

Protecting Information Assets



As seen in

BusinessWeek

Special Advertising Sections

© Copyright The McGraw-Hill Companies, Inc.

While securing corporate data may be the ultimate goal,
the bigger challenge today may be finding it.

Companies today must safeguard and precisely catalog millions of bits of data every day that, until recently, they rarely even bothered retaining at all. Those crucial, everyday employee, contractor and customer communications are hidden in seemingly innocuous instant messages, voicemails and files beamed among Palm Pilots, BlackBerries or other types of personal digital devices.

Companies must not only keep such data safe from hackers and crooks, but executives must be able to quickly find critical information within that data when an accountant (or a lawyer) demands it. That holds true whether the data is in a spreadsheet e-mailed to a customer, a USB drive belonging to a disgruntled employee or a lost laptop with crucial procurement contract changes.

Experts recommend focusing security efforts on the data that is most crucial for critical business operations. In today's world of mobile devices and mobile workers, that can be harder than it seems.

Take voicemail, for instance. Voicemail messages are especially hard to index and retrieve because there are so many of them and each message is short and often ad-

resses multiple issues. The best speech-to-text technology today can barely translate in real time, which means that people will need to listen to every voicemail message, summarize it, catalog it and then link those text descriptions with the audio file.

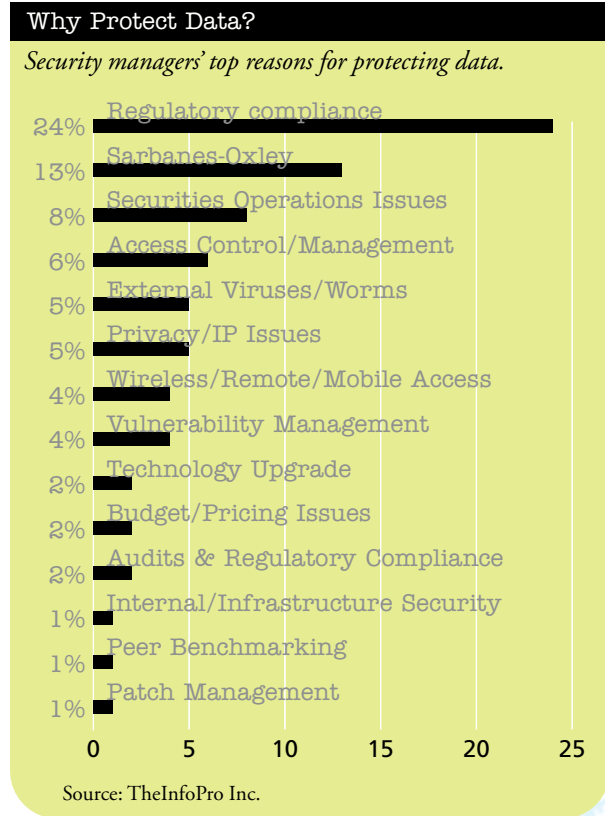
Considering that it's not unusual for a large corporation to literally generate as many as one million voicemails a day, the task is a challenge. Add to that the fact that voicemail messages are often in multiple languages and filled with industry shorthand, and voicemail categorization becomes almost impossible. On the other hand, it's equally critical that companies do track such messages, both to defend against various legal (criminal, civil and regulatory) efforts and to provide advance notice to executives about improper activities such as insider trading, harassment or theft.

Data, Data Everywhere

Traveling, telecommuting, part-time or contract workers roam the country or the world with sensitive corporate information on their laptops. They read and store sensitive e-mail on handheld BlackBerries and download files

onto inexpensive “thumb” drives that can store up to a gigabyte of information on a key chain.

E-mail is, in some ways, as great a threat as small USB drives when it comes to stealing or sending sensitive



information to people who should not have it, says Paulus Sachar, chief security officer at independent software supplier SAP AG in Walldorf, Germany. Although some U.S. companies use e-mail filtering and blocking to prevent such unauthorized data transmissions, companies elsewhere in the world are not because of a growing trend by governments to preserve users' privacy while using e-mail. “The trend toward more privacy worldwide makes it harder for security professionals to protect company data,” Sachar says.

Even within the corporate network, e-mail poses a huge security challenge because of the rate at which it is growing and the critical nature of files sent as e-mail attachments.

Telephone conversations, voicemail and instant messaging chats also can be used to send sensitive information and may be subject to “discovery” as evidence in regulatory or legal proceedings.

When a handheld device is misplaced, the security officer remotely “stuns” (temporarily disables) or “wipes” (permanently deletes) all device data.

What’s more, keeping data secure is harder these days because companies share confidential information (such as prices, designs and production schedules) with suppliers, customers and shippers. When network and infrastructure services provider VeriSign Inc. joins another company to bid on a project, “We might put a lot of proprietary information into this document, such as the strength of our infrastructure, the scale of our infrastructure, the kinds of software we use,” says Ken Silva, chief security officer at the Mountain View, Calif., company. “At the conclusion of the bid, we want to make sure both parties destroy each other’s proprietary information,” lest that information be used against VeriSign in a future bid—or to breach its systems.

