

broadly includes:

- Interactive sites and tools that allow users to generate and modify publicly facing content
- Hosted applications that allow your organization to offload complex business processes
- The increasing “webification” of many applications, providing easy access from anywhere
- Local applications that use HTTP transparently in the background for updates or information sharing
- Web mashups—integrating content from multiple sites and applications onto a single page
- New communication tools that allow users to connect and share data via multiple channels

Enterprises are still exploring the best uses of Web 2.0. Corporate sales and marketing departments have taken the lead, using social applications to enhance customer relationships, attract new audiences, and heighten brand awareness. For example, Ford Motor Company has a Facebook page where enthusiasts and potential buyers trade information on new models. And BMW, which initially marketed short films on its Web site, now has thousands of videos on YouTube.

Then there’s Unilever’s highly successful “Dove Real Beauty” campaign. The company used traditional marketing such as print ads and billboards alongside Web 2.0 methods such as a dedicated, interactive Web site; blogs by experts; and user-generated content in discussion forums. Dell offers a community network that provides forums, idea centers, and blogs and feeds that keep their visitors informed, as well as provides opportunities to learn, participate, and collaborate.

Other departments are taking advantage of Web 2.0 as well. For example, IT departments have created internal wikis and blogs to keep employees up to date with company information and allow for easy communication—which simultaneously reduces volume on e-mail servers.

Enterprises are embracing Web 2.0 as a critical business tool that enables them to share information,

create communities and user networks, and glean referrals that build loyalty by showing expertise and responsiveness to their most important asset: their customers. As organizations continue to explore ways to take advantage of Web 2.0 and its collaborative nature, Enterprise 2.0 will take on new meanings.

THE RISKS

Even though Web 2.0 has many advantages, it still poses significant risks. It breaks down many of the legacy models around which IT security has been built. These traditional approaches include securing the perimeter, reactive threat protection, and reputation analysis.

- **Securing the perimeter**—controlling egress points to the network while identifying who is entering.

The new network perimeter is no longer a building with walls and network cables, and securing it is becoming as difficult as defining it. Users now demand access from anywhere, using laptops, remote kiosks, and PDAs to access corporate information. So if you’re sitting at a coffee shop accessing Webmail, communicating with friends, and updating your blog, are you inside or outside the company network? Further complicating the matter, Employee 2.0’s are likely making contributions to mainstream

Web sites for business and personal reasons. This presents a new security predicament for CIOs, who must distinguish appropriate from inappropriate activities.

- **Reactive threat protection**—such as using AV signatures to identify and block known malware when it enters the corporate network. Although most organizations have established standard protections such as e-mail filters, firewalls and virus signatures, the ingenuity of hackers means that viruses, worms, and malware take on new shapes and infiltrate in new ways—often via the Employee 2.0 risk factors noted above. How these security risks affect the enterprise is a constant worry for CIOs.

- **Reputation analysis**—deciding to allow inbound

Stephan Chenette, manager of Websense Security Labs, says that while security vendors differ on many things, they all agree that compromised legitimate sites currently serve most of the malicious code in circulation.

traffic such as e-mail or outbound Web access based on the past behavior or known reputation of a sender or site. Because many Web pages and sites can no longer be classified as simply good or bad, reputation is becoming less reliable as a sole indicator of threat potential. For example, Google may be trustworthy in and of itself, but users who build their own iGoogle portals with content coming from non-Google sites are beyond the hosting site's control. Yet few companies will ban Google and other similar sites from employee use. It's simply no longer feasible to block content from all sites that have Web 2.0 content.

SHOULD EMPLOYEES BE BANNED FROM WEB 2.0?

Some people believe that Web 2.0 is limited to a few popular social networking sites—so if you block access to Facebook and MySpace, your employees will go back to work, right?

Realistically, it is nearly impossible to attempt to keep Employee 2.0 from encountering Web 2.0. Due to the increasing use of mobile devices, cloud computing, SaaS models and customer portals, Enterprise 2.0 is inevitable.

Plus, by banning all Web 2.0 technologies, your enterprise risks losing a competitive edge. Web 2.0 has the power to sort out best-in-class survivors from laggards, says the industry analyst firm Gartner Group. And according to a survey by the Direct Marketing Association, more than 80 percent of companies use Web 2.0 technologies to generate leads and sales. If you're not getting

those leads, you can be sure your competitors are.

