

Effective IDENTITY- THEFT Protection

BY DAN SCHEUBLE

IF INFORMATION IS THE LIFEBLOOD OF AMERICAN BUSINESS, OUR COMPANIES ARE at risk of bleeding to death. The news broadcasters have been bringing us the stories all year long: lost or misplaced data tapes, network security breaches, laptop theft. Sensitive financial

Firewalls and encryption technology are tools lenders should consider using to protect the identities of their customers from cyber-crimes.

data relating to more than 2 million individual consumers were stolen last year alone. ■ According to Forrester Research Inc., Cambridge, Massachusetts, the majority of identity-theft fraud is bank-related—56 percent in 2003. Gartner Group, Stamford, Connecticut, reports that identity theft cost credit-card issuers and banks \$1.2 billion in direct losses last year. ■ And it's getting worse. According to Privacy Rights Clearinghouse (PRC), San Diego, more than 50 million Americans have had their personal data files put at risk by security breaches since Feb. 15, 2005 (including an estimated 40 million at a single company; most breaches number in the tens of thousands of consumers at risk). ■ Consumers and legislators want this problem solved quickly, and they're willing to pass almost any law designed to stop it.

Unfortunately, laws by themselves don't stop criminals; adequate security and rigid enforcement usually do. But that's exactly what needs reinforcement in some areas of the financial services industry to prevent a flurry of new state and federal legislation.

A serious industry threat

Banks and other financial institutions are already highly regulated. The cost of compliance runs into millions of dollars annually, even for mid-tier firms. Additional layers of legislation, while not likely to curb the problem of identity theft, will add to the expenses incurred by these firms.

There are already many laws on the books intended to protect the privacy of consumer information—the Fair Credit Reporting Act, the Truth in Lending Act and the Privacy Act of 1974, and more recently, the Fair and Accurate Credit Transactions Act of 2003 (FACTA)—just to name a few. But lawmakers seem intent on passing more legislation in an attempt to further safeguard the privacy rights of their constituents.

Currently, Congress is considering several new bills that could drastically change the way bankers do business. According to The Congressional Record, The Personal Data Privacy and Security Act of 2005 (S. 1332), the Social Security Number Privacy and Identity Theft Prevention Act (H.R. 1745) and The Notification of Risk to Personal Data Act (H.R. 1069) are all under debate at this time, as well as about a dozen others and countless state proposals.

S. 1332 would require businesses collecting personally identifiable information to develop and publish a data privacy and security program. It would prohibit the display and purchase of Social Security numbers (SSNs) without prior voluntary consent, and limit their use in commercial transactions.

H.R. 1745 would consider refusal to do business without receipt of an SSN an unfair or deceptive act or practice.

H.R. 1069 has many ramifications: It would require financial institutions where a breach of personal information is reasonably believed to have occurred to notify affected customers, consumer reporting agencies, the information clearinghouse established by the Federal Trade Commission (FTC) under this act, and law enforcement agencies. Entities maintaining personal information on behalf of financial institutions would be required to notify the financial institution in case of security breach. Consumer-reporting agencies would have to place a fraud alert on individuals affected by a security breach.

State attorneys general would be authorized to bring civil actions in federal district court to enforce this act on behalf of the residents of a state. The FTC would establish and maintain a clearinghouse to collect and analyze information required under this act.

Should any of this new legislation be enacted, it will mean higher compliance costs, slower and more complicated transactions, and more chances that a bank will fail to comply with the law and face fines or lawsuits. But these are not the only risks bankers face if they cannot find a (non-leg-

The average electronic consumer transaction is actually safer than the use of checks or even credit cards.

isolated) way to stem the potential for sensitive data to escape their institutions.

Risk to a firm's reputation is extremely high today. Banks work for years and spend millions to build a brand, only to see it critically damaged by one national news story describing a potential security breach—to say nothing of the cases where computer tapes full of consumer information suddenly disappear.

As more stories emerge of sensitive information falling into the wrong hands, we expect to see legislators make encryption their first targeted solution.

We also expect to see legislation requiring the masking of all Social Security numbers, so Fidelity National Financial Inc., Jacksonville, Florida, has begun to make that change in all of our systems.

