



Sad State Of Data Security

Businesses and government agencies seem inept when it comes to protecting personal information, as the list of mishaps keeps getting longer.

By Tony Kontzer, Larry Greenemeier, [InformationWeek](#)

Jan. 2, 2006

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=175800226>

How does this keep happening? Companies have been publicly humiliated, slapped with audits, and threatened with prosecution, but sensitive personal data continues to be compromised. The U.S. Department of Justice is the latest to demonstrate its information-security incompetence. The mistake: exposing Social Security numbers on its Web site.

It's the IT problem that just won't go away. From the time early last year that ChoicePoint Inc. admitted it had been duped into revealing personal data to identity thieves, dozens of other businesses, government agencies, and schools have followed with their own admissions of ineptitude. In most cases, victims can't do much more than keep a watchful eye on their financial statements and credit reports--and hope for the best. Not surprisingly, fraud is on the rise and consumer confidence on the decline.

The Justice Department's blunder came to light when *InformationWeek* investigated the concerns of Nick Staff, a systems security manager at a large bank, who had grown frustrated when Justice failed to remove several Social Security numbers from its Web site, www.usdoj.gov, after Staff contacted the agency directly. In one case, the Social Security number of a woman involved in a 2003 immigration-review case was included in documentation about the case. Additional site searches yielded other peoples' numbers in a half-dozen other places.

It's not clear whether the Justice Department broke any laws or regulations in exposing Social Security numbers. It's bound by the Privacy Act, which sets terms for how federal agencies use and disclose personal information, and by its own privacy policies. The Privacy Act, however, is frustratingly fuzzy and comes with a dozen exceptions.

A spokesman for the Justice Department's Executive Office for Immigration Review acknowledged last week that Social Security numbers shouldn't be available to the public and said the information would be removed from the site. He added that, in the 2003 immigration-review case, the affected person would be notified about what had happened.

But cleaning up is harder than it sounds. A subsequent search of www.usdoj.gov showed that the PDF

document on the 2003 immigration case had been blocked from public view, but Google and Yahoo searches provided a link to a text version of the blocked PDF, and the Social Security number continued to be visible. The spokesman said his office still was looking into how to have the documents removed from Google's and Yahoo's search caches. The department was unable to provide further information last week, as many employees were out of the office during the holiday week.

Staff came across the Social Security numbers while looking for FBI comments on phishing and notified the Justice Department by E-mail on Nov. 12 that the numbers were displayed on its site. He followed up via E-mail three weeks later and was notified on Dec. 6 by the site's Webmaster that his E-mail had been forwarded to a "responsible component" within the department. Staff contacted *InformationWeek* almost two weeks later, on Dec. 19, when he saw that the name and number were still on the site. "I would not have gone public with this had the DOJ acted accordingly," he says.

Dark December

The Justice Department's screwup is just one in a string of year-end data fiascos. Earlier in December, Sam's Club, a division of Wal-Mart Stores Inc., revealed that at least 600 customers who bought gas at its stores between Sept. 21 and Oct. 2 had their credit-card data stolen by hackers. On Dec. 16, ABN Amro Mortgage Group, a subsidiary of LaSalle Bank Corp., reported that a backup tape containing data on 2 million people had been missing for a month; it subsequently was found Dec. 19. Ford Motor Co. informed 70,000 current and former white-collar employees that a computer with personal data, including Social Security numbers, had been stolen from a company facility, according to The Associated Press. A few days after that, confidential information on Florida Gov. Jeb Bush and several other high-ranking state officials was made public because of inadequate safeguards on a new state personnel system.

But that wasn't the end of it. On Dec. 28, Marriott Corp. revealed that a backup tape recently recalled from an off-site storage facility was missing, potentially exposing the Social Security, credit-card, and bank-account numbers of 206,000 employees, time-share owners, and rental customers of its Marriott Vacation Club International time-share unit. The company says it sent letters to affected customers and employees, offering free credit-monitoring services for a year. Marriott's public statement echoes what other companies have said in similar situations: It's conducting an internal investigation, working with state and federal law enforcement, and "re-evaluating our process to make sure we're taking any additional steps to have it not happen again."

That doesn't satisfy Vic Christensen, a Marriott time-share owner since 2002 who also happens to be a software engineer with a background in data security. "You would expect someone of their caliber to do a better job of protecting customers' information," he says. Christensen says he'll have a hard time believing anything the company says from this point forward--especially if he gets a letter saying he wasn't affected and thus doesn't qualify for free credit monitoring. The incident, he says, "will make me raise my eyebrows forever" when it comes to correspondence from Marriott.

The risks posed by the nonstop stream of data losses and exposures are worrisome. In a recent survey by Deloitte & Touche, Harris Interactive, and Privacy & American Business, 20% of respondents said they had fallen victim to identity theft or fraud, suggesting a total of 44 million victims nationally. The Federal Trade Commission puts the number at 10 million, but even that conservative estimate translates into damages of \$5 billion for individuals and \$48 billion for businesses.

What To Do

Security professionals must reorient themselves if they're going to slow or stop this growing problem. "I think of data loss as the whole reason the profession exists," says Pete Lindstrom, research director at Spire Security. "We get caught up in lots of flotsam and jetsam janitorial activity with worms and viruses. But it's the data that really matters."

