Is It Time for a Fresh Look at the Bank Protection Act?

Chris Swecker and the SEC examine the 41-year-old physical security legislation

By Chris Swecker and Marleah Blades

When banks are suffering their biggest losses from fraud-related and cyber crimes, it is easy to overlook the importance of such mundane things as physical security standards. But even if their loss figures are lower, bank robbery and bank burglary are still significant threats, says Doug Johnson, vice president of risk management for the American Bankers Association. "Physical crime can have a potentially significant impact on the customers and the employees," he says. "A bank robbery is something you remember. So regardless of what the loss might be, it is safe to say it's a significant event, and that's why we take it so seriously."

One 41-year-old piece of federal legislation sets physical security standards for banking institutions. Has it improved security against the stated physical threats it targets? Does it provide the best protection in the very different banking environment of today?

The Bank Protection Act of 1968

The Bank Protection Act was passed in 1968 in response to an increase in the rate of bank robberies in the United States. The Act placed minimum security guidelines on banks "to discourage robberies, burglaries, and larcenies and to assist in the identification and apprehension of persons who commit such acts."

It designated four Federal supervisory agencies — the Comptroller of the Currency; the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation; and the Director of the Office of Thrift Supervision — to promulgate minimum security standards for the banks or S&Ls they regulate. The four resulting sets of rules are basically identical.

On the management side, they make the bank board of directors accountable for compliance, and they require that banks create a written security plan, designate a security officer, establish opening and closing procedures, provide training for officers and employees, and present annual reports to the board on the effectiveness of the security program. Regarding technology, they state that banks must:

1. Use some method of identifying robbery or burglary suspects;
2. Have devices in place to protect cash (such as a vault);
3. Have lighting for the vault if it is visible from outside the office;
4. Have tamper-resistant locks on doors and windows;
5. Have an alarm system; and
6. Have other devices deemed necessary by the security officer.

By all accounts, banking has changed remarkably since the advent of this legislation, and even since its amendment in 1991. That fact alone is enough to warrant a fresh examination of what the Bank Protection Act (BPA) does and does not accomplish.

The Evolution of Banking

Banking in 1968 was about face-to-face transactions — a customer walked into the bank office or branch and did all his or her business with a teller or cashier. ATMs were not rolled out in scale until

the 1970s, and their use did not begin to explode until the 1990s. Today, a single commercial bank may maintain more than 18,000 ATMs — approximately the total number of ATMs in the United States in 1980. And while American Bankers Association surveys year after year have shown that customers still prefer branch banking above other methods of banking by a nose, the survey results released this September revealed that the lead has finally been lost. For the first time, more bank customers (25 percent) prefer to do their banking online compared to any other method. Seventeen percent of respondents prefer ATM banking over other methods, and 1 percent would rather use PDAs and mobile devices.

All these changes in banking methods and trends mean changes in the nature of risk for banks and bank customers. The BPA does not expressly regulate the media for any of these trends — mobile devices, ATMs and online banking methods. Do its minimum security requirements adequately address the evolved risk picture? Perhaps we should first answer the question: Should they?

Has It Been Successful?

The stated purpose of the law is "to discourage robberies, burglaries and larcenies and to assist in the identification and apprehension of persons who commit such acts." Surely the crimes of robbery, burglary and larceny have not changed much, even if the methods of banking have changed. Per Webster's, burglary is breaking and entering at night or after hours for the purpose of committing theft. Larceny is the unlawful taking of personal property. Robbery is larceny through threat of violence. These terms apply to bank crime in fairly obvious and conventional ways — a bank robbery or burglary is a crime perpetrated against a bank office or branch. If the law was intended to deal specifically and solely with those threats in their traditional sense, then we can look at history as a measure by which to gauge its success.

Has the BPA been successful in discouraging robbery, burglary and larceny? A 1983 report by Philip J. Cook, contracted by the U.S. Department of Justice, found that between 1970 and 1980, the number of bank robberies increased at a compounded rate of 11 percent each year. In his 1981 book Bank Security, R.E. Anderson wrote, "There is little doubt whether the (Bank Protection Act) has been successful in controlling bank robberies. It has not." Publicly available FBI bank crime statistics indicate that the rate of bank crime in general has waxed and waned since 1970, but overall has continued on an upward trend. We certainly cannot blame all such statistics on a failure of the BPA to discourage bank crime; however, based on this evidence, it seems the BPA has not made great strides forward in the first stated part of its mission.

Has it been successful in increasing the identification of perpetrators of these crimes as understood in 1968? That remains unclear. Bank robbery has one of the highest clearance rates of any crime, meaning that bank robbery suspects are apprehended at a high rate compared with suspects in other crimes. This implies that identification methods work. However, according to the Center for Problem-Oriented Policing, the clearance rate declined from 80 percent in 1976 to 58 percent in 2001.

