



KPMG ANALYSIS

Web 2.0 Tools Fostering Collaboration - and Risk

November 15, 2007

By Dave Pelland, Managing Editor, Digital Insider

As interactive, so-called Web 2.0 applications designed for consumer use make inroads into corporate settings, IT departments are racing to guard against data leaks and other information-security exposures.

"Web 2.0" includes interactive tools and Web-delivered applications such as online document creation and collaboration, e-mail, social networking, videos and podcasts. Workers use Web 2.0 applications to produce and share documents, but often do so outside corporate firewalls, which could lead to accidental data disclosure.

For example, a search engine can index information posted to an internal corporate blog and expose it to the public at large, according to John P. Pironti, chief information risk strategist for IT services provider Getronics. Similarly, information posted to an internal Web site may become subject to legal discovery.

"Web 2.0 in many respects is about openness and collaboration, and the fact that the word 'Web' is in there means it's going to be about ubiquitous access," says Toby Weiss, president and CEO of database security provider Application Security. "That means more companies are opening their data to the outside world."

According to an upcoming KPMG survey of corporate executives on Web 2.0, 86 percent of respondents "agreed" or "strongly agreed" that Web 2.0 tools will help their companies share knowledge more efficiently; 75 percent believe it will help to foster innovation.

But 51 percent of respondents felt that security is the chief barrier to Web 2.0 adoption at their organizations. Just 47 percent are creating governance programs to guard data from unauthorized external access.

Interactive Security Holes

Paul Henry, vice president of technology at software provider Secure Computing, says the interactivity that makes Web-based tools convenient opens potential holes for criminals to exploit.

Because Web 2.0 applications such as wikis allow users to contribute or edit content, malware writers have added malicious URLs and software code to legitimate sites that rely on code running within Web browsers.

"Web 2.0 effectively has provided a much better vehicle for the transport of malware on the public Internet," Henry says.

MORE...

[IFRS for Technology Companies: Closing the GAAP?](#)

AUGUST 14 A KPMG white paper examines industry-specific issues for technology companies considering a transition to International Financial Reporting Standards.

[The Consumer Electronics Boom](#)

AUGUST 6 A new KPMG white paper identifies the critical issues inhibiting faster time-to-market for consumer electronics and semiconductor manufacturers.

[Wireless Carriers Put Money in Mobile Banking](#)

JULY 29 Cell phone carriers are targeting mobile banking applications for growth.

[Selected Technology Company Earnings](#)

JULY 25 Slowing economic conditions in the United States affected the results of several technology companies in the second quarter.

[Companies Taking Green-Tinted Look at Data Centers](#)

JULY 18 As corporations become more environmentally aware, they're looking at their data centers and PCs to reduce energy consumption and carbon footprints.

[Social Media: a New Political Animal](#)

JULY 10 Social media is reaching beyond the traditional corps of political pros and playing a major role in the fall elections.

[KPMG's Quarterly New and Emerging Markets Magazine](#)

JULY 2 In this issue, KPMG examines how the wireless revolution is shaping everyday life in emerging markets to its logistic systems.

In a recent example, hackers attacked musician Alicia Keys' MySpace.com page on Nov. 8. The hackers replaced images with links to malware that could capture keystrokes and tried to sell fraudulent antivirus software. Within 24 hours of its discovery, MySpace disabled the Keys attack, one of at least 50 similar attempts to hack music-related pages on the site.

Another potential issue complicating Web 2.0 corporate security efforts is many organizations think workers are only using approved, internal applications.

"Many enterprises feel incorrectly that because they're not hosting Web 2.0 services on their Internet-facing servers, Web 2.0 risks are not a concern to them," Henry says. "They're not considering the fact that their internal users are taking advantage of other organization's services, and bringing risk into the enterprise."

Most organizations assume that if an employee is accessing a benign site, the data from that site is trustworthy.

"Rarely do organizations scan returned content coming from the Internet," Henry says. "That's actually a large hole in most network security implementations."

One way companies are addressing Web 2.0 risks is examining online traffic closely as it travels through their network gateways. According to Henry, some companies are inspecting software code being sent to Web browsers to identify potential threats, such as trying to alter a PC's security settings or to download unauthorized software.

More companies also are using software to examine outgoing Web traffic to ensure sensitive data, such customers' personal information, are not e-mailed or uploaded outside the network.

"Certain materials shouldn't be allowed to leave the trusted [network] segments of the corporation," says Getronics' Pironti. "You may want to, but shouldn't be allowed to unless you have appropriate controls elsewhere."

Adoption Outpacing Policy

According to the KPMG survey, awareness of potential Web 2.0 threats varies widely by industry. Within financial services firms, 60 percent of respondents said they have policies to protect digital content from unauthorized access. For technology companies, that figure was 52 percent, but the percentage was smaller at telecommunications (35 percent), entertainment and media (33 percent) and consumer goods (25 percent) companies.

Within those industries, nearly all respondents who don't have Web 2.0 policies in place today plan to do so within two years.

Employee education is a central component for an effective information risk management policy, Pironti says.

"A lot of people don't understand the implications technology can have for an organization if it's exploited," Pironti says. "People have to understand what's appropriate to communicate and what's not. They have to understand the implications

of what the technology can do, and appreciate the threats and vulnerabilities that are created."

According to Application Security's Weiss, the popularity and potential benefits of Web-based software tools in a corporate setting means that banning them may not be practical. Because many workers aren't waiting for IT permission to use online collaboration tools, companies have to look for ways to secure how data is accessed and stored.

"There's a question about how companies protect their data when they have people coming in and out [of the network]," Weiss says. "If we're going to open our firewalls and do more collaboration, what protections do we need? We need to be sure our applications, and the databases behind those applications, are secure."

To print this article or share it with a colleague, click an option below.

[Print this Article](#)

[E-Mail this Article](#)

PLEASE RATE THIS ANALYSIS

Quality of Analysis

1 2 3 4 5
POOR EXCELLENT

Comments or Questions

e-Mail Address (optional to enable Insiders to reply)

[Submit](#)

© 2008 KPMG LLP, a U.S. limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

[Privacy](#) | [Legal](#)