



Security Strategies

Deterring would-be robbers is a matter of consistency, multiple deterrents ... and dogged persistence.

By Jamie Swedberg

Here's some good news, sort of. According to the FBI, there were fewer bank and credit union robberies in the United States in 2008 than in 2007. The numbers for 2009, still being compiled at the time of this writing, are on track to be lower still.

But it's cold comfort, because there are still far too many robberies for anyone's liking. There were more than 6,200 in 2008—a startling number. And robberies seem to happen in clusters, with little warning or reason. For example, Tulsa, Okla., faced a veritable epidemic of bank and credit union robberies last year. Police there investigated 29.

"It moves around geographically," says Dennis Godfrey, chief officer of innovation at \$40 billion Navy Federal Credit Union (www.navyfederal.org), Merrifield, Va. "We've seen an increase in takedown robberies over the years, particularly on the West Coast. I don't know that the numbers are spiking nationally, but we've seen these types of robberies occur on a more frequent basis than they have in the past."

Takedown robberies—the kind where a group of individuals comes in armed and forces all the employees and customers

to get on the ground—are only one of the many types of bank and credit union robberies. About half of all robberies are perpetrated by "note passers," who quietly approach the teller line and hand over their demand in writing. There are numerous other types, too.

"They may use a verbal threat, such as 'This is a robbery; give me all of your money,'" says Dana Turner, security practitioner at Security Education Systems LLC (www.secedsys.com), Pipe Creek, Texas. "Or they might pull back their jacket and show that they have a handgun. Those, along with the note-passers, are what we call simple robberies. But there are also the sophisticated ones: They may use a bomb or a bomb threat. They may kidnap an employee at home, and hold the family hostage. They may effect a full takeover, like a morning glory robbery (so-called because the robber takes over the facility before it opens in the morning). Or sometimes they just



walk in and shoot somebody and say, 'Now, there's your lesson. Give me your money.'"

The sophisticated robberies account for fewer than 10 percent of bank and credit union robberies, Turner says. But they still happen, and they have a profound, long-term emotional effect on employees even if no one is hurt.

"Every robbery is a threat," says Godfrey. "Obviously some are more dangerous than others. But we treat them all equally. We just take it very seriously."

The economy has added extra complexity to the problem. Many robbers of financial institutions are hardened criminals who have spent time in prison and learned techniques from their colleagues. But Turner says the economy has changed the robbery environment in the last 18 months.

"We're having more and more robbers who are totally inexperienced former family people, losing their houses, can't pay their bills, have gotten into the robbery game," he says. "They are desperate people who are typically unfamiliar with firearms. You can get shot by accident, and it hurts just as badly as it does to get shot on purpose. They don't plan well. They panic more frequently because it's outside the realm of their normal behavior."

And while credit unions might have experienced fewer robberies in the past, because they were flying under the radar or thieves didn't think they had cash on hand, those days are gone.

"Credit unions lucked out for a while,"

says Paul Seibert, certified management consultant and VP/financial services at EHS Design Inc. (www.ehs-design.com), a CUES Supplier member based in Seattle. "But now I think everybody knows they have cash. And robbers know more than that. There's a lot of knowledge in jail about banks and credit unions and who has the best and worst security."

Yet despite all this, many CUs let their robbery prevention efforts become stale or out-of-date. They fail to check their equipment or train their employees. Many are only jolted into action when they experience a robbery—or several. But by leaving themselves unnecessarily vulnerable, they help perpetuate a type of crime that every financial institution ought to be working against.

"Every robbery is every bank or credit union's problem," says Turner. Robbers don't usually stop at one financial institution; they go on to the next and the next. "It's a community issue. It's not just your credit union. So do a better job of learning about what options are available to you, many of which are low or no cost."

A Novel Approach

One of the most effective new anti-robbery tools is a program called SafeCatch. Developed in 2006 by Seattle-based FBI agent Larry Carr, with help from Seibert, SafeCatch is a behavior-based system designed to prevent and thwart robberies and fraud. Its key points include staff training, branch architecture and design, video-camera placement,

restructuring procedures for better response time, and ongoing performance measurement. But its most recognizable feature is the fact that it melds robbery prevention with excellent member service. Carr and Seibert found that what's good for one is good for the other.

Here's how it works: A man walks in the front door of the credit union, and before he can take more than a few steps, a branch employee walks up, looks straight into the person's face, and extends a cheerful hand. "Hello!" the employee says. "My name is Chris. What can I help you with today?"

If the man is a member or a prospective member, the employee has just given him excellent service. Perhaps the man wants to apply for a loan, or just needs to deposit a check. He will be pointed cheerfully in the proper direction.

If the man is a would-be robber, he's just lost his anonymity. He knows he has been noticed, and hasn't even made it to the teller line yet. Most times, Seibert says, the person will mutter something about wanting to cash a check, then will pretend he can't find his driver's license and slink out the door.

