

News from globeandmail.com

Wednesday, April 18, 2007

Web tools can be business friends or business foes

Cost savings and productivity gains are appealing, but security issues hinder use

TED KRITSONIS

Special to The Globe and Mail

The advent of Web 2.0 business applications has opened the door to new ways of doing business and increased productivity, but experts say the security risks that come with them may be too high.

While domains such as YouTube, Facebook and Wikipedia largely have an entertainment-driven reputation, there is an increasing demand for online business applications that create a more mobile work force.

Google's offerings, which include mapping, word processing and spreadsheet programs, have been good examples of the rising popularity of Web-based applications for generating everything from sales reports to income tax returns using ubiquitous Internet applications.

But nonetheless, there's a reasonable amount of consternation among security experts and analysts who suggest that whether they will truly change the way we work comes down to how comfortable a business is with having its data in third-party hands.

"An internal breach is one of the key problem areas for protecting data," says Warren Shiao, lead analyst with The Strategic Counsel. "With [Web-based] apps, the 'internal' breach can now come from outside. There would be procedures in place to protect against this, but you could still suffer a breach if you were running Web-based apps in-house too."

Mr. Shiao adds that security is a "major, but probably not gigantic, concern [yet]" as it relates to Web-based applications. Without adequate precautions, he says, employees accessing a theoretically secure corporate network at a hotel or a Wi-Fi connection in an airport, for example, could be just as dangerous as doing corporate work through completely public Web-based channels.

Industry insiders agree that a big reason for the relatively lukewarm concern is that cost savings are even more appealing to businesses than the prospective gains in employee productivity to be had. Using Web-based applications could mean saving money that would be paid to companies like Microsoft and Adobe for software licences.

LBS Financial Credit Union, based in Long Beach, Calif. has "strict rules against social networking sites" but uses tailor-made Web-based applications. A good collaboration tool for LBS has been Passageways Portal, an Intranet portal system designed specifically for credit unions and banks.

Kevin Reed, vice-president of information systems for LBS Financial, says: "It's not just that our

employees can form workgroups and share resources. Since [Passageways] is based on a .Net framework, our in-house developers can create our own Web apps and make them available on our Intranet portal."

But naturally, security is a concern. Mr. Reed indicates that the credit union also bans the use of public, Internet-based "Office-type applications" because data would be stored online rather than in an in-house system.

As a customer of Websense, a California-based Web filtering and security software provider, Mr. Reed says LBS Financial has been safe from any breaches thus far. The security protocols and software in place have prevented the accidental transmission of member account information via e-mail on a number of occasions.

"There's a big worry of information flowing in the clear," says Dan Hubbard, vice-president, security research with Websense. "Proprietary information could be flowing freely across the Internet that people can pick up on because you're hosting sensitive data in a non-sensitive location."

People might also overlook the unsanctioned use of these technologies, adds Mr. Hubbard. For instance, a sales rep might find an effective Web-based tool or service that helps with sales tracking, sharing profiles and meeting quotas.

But that could also mean that company data would be sitting in an online account somewhere without the company knowing about it or being able to control it.

However, the widespread use of instant messaging in business is a bit of a Catch-22. While there could be all kinds of security risks, at the end of the day, the possibility of securing a lucrative deal through IM shows how functionality wins out over security.

Security pundits have long suggested that part of the problem that plagues businesses of all sizes is the lack of urgency given to security before a product or service is implemented. The use of Web-based applications would probably not reverse that trend, according to a security expert at McAfee.

"As long as they're thinking of security and exposure issues, they should at least go in the right direction, but the fear is that they would start using these services and then look at security as something to check into afterward," says Dave Marcus, security research and communications manager at McAfee Avert Labs.

Mr. Marcus also says there's little doubt that providers like Google would do a "very good job" of securing data, but that clients might be uneasy about having confidential corporate information stored along with dozens, hundreds or even thousands of other companies on a publicly accessible server.

But for those that are willing to give it a chance, there could be an advantage in centralizing the data in a different location. IT departments would have less data residing on local computers, thereby making security maintenance easier, Mr. Shiau says.

"It becomes a matter of controlling access to the network instead of controlling access to every end user's machine -- as well as to the network," he says.

"But it still all comes down to how comfortable you are with putting something in someone else's hands."