

Bank Director Magazine - 3rd Quarter 2006

## It Pays to be Paranoid

Charles Keenan

*Banks are investing in sophisticated technology to protect customer data from theft while oftentimes ignoring more mundane details like leaving the back door unlocked.*

It is a scenario that has the makings of a nightmare for bank executives everywhere.

Personnel at a bank branch leave a back door unlocked so that smokers can easily slip in and out during the day for a cigarette break. The door is inadvertently left open after hours, allowing an intruder to make his way into the building at night.

His first stop: human resources. There, on a desk, sits a lamination machine. Normally, the password-protected device would prevent him from using it, but someone has foolishly attached the necessary code on a Post-It note. However, instead of using his own mug, the intruder cuts out a head shot of George W. Bush from a picture tacked to the wall and uses the mug to complete his employee identification. The next day, he poses as a new technology staffer hired by corporate and starts prowling around the building looking for trouble. After two days, employees still fail to notice his counterfeit badge, which has a photo of the president of the United States.

Fortunately, the intruder in question was actually a consultant hired by the bank to test the strength of its overall security. The incident—which exposed several potential breaches—was a wake-up call, putting the bank on notice that its data was far more vulnerable to theft than originally thought.

“Many times banks will build a fortress around their data, but they forget to lock the doors or train the guards,” says Roger Peters, executive managing director of the technology risk management services group at RSM McGladrey, an accounting and consulting firm based in Bloomington, Minnesota. “There are so many ways to compromise the security system of a bank, [which has] a lot of potential weak spots.”

### Cyber-security creates high stakes

Banks these days are grappling with how to best protect their [customer] data from thieves employing a variety of high tech - and not so high tech - means. In an age where hackers can steal identities right off the Internet, or where inside employees rifling through loan documents can walk away with sensitive information, banks face one of the most challenging and daunting tasks in data protection. The challenge is not only to make sure a bank has the right technology to do so, but also to ensure the physical controls are in place to avoid major breaches. For the nation's banking industry, the stakes in this ongoing game of data security are incredibly high.

“The biggest stake we have is our reputation,” says D. Scott Huggins, chief risk officer for Pennsylvania Commerce Bancorp., a \$1.8 billion institution headquartered in Harrisburg, Pennsylvania. “If a bank has a major security breach, that is the kiss of death. It just destroys credibility and reputation. We do not want to find ourselves in the position [of having to] defend ourselves because our data was stolen.”

Banks often receive big reminders that they had better be making sure they are doing everything they can to protect their data. The Veteran's Administration announced in May that up to 26.5 million names were stolen from the home of an analyst. Included in the data were social security numbers and dates of birth. Banks have had their own share of gaffes. In June 2005, important information from [as many as] 40 million Visa and MasterCard accounts was reported exposed by CardSystems Solutions Inc., a thirdparty processor in Tucson. In separate incidents last year, computer tapes containing information on both Bank of America Corp. and Citigroup customers were lost by couriers while in transit.

These disturbing mishaps occur despite increases in security spending. While overall security spending is difficult to track because each bank accounts for it differently, increases in information technology security expenditures suggest banks are shelling out more each year to manage the problem. Banks globally are expected to spend \$7.3 billion this year on IT security, up 5.5% over 2005, according to TowerGroup, a consulting firm based in Needham, Massachusetts. That number is expected to climb to \$9 billion by 2010.

The threat of having vital customer data either lost or stolen has led many banks to adopt more of a companywide approach to address security problems. And not all the solutions involve highly sophisticated and expensive technology. “Because of all these risks and the complexity, we are watching financial institutions take an end-to-end enterprise approach to data,” says Cheryl Charles, a senior director at BITS, a financial services industry consortium made up of 100 of the largest financial institutions in the United States. “You are going to see people taking a far more comprehensive, systemic approach to data management.”

That includes moves by many banks over the years to appoint chief risk officers. They are also changing the reporting structure for many information security officers. Before, these officers often reported to the bank's chief technology officer. Now, many banks place

them underneath chief risk officers or chief executives. "Information security is not a technology issue," says Eric Holmquist, vice president, director of operational risk, and information security officer for Advanta Bank Corp., an issuer of business credit cards with \$4 billion in managed receivables headquartered in Spring House, Pennsylvania. "That is one of the worst mistakes you can possibly make."

## **Mitigating the risk**

Holmquist says information security officers should be directly plugged into the business level of the company, reporting to a person who has a connection to the different disciplines across the bank. That helps spread the message. "At the end of the day, it comes down to awareness and accountability," he says. "The more people who are aware, the more they have the opportunity to say, 'Oh, wait a minute, this is a potential risk.' IT, audit, and risk management people can't be everywhere. You need everybody thinking in terms of 'What can I do to mitigate risk?'"

Peters at RSM McGladrey strives to convince banks that data security is really a business issue. He is often hired by bank executives to test a bank's data security, and he has plenty of tricks up his sleeve. (It was an associate of Peters who walked around for two days at one client's facility with the identification badge showing President Bush's picture.) One exercise includes having someone on his staff walk up to a bank entrance, hands full, with the intention of getting in a locked door of the bank with the help of an unsuspecting worker. Other sneaky ideas include posing as a cleaning person at night in order to install key logging devices that fit into the USB port on the backs of PCs. "It only takes a simple few seconds to attach a device to the back of a PC in order to record every keystroke that goes on the next day," he says.

