Making financial data more secure
13 Jan 2006
Dalia Fahmy

As cybercriminals become ever more crafty, institutions seek new safety solutions.

A few years ago during an inspection to evaluate how safely data was being kept at a large financial institution in Charlotte, North Carolina, a group of risk consultants found that more than a third of employees with access to sensitive information had chosen "password" as their password. The consultants alerted the firm's managers.

Two years later the consultants returned. Financial executives proudly showed off how security had been tightened since the previous visit. As instructed, most employees had personalized their passwords. Unfortunately, a quarter of those employees had posted the new password on their monitors.

Such carelessness might have been dismissed with a chuckle not long ago, but with confidential information at financial institutions increasingly under attack, it has become a chilling illustration of just how ineffective bank data system security can be.

TowerGroup, a Needham, Massachusettsbased consulting firm, estimates that online security attacks on U.S. businesses have doubled every year since 1997. Banks rarely report specific financial data breaches, but TowerGroup believes that worldwide the number of breaches is soaring. Successful "phishing" incidents, in which crooks send e-mails directing recipients to Web sites purportedly representing vendors to elicit such sensitive information as account passwords, have increased by an average of 30 percent a month since July 2004, according to the Anti-Phishing Working Group, an industry monitor whose members include Visa, MasterCard, EBay and Microsoft Corp. In January 2005 alone, 12,800 phishing e-mails were reported and tracked by the group. TowerGroup expects the number of such incidents to jump to more than 86,000 in 2006.

"We've gone from criminals hacking for fun to hacking for profit," says Paul Kurtz, executive director of the Cyber Security Industry Alliance, an Arlington, Virginiabased trade group. "Organized crime has recognized the opportunity and is getting very serious about it."

Criminals typically go after three types of data: retail customers' personal financial information, which is the most desirable because it can be used for identity theft; information about institutional customers, such as bank account numbers, which can be used to make unauthorized fund transfers or to falsify records; and confidential information about a bank's business activities, such as trading data, investing strategies, deal information and business models -- anything that might give an adversary a competitive advantage or lead to market front-running. In 2000, for example, an investment associate at Salomon Smith Barney and his friend, a vice president at Bank of Tokyo Mitsubishi, were found guilty and fined $1 million for trading on insider information about more than a dozen mergers. The Salomon banker had obtained the information from documents found in copiers, printers and confidential computer files.

The surge in data theft is compelling financial institutions to step up their data protection efforts. According to Forrester Research, a Cambridge, Massachusettsbased technology and market research firm, U.S. financial institutions already spend almost $9 billion a year on data security. U.S. money center banks alone spend more than $100 million a year each, estimates Brian McGinley, senior vice president and group executive director of loss management at Wachovia Corp.

What information should a financial institution protect? Simple, says Jennifer Bayuk, managing director of information security at Bear Stearns & Co.: "If there's something you don't want to see on the front page of the *Wall Street Journal*, it's got to be protected."

Protection can be difficult and costly because crooks are becoming increasingly creative. High-tech thievery methods range from phishing to hacking to disabling a bank's computer system with viruses and worms. Low-tech methods like bribery also work. This spring New Jersey police uncovered a ring that allegedly paid off employees at Bank of America Corp., Commerce Bank, PNC Bank and Wachovia to obtain the records of as many as 500,000 customers. The ringleader is said to have made at least $2 million on the scheme, paying bank employees $10 a pop for customer records, which he resold for up to $100 each. BofA and Wachovia now face class-action lawsuits.

"It is very apparent to us that customer information has become a criminal commodity, and its value on the open market has increased at an unprecedented scale," says Wachovia's McGinley.

To keep outsiders from entering private networks, institutions are installing a range of technologies, including firewalls, intrusion detection software and antivirus shields. At Depository Trust & Clearing Corp., James Routh, chief information security officer, says many layers of protection are in place, including firewalls and switch configurations that determine who can connect with what device. "We have a number of controls that allow people to access information depending on their role or responsibility. These privileges are validated on a periodic basis."

Henssler Financial Group, a Kennesaw, Georgiabased wealth advisory firm with $1 billion in assets, has been using Lumigent's Audit DB software for three years to track access to and modification of information on databases and to provide an electronic trail to unauthorized users. But Tim O'Pry, the group's chief technology officer, won't comment on the protective software he uses, saying that each one has vulnerabilities. "If people knew the one we use," he says, "they'd know what exploits to try."

One technology now going mainstream is "two-factor authentication." It requires two proofs of identity -- typically a password or mother's maiden name and a credit card or an identity token. The latter is a digitally encoded smart card or a small hardware device such as a key fob that requires a personal identification number; the devices generate a new system-access code every few minutes, permitting entry after an electronic "handshake" with a companion reader device. In October the Federal Financial Institutions Examination Council prohibited banks from permitting single-form authentication for online transactions after year-end 2006, describing it as "inadequate for high-risk transactions."

Experts say banks will have to start providing customers with biometric tools to identify fingerprints or with identity tokens, a prospect that makes vendors of smart cards and other devices, including companies such as Vasco Data Security and RSA Security, giddy with anticipation. "A growing number of banks are providing tokens to institutional customers who authorize large transactions electronically," says Melissa Bisciotti, director of financial accounts at Vasco Data Security in Oakbrook Terrace, Illinois. The devices cost between $8 and $59 per user, depending on how widely they are used.