So it seems that even if we limit the interpretation of the BPA to address strictly burglary, larceny and robbery in their traditional brick-and-mortar, branch bank sense, the legislation has not made a great, lasting impact.

A Case for Hardening Security

The BPA's standards are broad and clearly intended to provide flexibility for banks of different sizes, in unique locations, with unique needs. However, over time, many individuals have offered up ideas on how to enhance the baseline security the BPA requires in order to help it fulfill its mission. Some examples:

- **Surveillance in the parking lot.** Most banks have cameras or other monitoring technologies inside to help meet the BPA's requirement for devices that help identify perpetrators. Few institutions have cameras facing the parking lot. Robbers are likely to case a bank before they rob it, and parking lot cameras with broad scanning capability and strong resolution could help identify perpetrators before they put their masks on. They could also act as a deterrent.
- **Minimum surveillance standards.** The BPA no longer expressly requires CCTV or video surveillance, though many banks use those systems to meet its broader requirements. Perhaps minimum standards for surveillance systems would help banks in implementing technology that will best meet the needs of their environment.
- **Design considerations.** Crime Prevention Through Environmental Design (CPTED) is a powerful mitigation technique that many banks already use. It would be difficult to set a complex standard for this given the variances in archi-

tecture and location, but baseline guides could be set, such as ensuring that the main entrance is not obstructed with foliage and other natural hiding places.

• **Alarm protocols.** The BPA requires alarms, but what about redundancy? What about backup power? There are some protocols around alarms that could be helpful for many banks. For instance, one popular method of burglarizing a bank is to probe the building to set off the alarm, wait for the police to come and leave, and then go in again for the burglary. Often, the police do not return immediately because they have already had one false alarm. A useful protocol could require that someone from the bank respond at a second alarm.

• **Minimum training standards.** The BPA requires employee and officer training, but none of the supervisory agencies specify what that training should entail. Broad minimum standards would ensure that employees have the knowledge they need to help deter and identify perpetrators.

• **Issues of repeat victimization.** Bank branches that have already been robbed once are often robbed again. Several studies bear out that a branch that has never been robbed faces a low risk of robbery, and a previously robbed branch has a substantially higher risk. It would be helpful for banks and branches to maintain a schedule for escalating security measures after an event to mitigate the increased risk that event represents.

• **Risk assessment.** The word "risk" does not appear in the BPA or any of the four supervisory agencies' resultant requirements. A risk assessment is a must to adequately protect any individual branch against these kinds of physical threats.

These are the issues that some feel the BPA neglects, even if read strictly as a law targeting traditional methods of robbery, burglary and larceny. A case can also be made that the terms robbery, burglary and larceny do indeed encompass newer crimes than the 1968 Act could have foreseen, and this introduces more concerns.

A Broader Interpretation

Does uprooting an ATM with a pickup truck and a chain constitute burglary? What about installing a card skimmer on one? Is online banking crime, like theft or cracking of usernames and passcodes are a form of larceny? Or are such things more properly referred to as fraud?

In that same vein, can a broader interpretation be given to the mission of the BPA? It is very possible that its full intent was to address burglary, larceny and robbery only, and to leave other risks to other legislation. It is also possible that legislators meant it to address the predominant security threats to banks and bank customers, which legislators at the time viewed as burglary, larceny and robbery.

If we espouse this broader interpretation, the BPA should be addressing the security threats that are of importance to banks and their customers now. If that is so, it appears to fall short in two specific areas: ATM crime and data security or online banking crime. Other federal legislation and guidelines exist to deal with the latter (see this month's *Compliance Scorecard* below for a discussion of one such rule), so we will focus on the former.

The American Bankers Association's Doug Johnson cites ATM skimming as the biggest physical security risk that bank customers are facing today, and one of the threats that's most front-of-mind for bank

Compliance Scorecard

Security Leadership Solutions Executive Council

FFIEC Authentication Guidance

By Marleah Blades

"Authentication in an Electronic Banking Environment" is a document released by the United States Federal Financial Institution Examination Council (FFIEC) in 2001 to provide guidance to U.S. financial institutions on authenticating customers in electronic or online transactions. Its goals in doing so are to safeguard customer information; to prevent money laundering and terrorist financing; to reduce fraud and the theft of sensitive customer information; and to promote legal enforceability of financial institutions' electronic agreements and transactions. The guidance was revised in 2005.

The FFIEC guidance clearly states that "single-factor authentication, as the only control mechanism, (is) inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties." That means that a simple username/password combination is officially recognized as insufficient security for online transactions.

While guidance does not equal regulation, many banks treat the FFIEC document as law, because other rules, such as the Uniform Commercial Code and GLBA, require that banks take reasonable precautions to protect customers against fraud and information theft, and the guideline legally raises the bar for what is "reasonable."