Doors themselves can expose big breaches. Peters has found doors that have proximity sensors on them, which unlock doors on the inside. But some entrances can be activated from the outside simply by wiggling a piece of cardboard underneath the door.

Bank executives and consultants cite training as a key data theft-prevention tool. While regulators require training once a year, bankers using best practices say doing it more often is better, in order to keep the idea of security on the minds of employees. First Horizon National Corp., based in Memphis, Tennessee conducts training each month, typically using a five-minute session on the Internet. Recent sessions included e-mail security and how to keep the desktop computer secure from other employees. "I don't want to hit up employees for an hour and say you're done for the year," says Christopher Leach, a senior vice president of information technology risk management at the \$37 billion bank. "We hit them up five minutes here and there to constantly remind them. They can take it home with them and think about it more."

"We are also constantly pushing awareness that security is everyone's job, not just my team's job," Leach adds. Simple prevention measures include being careful while working in public places such as airplanes, where passengers can peer over a shoulder, or coffee shops, where others can easily eavesdrop on conversations. "In general, we try to bring good security practices to the forefront," he says.

When Holmquist arrived at Advanta three years ago, one of his first tasks was to implement a training program. "I wanted to [further] reinforce the business side of things," he says. "It's amazing what people tell you. People want to participate. The two biggest things our training does is let people know what is expected of them, and it also lets the bad guys know—and they are out there—that they are being watched and those who cross the line will be prosecuted. Shame on you if you never told your staff that. As a result, we built a much bigger army."

Banks also need to take the cumbersome step of documenting where all of their data is. That means rummaging through places ranging from the mainframe to desktops and laptops to vendors. Every bit of data - including social security numbers, addresses, transaction amounts, and credit card numbers - needs to be classified, says Stephen Barlock, a senior executive at Accenture's San Francisco office and head of the consulting firm's North American security practice. "The key to the whole thing is really understanding as an organization what sensitive data you have, and where it is," Barlock says. "That is critical to the starting point. You would be surprised. A lot of banks don't understand what data is where, who is carrying it, and what systems it is tied to."

"A bank might have a policy that defines tiers of confidentiality," he continues. "Yet it still needs to go through the hard, grinding work of looking at the entire enterprise data model and all the systems it has and aligning at the elemental level all the pieces of data within the framework it has defined."

## **Data touch points**

As the Bank of America and Citigroup incidents illustrate, banks also need to know how customer data will be handled by their vendors. "Who is going to touch that information?" Peters says. He recommends that banks require vendors to provide so-called SAS 70 statements, short for Statement on Accounting Standards No. 70. The statement can provide valuable information on a third party's security controls. Many smaller vendors such as laser printing houses have not issued these, which should send up a red flag.

To be sure, vendors pose a particular challenge for banks, says Alex Berson, a director and practice leader for the relationship and identity management group in financial services at BearingPoint Inc., a consulting firm based in McLean, Virginia. "The federal regulators have stated clearly that, even though your data was stolen elsewhere, you are responsible," Berson says. "That makes choosing a third party a very interesting business proposition. You cannot just blindly say because the cost is right, I am going to give them my data."

While performing a comprehensive inventory of their customer data, banks should beware of marketing central information files—or

MCIFs—which are used by marketing and other departments for mailings and cross selling. Banks should also have a good idea of what paper printouts are made in all departments, and what the auditors have on their laptops. All told, taking inventory might involve looking at tens or even hundreds of thousands of data elements stored in all of a bank's applications, mapping them, and then translating that into policy and action.

That will help banks handle the next phase of data security, which involves examining so-called identity space management: determining who has access to what, depending on their role in the bank. For example, as tellers move up to another position, access to applications would automatically shut off.

"In corporate America, we are good at granting access and slow to take it away," Leach says. "Unless we're firing somebody—then we're good at taking it away. Otherwise, we tend to forget to turn off access to things employees no longer need." Last May, First Horizon was trying to solve this problem by hashing out rules that specify access according to position, a task easier said than done. "As you can imagine, this is very political, because everyone has an opinion," Leach says.

Of course, banks also need to pay attention to the latest technology issues. Multifactor authentication is one hot topic as a result of phishing attacks—where data thieves direct unsuspecting users to facsimile websites and steal information by asking them to enter personal statistics. The Federal Financial Institutions Examination Council, which is made up of five regulatory agencies overseeing banks, thrifts, and credit unions, has said that single-factor authentication is inadequate for high-risk transactions, that is, those "involving access to customer information or the movement of funds to other parties," according to the agency's guide lines. There are a variety of ways to authenticate users, such as secret questions, password-generating tokens, and biometrics. And banks can determine whether a customer is logging on to a website from the computer he or she typically uses, and whether the user is exhibiting normal transaction behavior. Banks meanwhile, if they haven't already, should also be encrypting data on laptops, e-mails, and data transfers, consultants say.

Of course, banks always need to question whether each investment decision to protect data makes economic sense. In essence, they will have to continue to work on both business and technological processes to protect the data that is so critical to their reputations and financial success, bankers and consultants say. "Data security is never going to be a destination," Leach says. "It is always going to be a journey. Because as soon as we get to one level, the bad guys get to the next."

[Close Window](#)

3rd Quarter 2006