There's more to it than that, of course. In helping develop SafeCatch, Seibert's firm contributed a lot of anti-robbery architectural specifications that are cheap or free to incorporate into a new branch. (Obviously it can cost a bit more to remodel an existing branch to match these specs.)

"We [EHS Design] worked on the architectural side to create an environment that enhanced the effectiveness of SafeCatch,"



says Seibert. "It causes low-level stress in the robber—not to the point where they get angry or feel the need to fight, but just so they're uncomfortable.

"We place an element in front of the person coming in the door, so they can't see the entire branch at once. They don't know if there might be a policeman present that they can't see. Once they're on the other side, they can see the teller line, but they can't see all the doors. Who might be coming in? We put the check stand facing away from the teller line, so that if they're standing there writing a note, they have to keep turning around to see who might have come in."

Under SafeCatch guidelines, cameras are

SafeCatch institutions, only to leave a moment later when they are greeted at the front door. He even has a video of a robber entering another bank down the street from the first one he tried—only to be bounced a second time by SafeCatch-style customer service.

Yet there seems to be some pushback from the industry. Seibert suspects some executives don't feel as though they're getting real robbery prevention unless they pay a lot for it.

"A bullet-resistant barrier costs \$50,000 at an average branch," he says. "It's expensive. But if you spend that money, you're doing something tangible, so that must be

to be able to see the front doors and the drive-throughs from the street."

Of course, neighborhoods change, and sometimes even the best-planned location ends up being undesirable. Then it's all the more important to make the building itself an unattractive target.

Cameras, prominently placed at eye level, are a major physical deterrent. But Turner says many credit unions haven't replaced theirs for a while.

"There have been tremendous advancements in cameras in the last couple of years," he points out. Lenses are better. Optics are better. A lot of [organizations] say they can't afford new cameras, but they don't need them. You can get your vendor to come in and install an upgrade to the optics and the memory card, and you're up to date again. Also, height-marker cameras are great." These tiny cameras are mounted in a strip flush to the door frame, opposite a measuring tape strip. They capture in full color the face of the culprit at eye level, against the measuring strip as they exit. Height-marker cameras are relatively cheap in security terms, with one on the market in the \$600 range.

Don't forget cameras outside the building. Video cameras in the parking lot can help indoor personnel monitor vehicular and pedestrian flow, and give them an early heads-up on a person's suspicious behavior.

Signage is important, too. First, the lack thereof: Turner advises keeping credit union signs off of facilities that don't serve members who walk in. For example, there's no reason a loan processing office needs to be branded with the CU's logo, since members don't go there. Yet many credit unions place signage on administrative buildings anyway. That can attract robbers who don't know there's no cash on site.

Conversely, Turner suggests more signage on member-facing facilities. He advises signs prohibiting firearms on the premises, as well as signs banning hats, hoodies and sunglasses inside the building. The latter advice is controversial; some credit unions have been sued by people who feel it amounts to religious discrimination.

One of the most common suggestions Turner makes is the installation of an electronic lock on the front door.

"Traditionally you've got a knob lock, or it requires a key. In the case of a robbery, you send someone you don't like or whose job you hope to inherit over to lock the door when the robber leaves the building," he jokes. "That's a very dangerous position. The robber runs out,

"Robbers don't like to see lower cameras. They like high cameras because they can put their head down and hide their face. Visibility is another thing that makes them uncomfortable and keeps them away."

Paul Seibert, CMC

placed at eye level—something financial institutions have often avoided in the past in the name of aesthetics. This helps capture better pictures of robbers' faces. Of course, the cameras are blended in with lots of friendly merchandising.

"Robbers don't like to see lower cameras," says Seibert. "They like high cameras because they can put their head down and hide their face. Visibility is another thing that makes them uncomfortable and keeps them away."

Instead of being behind one long counter, tellers in a SafeCatch institution stand behind individual pods. If a suspicious-looking person approaches, tellers can quickly and politely absent themselves, making an excuse about a computer glitch. That leaves the would-be robber twiddling his thumbs in the middle of the room.

"If a person doesn't leave, if they just hang around and wait, it's likely they're not a robber after all," Seibert says. "So you can come back in a minute and say, 'Gee, I'm sorry, everything is working now. How can I help you?'"

SafeCatch focuses on foiling simple robberies, not the much rarer and more dangerous sophisticated robberies. But in the vast majority of cases, it has been shown to work. Seibert has seen video documentation of known robbers entering

the solution. How about a different solution instead? How about we train people to be more friendly and proactive?"

Smile! You're on Candid Camera

Organizations employing SafeCatch are not the only ones making changes to their buildings. Other credit unions are also using what they know about robbers' habits and preferences to design safer branches.

"What a robber wants is a way to get away," says Seibert. "So what they want is the ability to get to a freeway. Often the branches that are hit most are those that are closest to a freeway, which usually coincides with their being in a very high retail area."