Financial firms also are encrypting more of their data. Formerly confined largely to data transmitted over fiber-optic communication lines that can be tapped fairly easily, encryption is now being employed on data stored on magnetic tapes, servers or hard drives -- so-called "data at rest." But not everyone is convinced this makes sense.

"If you have a lot of encrypted data at rest, then you have a lot of decryption utilities all over the place," argues Bear Stearns' Bayuk, explaining that once hackers gain access to unauthorized material, they will find a way to read it. "Access control is more important."

At the very least, however, encryption adds a layer of protection against embarrassment. Last year BofA lost tapes during shipment that contained account information on 1.2 million federal employees, including U.S. senators, that wasn't encrypted.

Experts predict that eventually most data will be encrypted. Until then financial institutions are proceeding a step at a time, figuring out which buckets of data must be secured first. One priority is e-mail, which for the most part is not secured. Technologists argue that e-mail is vulnerable because a message typically passes through several servers en route to its destination.

"E-mail is increasingly recognized as a significant risk," says Eric Guerrino, head of information security at Bank of New York. "It's like sending confidential data on a postcard."

Guerrino expects that as encryption technologies mature and reach a level where they no longer slow applications, banks will increasingly encrypt e-mails. BoNY says it encrypts e-mails to a small group of clients and business counterparts and plans to expand the effort. Tumbleweed Communications Corp., a large encryption provider whose clients include BofA, J.P. Morgan Chase & Co. and Wells Fargo & Co., says that about half of the top financial institutions now encrypt at least some e-mails to retail customers.

Other improvements in data security will come from such low-tech practices as shredding important documents and magnetically erasing computer disks. James Mazarakis, chief technology officer at T. Rowe Price Group, adds, "We're trying to reduce the number of tapes transferred to third parties pretty much to nil, so that everything can be sent through secure communication lines."

Because the biggest wild card in securing bank data remains human error and human corruption, banks are devoting more effort to employee screening and awareness training and to tightening internal controls. In the past two years, BoNY has started masking columns of data that employees don't need to see. Sensitive tasks are split among workers, so that when an account address is changed, for example, one employee enters the data and another verifies it. Other institutions, including Wachovia, monitor employees' activities to make sure they aren't gaining access to certain files more often than they should be.

"Institutions are working with detective controls that look for unusual use of information or unusual behavior patterns where people are requesting information in volumes that aren't typical," says Wachovia's McGinley.

Though financial institutions are "in much better shape than other entities because they've been scrutinized longer," they must not be complacent, because the cost of complacency has risen sharply, says Kevin Kalinich, a financial services risk consultant at Aon Corp., a Chicago-based risk management and insurance brokerage company. In the past if a customer's records or identity were lost or stolen, a bank's coverage cost was often less than a few thousand dollars. It was therefore cheaper to cover the cost of fraud than to try to prevent it, says Oliver Ireland, an attorney with the law firm of Morrison & Foerster in Washington, D.C., and a former Federal Reserve counsel.

Those days are over. Two years ago California legislators enacted a law that requires companies to notify customers when their information has been compromised; it has turned incidents that once passed unnoticed into headline news. Since then more than 20 states have signed similar laws, and others are considering doing so. Growing public concern over security has spawned costly class-action litigation; even if BofA and Wachovia win the data-theft suit brought against them in New Jersey, the associated legal fees alone will cost millions of dollars.

Government is concerned as well. Data security at financial institutions was addressed in the Gramm-Leach-Bliley Financial Modernization Act of 1999, which required banks to establish and implement written policies to address the administrative, technical and physical protection of customer data. Although the Sarbanes-Oxley Act doesn't directly touch on information security, it requires bank management to vouch for the integrity of its data. To attest to data integrity, financial executives say, they must be able to prove that their data has not been tampered with. Add to these rules the guidelines issued by the Federal Financial Institutions Examination Council and enforced by members, including the Federal Reserve, Federal Deposit Insurance Corp. and Office of the Comptroller of the Currency, and it's easy to see why financial institutions are complaining about overregulation.

"As companies we could all benefit from more clarification on what's expected and who's governing," says Mazarakis of T. Rowe Price. "There is some confusion on some of the rules and on who is the highest arbiter of a particular legislation."

Financial institutions clamoring for a national data security standard may soon have one. More than 20 bills are currently under discussion in various Senate and House committees; the one most likely to succeed is the Personal Data Privacy and Security Act of 2005, proposed by Senator Arlen Specter. It calls for the adoption of a national standard for "reasonable security practices," procedures for verifying credentials of third parties seeking to obtain sensitive personal information and rules on how to dispose of confidential documents. Experts say it will probably be combined with some of the other bills and passed early next year.

New legislation, however, won't eliminate the gnawing sense that anything can happen at any time to imperil sensitive financial data. Financial executives concede that even if they invest in the best technology and do everything the government and customers demand of them, the confidential records they protect can never be made completely safe; technological glitches, innocent human error and the fecundity of the criminal mind assure that.

Says BoNY's Guerrino: "Even the government can't secure our country 100 percent. But that doesn't mean you shouldn't take protective measures."