While the guidance states that single-factor authentication is not enough, that does not mean that banks should all be issuing biometric readers and tokens to their customers. Multi-factor authentication in the banking environment can mean many things, says Jerry Tylman, partner with business consulting firm Greenway Solutions. "For example, your ID and password is one factor. The second factor could be a risk score based on a suspect IP address," he says. "If you are logging in from an unusual address, they may ask you for your mother's maiden name before you can continue."

That type of additional security certainly strengthens authentication. But one of the complex problems with online banking fraud is that even information like your mother's maiden name can be acquired by a diligent criminal to bypass such methods.

"Most of the data that gets into the hands of fraudsters gets there through social engineering," Tylman says. "It was not the banks that gave the data away, it was the customer." For this reason, banks that want to go beyond the guidelines to protect customers should implement multiple layers of security that include knowledge-based questions (e.g. the color of your car), signature analysis (e.g. something that identifies your computer), and transaction analysis to assess if your online activity is normal or abnormal (e.g. this person has never attempted to wire money to Russia). Layered protection like this is by far the most effective way of preventing and detecting fraud.

Marleah Blades is senior editor for the Security Executive Council. For more information about the Council, visit www.securityexecutivecouncil.com/?sourceCode=std.

security officers. Skimming is the practice of installing some physical device on an ATM that reads information from the swiped or inserted card. The ABA is actively looking at expanding its existing bank robbery database to track where ATM skimming devices have been found in real time.

Another ATM crime, in which perpetrators physically pull the machine off its base and haul it away, is less insidious but also widespread.

While states including New York, Nevada, Washington, Oregon, Georgia, Louisiana, Maryland and Florida have passed laws on ATM security, there is no federal law that sets security standards for ATMs at financial institutions or in other locations. The BPA certainly does not. Laws, standards or guidelines — such as a revised BPA, perhaps — could protect ATMs from removal by requiring or recommending the placement of bollards around them, that GPS devices be included in them, or that they include some other mechanism to deter or prevent the machines from being pulled from their bases. They could also require or recommend the use of anti-skimming devices of various sorts to be installed on ATMs. Some of these recommendations would have to be met by manufacturers and others by bankers.

Should the Law Be Revised?

The question is, are the concerns we have discussed better dealt with by legislation or by industry cooperation and best practice?

"I do think (revision) is a worthwhile tact to take," says Richard Lefler, Dean of Emeritus Faculty of the Security Executive Council and former CSO of American Express. "The Act addresses the brick and mortar security issues. But banks have become virtual. So the applicability of the old rules has to be adjusted to reflect the reality of the banking world today."

Johnson disagrees: "We as a regulated industry are fairly accustomed to having the flexibility in our environment to look at the risks we have. It's in the financial institutions' best interest to make sure the customer is protected. I think as an industry we generally come to these conclusions without legislation." Johnson goes on to say that the ABA's Security Committee, which includes the security leaders from 15 of the nation's top banks, do not feel that improving the BPA needs to be a top priority at this time.

"One of the thing that concerns us about the suggestion that we need to harden the Act to require certain technologies is that technologies change," Johnson says. "If we mandated certain technology to defeat skimming, we would not know how long that technology would stand the test of time before the perpetrators find ways to defeat it. This is an arms race with the folks that want to commit fraud. We do not feel it's advisable to legislate technology."

Lefler offers one option for regulation that he feels is on the horizon for the financial industry: "We could create a regulatory environment that will require the banking industry to develop what I call a R.A.M.S. strategy — risk analysis, mitigation strategy — approach," Lefler says. "Before a new product is offered, the financial company has to, by legislative mandate, do an analysis of risks, including security risks, and develop mitigation strategies to deal with those.

"Take portable ATMs for example," Lefler continues. "They would have to analyze what the security risks are related to establishing ATMs at grocery stores, gas stations and parking lots. Then they would have to define what their mitigation strategies are. And they would have to put controls in place to manage the scale of risk that would impact those machines and the customers using them. If the banks failed to determine that the risk existed and did not develop a mitigation strategy, the regulators would then come in to legally mandate the issue."

This type of approach would avoid the sticky problem of legislating technology and potentially make regulation an easier pill to swallow for all parties. ▮

Chris Swecker is emeritus faculty for the Security Executive Council (SEC) and former head of Corporate Security at Bank of America. Prior to joining Bank of America, Mr. Swecker was assistant director of the Criminal Investigative Division and acting executive assistant director for Law Enforcement Services at the FBI.

Marleah Blades is senior editor for the Security Executive Council, a risk mitigation research and services organization for security and risk executives from corporations and government agencies responsible for corporate and/or IT security. The Council is dedicated to developing tools that help lower the cost of security programs, making program development more efficient and establishing security as a recognized value center. For information, visit www.securityexecutivecouncil.com/?sourceCode=std.