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.