IT professionals are giving the problem increased attention. Data security and protection is the top IT spending priority for 2006, according to a survey of 1,700 readers of *Network Computing*, a sister publication of *InformationWeek*. Perhaps the threat of new laws and penalties has convinced their companies finally to act.

California started the legislative trend in 2003 when it enacted a consumer-notification law that has forced many of the public corporate confessions of data loss and theft. Since then, 21 other states have put similar laws on the books, and another 17 are considering legislation. Some dozen states now allow consumers to freeze or place fraud alerts on their credit reports so their identities aren't stolen after a breach.

Congress has been trying to write a federal law to override the different state rules, though efforts have stalled. At one point earlier this year, 30 different identity-theft bills were circulating on Capitol Hill. Some of the bills lack teeth, requiring consumer notification only when a breach is thought to present a "significant risk" of identity theft and if a "third party" has seen the data. Other bills require notification when there is "reasonable risk" of identity theft.

A bill introduced last summer by Sens. Patrick Leahy, D-Vt., and Arlen Specter, R-Pa., would require companies that store information on more than 10,000 people to formally train employees in security practices, perform vulnerability tests, and ensure adequate security is practiced by third-party service providers. A similar plan backed by Sens. Charles Schumer, D-N.Y., and Bill Nelson, D-Fla., would create an Office of Identity Theft within the Federal Trade Commission, funded to the tune of \$60 million a year for five years.

All Too Common

As the Justice Department situation highlights, the government has its own problems with data security. Two reports by the Government Accountability Office in the last 14 months have found that agencies aren't doing enough to reduce the public display of information like Social Security numbers in public records. A November 2004 report found that 63% of court records and 59% of the records of recording officials made Social Security numbers available to the public. A second report said that Social Security numbers were available in public records in 75% of U.S. counties and 41 states and the District of Columbia.

IT managers shouldn't need laws to force them to protect the personal data of customers and employees. But it's a difficult job. Data can be compromised in many ways: absent-minded posting of data on Web sites, lax controls in handling backup tapes, failure to encrypt, deployment of new systems before security is adequately tested, and the hacker practice of "skimming" data from magnetic strips when credit cards are slid through readers, a technique thought to be used in the Sam's Club incident.

A breach can have long-term consequences for a company, beyond damage to its reputation. BJ's Wholesale Club and DSW Inc., both of which were facing FTC charges for failing to adequately protect consumer data, agreed to implement comprehensive information-security programs and subject themselves to security audits every other year for the next 20 years.

At ABN Amro, the scare caused by its misplaced tape convinced it to replace backup tapes with electronic data transfers across a secure network when it needs to move data to credit-reporting agencies. Health insurer Empire Blue Cross says it has stopped using Social Security numbers as health-care plan ID numbers and has shipped cards with new numbers to all of its members.

Other businesses better take their own steps before they become the next data-security headline. Security 101 is to write a formal security policy and take a data inventory to determine what's most at risk. Firewall traffic must be monitored for suspicious activity, and managers should get very familiar with all the ways data can leave company networks and systems. It also can't hurt to establish access controls, ensuring that only those who truly need sensitive customer data can get at it.

And then there's the most obvious technical solution: data encryption, making it nearly impossible for the bad guys to use any data that's stolen or lost. Yet 99% of companies still don't encrypt backup data, says Greg Shipley, chief technology officer at Neohapsis, a security consulting and IT product-testing company. The reasons IT execs give for shying away from encryption range from cost and complexity to performance and efficiency issues.

Encryption of backup tapes is "one of the few areas in information security where both the industry and the vendors are woefully behind," Shipley says. The ideal approach is to deploy tape drives that have encryption built into the hardware, which would help protect the data on tapes, even if they fall into the wrong hands. Several vendors, including Cybernetics, Quantum, and Sun Microsystems, plan to introduce such products this year.

Software-based encryption can also go a long way to protect data. Vendors like Decru, Kasten Chase Applied Research, and NeoScale Systems sell products that let companies encrypt data en route to tape devices. Businesses also can encrypt subsets of data at the operating system level before specific files are backed up, but this approach is often hard to deploy in transaction-oriented database environments that haven't been designed for it.

The most important policy companies can put in place is one that protects data at rest, as well as data that's transported over networks or on tapes. "The fact that companies haven't factored this in as a potential threat is scary," Shipley says. "As a community, we've got a lot of work to do in 2006."

That may just be the understatement of the new year.

-- with Elena Malykhina and J. Nicholas Hoover

Security Checklist

Set A Data-Protection Policy

Too many companies still don't have one

Inventory Data

What do you have? What's most at risk?

Use Encryption

It protects data that might fall into the wrong hands

Avoid "Bagel Defense"

A hard exterior isn't enough if your network interior is soft

Think Outside The Box

Policies should extend to laptops and cell phones

Invest

Good security requires more than a single system upgrade

Aim High

Consult standards such as ISO, the British Standards Institution, or the credit industry's Payment Card Industry Data Security Standard



Copyright © 2005 [CMP Media LLC](#)