Some argue that without such laws, consumers will lose confidence in the Internet as a tool through which to conduct business. If that happens, banks will lose their lowest-cost channel, and their operating expenses will increase significantly.

Even more damaging could be legislation limiting how the Internet is used to transfer information, which could undo years of work promoting the convenience and, yes—security—of electronic transactions.

The average electronic consumer transaction is actually safer than the use of checks or even credit cards. Handing a credit card to an unknown server in a restaurant, who then disappears with it for several minutes, is far less secure than paying a bill online. While fear of identity theft may cause a loss of consumer confidence in the Internet, we must really focus on preventing institutional attacks that result in the risk of theft of large numbers of consumer identities.

How banks can fight identity theft

Information exists in two primary forms within the financial institution. It is either data at rest, residing on a server or some other storage medium; or it is data in transit, being moved by some means between points. With the rise in wireless networks, data in transit can be almost anywhere, from an Internet node to a BlackBerry® or wireless phone, or anywhere in between. However, most large-scale data transmission still occurs over relatively secure private networks between large institutions.

To protect all the data in the enterprise, a layered security plan must be formulated, funded and implemented across the entire company. This plan will identify the required information technology (IT) infrastructure, standardize data-related processes and provide a method for auditing performance. Such plans can be expensive.

This is an expense that banks will either incur now, when they have a choice as to how they protect their customers'

information, or later when it becomes mandated by law. If the industry takes appropriate action now and demonstrates that adequate data security is possible, some of the legislation now under consideration might never be enacted.

At Fidelity, we counsel our bank customers to layer their defenses. Fidelity adheres to a “security defense in depth” schema to layer security across the enterprise. It involves a number of tactics, depending upon the specifics of the network holding the data. For instance, data on an “untrusted” network (one with exposure external to the data center) will always use 128-bit (or greater) encryption, while accessing internal servers via the Internet always requires secure remote access through two-factor authentication.

This layered strategy addresses security from all perspectives—network, application host and data—and provides some form of protection for the information everywhere it might be stored, and on every network it might pass through.

It starts with high-availability/multilayer industrial-strength firewalls. These tools help protect data as they move from point to point, and deny all access unless specif-

ically allowed. All ports are closed except for those that are specifically required for the business.

Even when networks have firewall protection, intrusion-detection systems (IDSes) are an important part of the security plan. This includes network- and server-based systems. IDS identifies suspected malicious network traffic, such as viruses and other malicious software (malware) that may be attempting to access sensitive information or enable back doors to be opened on servers for later use.

E-mail filtering is used to identify and block “phishing” frauds. Phishing involves sending an e-mail to a user that falsely claims to be a legitimate business in an attempt to get the user to provide private information that will then be used for identity theft. Users are directed to special fake Web pages where personal identity information is requested.

Allowing access to trusted networks from outside the institution is an important part of doing business today, but it can be a source of data-security risk if mishandled. Unlike banking customers, bank employees have access to a wide range of sensitive information every time they log into the network.

For outside access to a network, two-factor authentication is a viable approach. That means an employee must have something (usually a universal serial bus-based [USB-based] key or random-number generator) and know something (password). Without both, the network remains locked and the data secure.

But just as important as the technologies banks employ to protect their data is the information they provide to their employees. We recommend holding quarterly events specifically designed to maintain up-to-date information on industry security issues and hot buttons. An internal committee on security awareness should disseminate information to all employees on a regular basis.

For IT developers, the need to be security-conscious is paramount. Application development checklists ensure that good programming habits are followed and weaknesses that hackers typically exploit are not present in new software. The process programmers use to develop new code that meets security standards must be used for every new project to ensure that applications are as robust as possible.

Encryption is the key

Defense in depth alone is not sufficient to protect all of the data in the banking enterprise. If the data are not routinely encrypted, the information will not be totally safe. Unfortunately, this can be an expensive process, which is why fewer than 10 percent of banks use this important data-security safeguard.