Secret IDs & Passwords

At Chase-Pitkin Home Centers in Rochester, N.Y., CIO and Controller Chris Dorsey is happy that new data-sharing technology lets any employee with a Web browser access critical corporate reports. But he worries about what happens “if some people began to learn other people’s user IDs and passwords.” And with more employees using handhelds to take orders in the field, “the discussion quickly became, ‘What if they lose the device?’” with all that customer data on it, Dorsey says.

“Full or partial copies of key corporate data may be anywhere—on PCs, laptops, PDAs, removable storage media, (network) file shares, backup media, insecure paper and media disposal systems,” says Daniel Blum, senior vice president and group research director at Burton Group, an IT research and advisory firm in Salt Lake City.

This underscores the fact that executives today must look at security issues differently. The “perimeter” model of security, in which company insiders can access information and outsiders cannot, “is not adequate anymore for securing company confidential data,” SAP’s Sachar says.

A wave of high-profile corporate scandals—complete with jail sentences—has made C-level executives and corporate boards eager to show they’re keeping corporate financial information clean. Even though the Sarbanes-Oxley Act and its strict record-keeping requirements apply only to public companies, privately held firms are also scrambling to comply to reassure nervous customers and business partners. That’s why regulatory compliance overall, and with Sarbanes-Oxley specifically, were the top two priorities for 2005 cited by security managers in a study conducted by

TheInfoPro Inc., a New York-based research firm.

"The whole world of corporate governance has exploded," says Peter Mojica, vice president of product management and strategies at AXS-One Inc., a vendor of records compliance management software in Rutherford, N.J. New regulations require many companies (not just traditionally regulated financial services firms) to keep more information longer and to be able to quickly find all references to a specific company or transaction. This is in addition to earlier regulations governing, for example, how long certain types of companies must keep records and when those records may be destroyed.

If a company's regulators don't force it to do all this work, its lawyers might. "Any company in the world can get sued," Mojica says, "and e-mail is the new 'discoverable' item during litigation." Telephone conversations and voice-mail might be next to come under the microscope, adds AXS-One Chief Marketing Officer Richard Dym.

To avoid getting overwhelmed with these challenges, it's important for businesses to classify information assets according to business value. Properly judging the business value of different types of data and IT infrastructure is a tough challenge for many companies, says Vince Rossi, senior vice president of product management and product marketing at McAfee Inc., a Santa Clara, Calif., security vendor. The result: Time-consuming and expensive work such as installing security patches isn't always done on the most important systems first.

Security Tools

Not all the technology needed to protect data is expensive or complicated. Authentication (verifying that someone is who he or she claims to be) can be as simple as enabling the password capability built into every notebook, PDA and Pocket PC, or as elaborate as two-factor authentication requiring the user to key in a number from an electronic token. Many word processing and

document management programs allow content creators to control who can receive a specific file or to set a date beyond which the file cannot be opened.

Tokens are rapidly becoming more popular because "they provide strong authentication," says Arthur Coviello Jr., president and CEO of security vendor RSA Security Inc. in Bedford, Mass. "Many people now believe passwords are not enough."

Victor Wheatman, managing vice president at IT research firm Gartner Inc. in Stamford, Conn., says some token vendors are replacing electronic code-generating tokens with less expensive printed cards on which the user must match numbers to log into the system.

Encrypting data so it can be read only by a person with the proper decryption key is a powerful tool, especially for protecting data on a lost mobile device. But

Resources

SAP AG

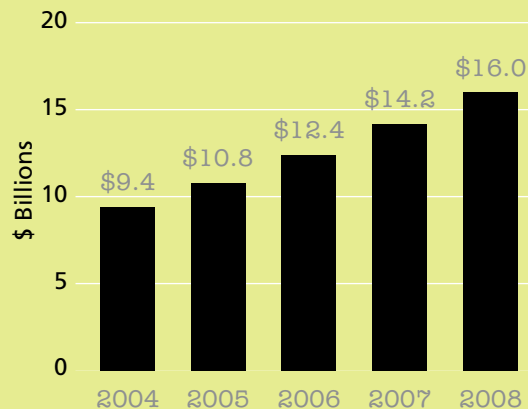
<http://www.sap.com>

VeriSign Inc.

<http://www.verisign.com>

Big Bucks to Protect Big Bytes

Worldwide sales of intrusion detection, spam controls and other secure content-management products.



Source: International Data Corp.

encryption is only as good as the system in place to manage the encryption/decryption keys and the electronic certificates needed to get a decryption key. "There's nothing worse than a disgruntled employee sitting down, encrypting all their data and walking out the door," VeriSign's Silva says, leaving no way to decrypt that data.

In cases where an employee misplaces a handheld device containing company information, he remotely "stuns" (temporarily disables) or "wipes" (permanently deletes) all information on that device. "We have to assume that device will wind up in the wrong hands," Silva says. After all, "The capital loss of a PDA or a cell phone or a laptop is nothing compared to the intellectual property loss." ■

For more information on Special Advertising Section opportunities, please contact Stacy Sass McAnulty at 212-512-6296 or stacy_sass-mcanulty@businessweek.com. Please visit www.businessweek.com/adsections

Triangle Publishing
Services Co. Inc.

The Best Strategic Content for Web, Print, Multimedia and Beyond

www.triangle-publishing.com ■ 617-244-0698

Special Advertising Section Writer: Robert L. Scheier
Designer: Carlson Webster Avery Advertising and Design