Businesses that ignore or fail to embrace the changes in the new Web 2.0 paradigm do so to their own detriment. The tack to take is to embrace Web 2.0 technologies as a way of empowering employees to be more technologically efficient and encouraging the Employee 2.0 mentality. The trick is to combine Web 2.0 technologies with the appropriate security measures.

EMBRACING A NEW APPROACH: SECURING DATA

The challenge then is to give employees all the functionality and rich experiences of Web 2.0 without opening the door to attacks, viruses, or other threats.

To do this, CIOs must take control of content (data) in the many forms and channels in which it is presented—Web content, messaging content, and data within the enterprise—and provide both inbound and outbound security. Remember, threats go both ways: A company can lose its essential information to hackers or viruses, or to an employee carrying it out on a flash drive.

Effectively controlling content and data in today's Web 2.0 environment calls for a shift away from passwords and filters and toward an all-encompassing Essential Information Protection strategy. Essential Information Protection involves identifying and tagging particularly valuable information and adding a layer of security to it. It's analogous to securing a house with an alarm system, and locking cash and jewelry in a safe. Some essential information is common to all organizations, such as employee Social Security numbers. And each organization in turn has its own unique essential information—for example, shipping coordinates, compliance guidelines, or patient records.

The technology exists to recognize malicious code before it is launched, even while it is being created, and administer protection automatically. Key to this Essential Information Protection strategy is treating any Web site or e-mail as suspicious, no matter what the source. For example, according to Websense research, in the last half of 2007, 51 percent of sites that

In The Time It Takes You To Read This Paper:

- 41,666 videos will be watched on YouTube
 - 8,233 blogs will be created
 - \$365,297 will be lost to cybercrime
 - 6 Web application exploits will be released
 - More than 5,000 machines will join a bot network
-

Websense identified as having malicious code were legitimate—banks, insurance companies, newspapers—as opposed to sites created by hackers. In the first half of 2008, Websense research found more than 75 percent of sites classified as malicious were legitimate sites with good reputations, nearly a 50 percent increase over the prior six months. Websense Security Labs™ uses its ThreatSeeker™ Network to mine and analyze more than 40 million Web sites every hour for malicious content. When combined with Websense Hosted Security, ThreatSeeker technology can also scan and analyze more than 10 million e-mails per hour for unwanted or malicious content.

Policy administration is not new, but technology has evolved to allow granular control of information by these parameters:

- Who can send what information where
- What information is sensitive and must be protected
- How information can be exchanged
- Where information is and where it can be sent.

Control is the crux. By categorizing data, a company can choose the who, what, how, and where. Websense Data Security Suite uses PreciseID™ technology to categorize data—from text, tables, CAD drawings, and much more—with over 99 percent accuracy. This industry-leading “electronic fingerprinting” solution enables users to precisely enforce access policies so that, for example, only the lead engineer may copy

Websense’s software and security solutions help enterprises effectively transition to Enterprise 2.0. The company’s integrated Web, messaging, and data security products help make businesses safer, more productive, and more efficient by securing the most essential business information assets. To find out more, please visit www.websense.com.

product designs and drawings to a USB drive, only the marketing department can view pop-up ads, or only physicians may enter diagnoses.

The right strategy, coupled with a security solution strong enough to support it, allows CIOs to ensure that essential information flows only between legitimate users, in approved methods and paths, and from anywhere in the enterprise.

CONCLUSION

It’s critical that CIOs lead the charge toward Enterprise 2.0 while keeping the organization secure. In light of the evolving and unpredictable nature of the Internet (see some details below), the right investment in security technology can bring organizations increased protections, higher Employee 2.0 productivity, and greater peace of mind. Let’s look at some figures:

- 60 percent of the 100 most popular Web sites either hosted malicious content or contained a masked redirect to lure unsuspecting victims from legitimate sites to malicious ones, according to new research from Websense Security Labs™.
- The top 100 most popular Web sites—many of which are social networking, Web 2.0 and search sites—represent the majority of all Web page views and are the most popular target for attackers.
- More than 45 percent of the 100 most popular Web sites support user-generated content.
- Websense Security Labs found that 29 percent of malicious Web attacks included data-stealing code.

CIOs have it in their power to both secure the enterprise and enable it to take advantage of Web 2.0 connectivity. Banning Web 2.0 technologies or waiting until later to create a strategy are not realistic or forward-looking options. Facing and embracing the possibilities of Web 2.0 and creating a secure Enterprise 2.0 is the best approach.

For more information, please visit www.websense.com.

Websense is a registered trademark of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.