There are currently few robust encryption solutions available in the market, especially for data stored at the host level. But banks must consider this their last line of defense, and it should be seriously considered. While it benefits companies that want to protect their data at rest, encryption is even more important for data in transit.

As long as the industry relies on computer tapes to transfer large volumes of data, the risk will exist that this information will not reach its intended destination. Encrypting these tapes is a necessary precaution.

Current and Proposed Privacy Legislation

THERE ARE A HOST OF CURRENT LAWS AND REQUIREMENTS protecting consumer privacy. They include the following:

- Privacy Act of 1974
- Freedom of Information Act
- Gramm-Leach-Bliley Act
- USA PATRIOT Act
- “Do-not-call” provision of the Federal Trade Commission’s (FTC’s) Telemarketing Sales Rule
- Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- Various state laws

In addition to the laws and rules already on the books, some newly proposed legislation is being considered by the U.S. Congress. These bills include:

- *The Personal Data Privacy and Security Act of 2005 (S. 1332)*: A comprehensive personal information protection bill designed to set a single national standard for protecting data both online and offline.
- *The Social Security Number Privacy and Identity Theft Prevention Act (H.R. 1745)*: A bill to regulate the use of Social Security numbers (SSNs) by government agencies and private companies by prohibiting the sale or display of SSNs.
- *The Notification of Risk to Personal Data Act (H.R. 1069)*: Modeled after California’s database security law, this bill would define as personal data an individual’s Social Security number, driver’s license number, state identification number, bank account numbers and credit card numbers.

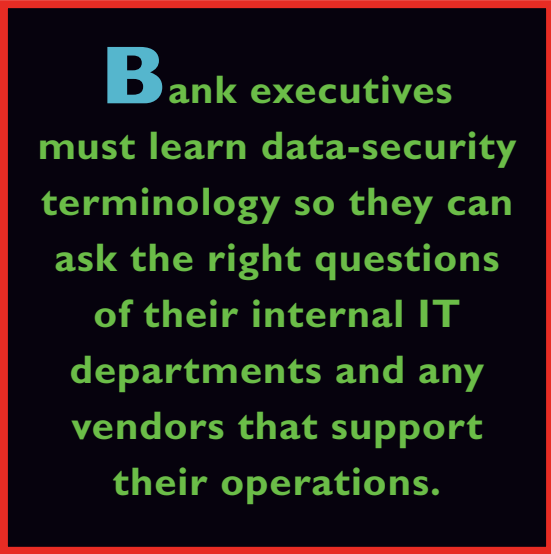
Key management is one way to make certain that only the intended receiver can actually decipher the information stored on the tape. Similar to password protection, software on the receiving system reads the key encoded with the data and can then decode them. Without the key on the receiving end, the data are meaningless.

This key-based encryption is also important when data are transmitted electronically. While difficult, it is not impossible for criminals to intercept data streams over unprotected networks. Unless these data are encrypted, the sensitive information in the transmitted files is at risk.

The tools required to protect data involve additional costs, beyond what companies are already paying for their IT infrastructures. It takes additional resources, including hardware, software and human resources, to operate a robust data-encryption program. Despite this, bankers must consider encrypting their data if they hope to avoid more stringent federal and state regulation in the future.

Asking the right questions

Bank executives must learn data-security terminology so



Bank executives must learn data-security terminology so they can ask the right questions of their internal IT departments and any vendors that support their operations.

they can ask the right questions of their internal IT departments and any vendors that support their operations. Finding out exactly how your company's consumer information is protected is a vital first step in formulating a plan that will protect your organization's consumers and its reputation. Knowing your vendors' capabilities is a clue to how well they can safeguard your data.

Dedicated teams made up of senior-level people must be focused on the problem of data security. A company's data are among its most valuable possessions, and should be guarded with all the diligence an organi-

zation can muster to make sure they are safe at all times.

Not only do our institutions deserve the best possible information security systems, but their customers are counting on them to make the investments that are required to protect their most valuable possession—their identity. **MB**

Dan Scheuble is chief information officer for Fidelity National Financial (FNF) in Jacksonville, Florida. More information about the FNF family of companies can be found at www.fnf.com and www.fidelityinfoservices.com.