So despite the fact that they want to locate their branches as conveniently as possible, many credit unions prefer to locate their branches away from highway onramps. But that's only one of many factors to consider when choosing a location.

"If the neighborhood is not conducive to running a safe operation, you really don't want to build a branch there," says Godfrey. "Before we ever dig a hole, or even sign a contract for a piece of property, we review the crime statistics for the area for a long period. Is it in a safe area? And will we have a clear view? We need



sees the cops, and wants to run back in. Meanwhile, the employee has just locked the door, but he's standing there in front of a piece of glass. You could take the risk away by installing a buzzer, a button that automatically locks the door."

For professional advice when building or remodeling branches, Turner suggests hiring a security architect versed in Crime Prevention Through Environmental Design. Through the careful placement and design of walls, ceilings, lighting, flooring and furniture, you can reduce people's opportunity and desire to steal, and lower your liability while you're at it. It adds only a couple thousand dollars to the cost of an architect's plans, he says, and is well worth the modest price.

The Tipping Point

Day-to-day procedures are probably the most common way credit unions address the risk of robbery; yet very few CUs are as consistent or rigorous as they should be. Sure, they have confidential opening and closing procedures. They avoid having extra cash at the teller line. And if they're smart, they use armored carriers to swap ATM cassettes and to move money from one branch to another.

But unless something bad has happened in recent memory, security procedures tend to become stale. Turner recommends forming a security committee so robbery prevention is never pushed to the back burner.

Andy Greenawalt, CEO of Boston-based compliance firm Continuity Engine (www.continuity.net/about/), would like to see credit unions go one step further. Because most CU employees are stretched thin, they usually don't have the time or energy to deal with robbery prevention in an organized way. So Continuity Engine offers what it calls an "Action Pack"—software that controls and automates the process. Designed with the help of ex-felon Troy Evans, who now works as a security consultant, the software alerts employees whenever they should be taking care of a security task.

"With physical security, there are things as simple as the ID validation," Greenawalt says. "When someone comes into the branch to fix the toilets, it could be that they're really casing the joint. There are things like inspecting the security equipment on a periodic basis, ensuring that bait money or dye packs are in place, and providing security training

for the tellers. We've put all of the little steps that make up a broader anti-robbery strategy into these very simple to-do items that go out to whomever the appropriate parties are."

Greenawalt says what often happens in the absence of an organized system is when credit unions experience employee turnover, some tasks fall through the cracks.

"Maybe they train everybody in January, but unfortunately the branch manager at the Main Street branch leaves in March," he says. "Then the new branch manager really doesn't understand the controls for the better part of a year, and he or she leaves some exposures."

CUs are experiencing a greater and greater compliance burden when it comes to robbery prevention, he says. And just as in the famous "I Love Lucy" episode, bonbons start falling off the end of the assembly line. Someone forgets to document the sequence numbers on the money; then there's a robbery, and the police are unable to convict.

\$200 million First Service Credit Union (www.1stservicecu.com) in Houston, Texas, started using CE's Action Pack after one of its branches was robbed in July 2009. Director of Compliance and Internal Audit Sid Zahn says his CEO wanted him to go over every detail with a fine-toothed comb.

"It's kind of a large task to make sure that every branch is doing everything the same way," says the CUES member. "That's what he wanted me to make sure of. We wanted to be consistent at all our branches, and to document it."

First Service CU has since implemented a wide variety of the procedures in the Action Pack, ranging from sign-in books to the placement of large male security guards. Zahn says all the controls, if consistently applied, add up to a very significant deterrent.

Perhaps one of the most important aspects of an anti-robbery program is the immediacy and consistency of training. It's crucial to give employees the preparation they need to keep themselves safe, get robbers out the door, alert law enforcement, and hopefully collect evidence that will lead to a conviction.

"A lot of people who run credit unions and banks will wait a couple of weeks or a couple of months before they put



new people through robbery training—until they get enough people to make a class worthwhile to them," Turner says. "That's dumb. It's a violation of every safety code I know of. And if that person gets hurt, then the credit union has lost its defense because it did not follow industry standard practice. So you've got to train them in robberies, bomb threats, hostage events, diffusing bad customer situations, and things like that before you ever put them in customer contact tasks."

What's the take-home lesson? When it comes to preventing and mitigating robberies, security is cumulative. There isn't any one magic bullet that will stop would-be robbers. What works best is a slew of deterrents, one after another, that make a robber turn around and walk away.

"You want them to look at you and say, 'This isn't worth it,'" Turner says. "You get to a certain tipping point, and they go 'Nah.' And that's the whole object."

Jamie Swedberg is a free-lance writer based in Georgia.

Resources

View the "Don't Get Socially Engineered" video at cues.org/dontgetsociallyengineered.

Read more on security at cumanagement.org/fyi/securityarchive.

Learn more about SafeCatch and branch security in *The Complete Guide to Credit Union Facilities* by Paul Seibert. Order at cues.org/compleateguidetocufacilities.