



PREVENT DATA BREACHES  
Vital Steps For Protecting Your Business (P.28)

DO YOU HAVE ENOUGH CAPACITY?  
Top Enterprise Storage Considerations (P.14)

SYNC TOOLS For Mobile Professionals (P.44)

TECHNOLOGY FOR BUSINESS

November 2010 Vol. 8 Iss. 11 | pctoday.com

# ACCELERATE

## YOUR BUSINESS

Oracle Accelerate  
Brings Enterprise Tools  
To Mid-Sized Companies

A photograph of a modern, curved glass building facade with the word 'ORACLE' in large, silver, 3D block letters mounted on it. The sky is blue with light clouds.

ORACLE

\$4.99 U.S. \$6.99 Canada



Complimentary  
Copy

# Avoid Data Breaches

What You Need To Know To Protect Your Business

by Rod Scher

According to the ITRC (Identity Theft Resource Center; [www.ittheftcenter.org](http://www.ittheftcenter.org)), a nonprofit organization with “understanding and preventing identity theft” as its primary mission, there were roughly 341 reported data breaches during the first half of 2010, with almost 9 million records known to be compromised.

These are conservative numbers, because with many breaches, there’s no way to determine how many records are involved. Also, data breaches are seriously underreported because most organizations that lose data would prefer not to have that loss publicized. And, as LifeLock CEO Todd Davis notes, state laws about reporting such breaches are less than rigorous: “According to most state data breach notification laws,” says Davis, “they don’t

rest—are also becoming a significant source of data loss. These sorts of leaks rarely trigger identity theft or other sorts of fraud, but they do often result in the compromise of confidential business information.

But it’s not just email and social networking tools that you have to worry about. A recent ITRC report makes it clear that most remaining data breaches—ones that do sometimes result in identity theft—are the result of one of three things: First, laptops or hard drives containing sensitive data are stolen from vehicles. Second, media (drives and optical discs) are simply lost, “misplaced,” or mysteriously disappear from an office, warehouse, or storage site. And finally, there’s plain stupidity. There’s no other way to explain how a hospital in New York managed to send out 1,250 bills to the wrong patients. Or why a financial services company sent out emails to 330 people that included the SSNs of all 330 people in every single email. Or why a large bank sent out over 600,000 tax documents to customers with the customer’s Social Security number printed on the outside of every single envelope.

In a business environment, leaks often result from disgruntled (or acquisitive) employees. “Employees take customer records, lead lists, source code, and other intellectual property from an employer when they change jobs,” says Ron Penna, chief strategy officer and cofounder of Awareness Technologies. “They usually do this by emailing the records from a Webmail service, copying the files to USB [flash drive], or posting them to a Web site.”

“Employees take customer records, lead lists, source code, and other intellectual property from an employer when they change jobs,” says Awareness Technologies co-founder Ron Penna.



have to notify [anyone] if it’s encrypted data and if it doesn’t look like a targeted attack—that is, if it was just a lost or stolen laptop.”

## Sources Of Data Breaches

A large number of breaches are due to email “leaks.” It’s incredibly easy for company emails to be copied, lost, sent to the wrong people, or through other means end up in the wrong hands. And while email remains the primary source of such leaks, social networking tools—blogs, message boards, Twitter, Facebook, YouTube, and the

## Mitigating Risks

Much of business centers on mitigating risk, and dealing with potential data breaches is no exception. If you know the typical causes, there is much you can do to help your company avoid a data breach.

**Pay attention to the basics.** LifeLock CEO Todd Davis encourages companies to disallow the use of P2P (peer to peer) file-downloading services. “As you’re setting up computers, you have to have enough standards and controls to disallow P2P,” he



It's so basic it shouldn't need mentioning, but unsecured Wi-Fi networks are still common, even in business environments. Activate the appropriate wireless security protocol to protect your data.

says. "Then, take the basic precautions: Utilize encryption and firewalls. Finally, you can take the incremental step of having a service like LifeLock—someone out there who will be monitoring both for your or any of your employee data being compromised somewhere else."

**The basics matter.** In 2007, TJ Maxx—the operator of various retail store chains, most located in malls—was breached, and hackers got away with millions of credit card numbers. In the end, the parent company spent over \$8 billion in fines, legal fees, and settlement costs. The cause? "They didn't even have a WEP key," says Davis. "Hackers would drive by the malls and just hop right on to their wireless network, which was sending unencrypted retail transactions back to the corporate headquarters."

**Just say no to data storage.** One way to avoid losing sensitive information is simply to not have any on hand. "To the extent possible, SMBs should do everything they can not to store or process sensitive data," says John Viega, executive vice president of products and engineering at Perimeter E-Security. "For example, if you're doing electronic commerce, you can outsource all card processing to a third party, including storing credit cards for later visits."

**Hide in the cloud.** Another tactic is to hide your data in the cloud. Yes, cloud-based apps are themselves often cited as potential security risks, and for good reason. But if much of your customer and employee data resides on external servers and can be accessed only via Web-based apps that communicate securely with those servers, then the data is not as likely to be stolen by an employee, because it's not sitting in a freely accessible directory waiting to be copied over to a thumb drive.

**Failbook.** Watch out for social networking among your employees. Multiple (and often mutually

exclusive) networks sometimes collide, with information intended for one group accidentally being delivered to all groups. Employees should not be using social networks at work unless it's actually for work.

**Additional tools.** We've already mentioned firewalls, but consider other tools and procedures aimed at minimizing the risk of fraud and identity theft: Intrusion detection and prevention software guards your network, generating alerts when it encounters abnormal behavior. Don't neglect training—there are courses designed to explain security issues to your employees. User access auditing software alerts administrators if suspicious user authentication activity occurs. Use Web content filtering tools to restrict employee access to inappropriate (e.g., potentially dangerous) Web sites. Utilize content- and spam-filtering software to clean up incoming emails. Consider remote data backup services to reduce the risk of media

being lost or stolen. Finally, use policy compliance software to scan individual servers and workstations for the status and configurations of specific policies.

**"To the extent possible, SMBs should do everything they can not to store or process sensitive data," says John Viega, executive vice president of products and engineering at Perimeter E-Security.**

### After The Breach: Dealing With The Aftermath

It's important to do everything you can to avoid a serious data breach. Why? Because, frankly, there's not much you can do afterward. "Unless the actions of the person who committed the breach are being recorded as they happen, reconstructing the event and fully understanding it are impossible," says Ron Penna.

All you can do is report the breach—if required—and take steps to mitigate any potential damages. "It's important to not risk any unnecessary exposure by failing to follow regulatory guidelines. And it's important to get legal advice and follow it exactly," says Viega.

You might consider taking a cue from McAfee: In 2005, when a Deloitte auditor lost a disc containing McAfee employee personal data, McAfee paid for two years of a credit watch service for all affected employees. ▲



Use a business-class firewall to protect your network by blocking spyware, DoS (denial of service) attacks, and other threats.