

Ubiquitous Technology, Bad Practices Drive Up Data Theft

By Jonathan Krim

Call 2005 the year of the data breach.

One day, tapes with the Social Security numbers of 1.2 million federal workers are reported missing. Another day it's hackers gaining access to private information on 120,000 alumni at Boston College. Then, last Friday, comes word that 40 million credit card numbers fell prey to computer criminals.

Collectively, nearly 50 million accounts have been exposed to the possibility of identity fraud since the beginning of the year, a significant increase from last year.

Security experts, law enforcement officials and privacy advocates agree that while computer crime is on the rise, it is hardly new.

So why the apparent escalation?

In part, organizations are telling their customers or employees about incidents more than they used to, many complying with a California notification law that is being considered as the basis of possible federal legislation.

After data broker ChoicePoint Inc. reported in February that it was infiltrated by identity thieves posing as legitimate customers, the company received a second black eye when reports surfaced that it did not notify consumers about a previous breach, before California's law took effect. Now, most organizations are choosing to notify potential victims.

Experts see other factors contributing to the data-theft siege.

A boom in data collection has created a marketplace of valuable information stored on computers in thousands of places, many with weak security.

"The current fiascos in cyber-security have been occurring for the past 10 years," said Tom Kellermann, who recently left his position as senior data risk management specialist for the World Bank.

Kellermann and others blame poorly designed software, inattention to data security and an underappreciation of the problem by top management in corporations and other institutions.

"We've used weak practices for some time," said Chuck Wade, an Internet security and commerce consultant. "The vulnerabilities are well known, and we have not been improving the security measures . . . as we should have been."

At the same time, some hackers who used to get their kicks merely being disruptive are pooling efforts with organized criminals, said Jonathan J. Rusch, a special counsel in the fraud section of the Justice Department.

"The motivation now is money," Rusch said. In addition to using stolen data for credit card or other financial fraud, a thriving black market for the stolen data itself exists online, run in large part from Eastern Europe.

Among the most extreme examples of data for sale are offerings known in the online underground as "fulls." These reports include not only Social Security and credit card numbers, but also account passwords for Web sites that a consumer might use, such as eBay or a bank.

"There's so much information that has been leaked out over the years, it may be that there are, outside of the country, criminal elements with huge databases on American consumers," Wade said.

With more and more people getting high-speed Internet connections, and participating in online commerce and banking, the targets of opportunity for criminals only grow.

Wade and others argue that many industry players have not responded aggressively enough because they are insulated from the financial consequences of breaches.

Banks and credit card companies, for example, pay nothing when a criminal uses someone's credit card for a fraudulent charge. The same is true for credit card processing companies such as CardSystems Solutions Inc., which announced last week that it housed the 40 million credit

card numbers that hackers may have obtained.

Payment processors and banks collect fees for charges that are reversed.

"They are making money on fraudulent transactions," said Brian Mortensen, head of a New Jersey company that sells telecommunications equipment. "They should not be allowed to do that."

Mortensen said that as a result of fraudulent purchases, his firm has lost \$12,000 to \$15,000 on equipment that will never be recovered and owes several thousand dollars more in various fees.

Although consumers generally don't have to pay for fraudulent charges on their credit cards, if their identity has been compromised it can take years and thousands of dollars to restore good credit.

Some security experts say many financial companies have been slow to adopt multiple layers of customer verification, such as requiring a password and a second identification number. Many companies also are not encrypting stored data.

But many firms argue that while data protection is a top priority, such measures could make online commerce too inconvenient for consumers without adding appreciably to security. And security already is a large business expense.

Companies must monitor their computer networks and "patch" vulnerabilities in software that are discovered regularly.

That can be especially complex when firms merge and one company's system needs to be incorporated into another's, said David Thomas, head of the FBI's computer intrusion section.

"It's very, very difficult to stay on top of it," Thomas said.

Moreover, said Mark Rasch, a former federal prosecutor who works for an Internet security firm, "The company has to try to protect against every kind of attack. The intruder only needs to find one."

Some breaches, such as mortgage data from General Motors Acceptance Corp. that was stored on a laptop stolen from a car, leave consumers wondering how seriously companies take information security.

Sen. Dianne Feinstein (D-CA), one of several on Capitol Hill sponsoring identity theft legislation, said the CardSystems incident last week "is a clear sign that industry's efforts to self-regulate when it comes to protecting consumers' sensitive personal data are failing."

Thomas F. Holt Jr., an attorney who represents companies involved in breach cases, said he expects things to change when large class-action suits begin to get filed against firms for improperly protecting information.

"When that game is afoot . . . companies will begin to redouble their security efforts and reexamine a lot of assumptions they have regarding the gathering and storing of sensitive data," Holt said.