
mark.a.lobel@us.pwc.com

Sloane Menkes
Principal, Washington
sloane.menkes@us.pwc.com

Joe Nocera
Principal, Chicago
joseph.nocera@us.pwc.com

Chris O’Hara
Principal, San Jose
christopher.ohara@us.pwc.com

Fred Rica
Principal, New York
frederick.j.rica@us.pwc.com

Sohail Siddiqi
Principal, San Jose
sohail.siddiqi@us.pwc.com

Andy Toner
Principal, New York
andrew.toner@us.pwc.com

pwc.com

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

The information contained in this document is provided “as is,” for general guidance on matters of interest only. PricewaterhouseCoopers is not herein engaged in rendering legal, accounting, tax, or other professional advice and services. Before making any decision or taking any action, you should consult a competent professional adviser.