

www.bankersonline.com

Panic & Alarm Buttons

by [Barry Thompson](#), BOL Guru

Question: I have a client bank who has opted to remove the teller's alarm/panic buttons. Is there a trend in doing this for some reason and can you speculate on the pros and cons?

Answer: Regulation H states:

“(iv) An alarm system or other appropriate device for promptly notifying the nearest responsible law enforcement officers of an attempted or perpetrated robbery or burglary;”

Some financial institutions no longer believe that alarm/panic buttons are the fastest way to notify law enforcement. Instead these institutions are opting for a direct call to 911. They believe the dispatcher can relay information directly to the road patrol for a faster police response. I will not discuss the pros and cons of this on the internet.

First published on BankersOnline.com 4/19/04

Security Tips for Supermarket Branches

by [Dana Turner](#), BOL Guru

Question: Any special tips on security training for tellers and CSRs working in our supermarket branches?

Answer: "In-store" branches may pose special security problems for both employees and customers. The institution must comply with the host's own security practices first, before it can use its own. The host's security practices may conflict with the institution's practices, particularly regarding.

- Opening and closing activities
- Alarm activation procedures
- Placement of security cameras - or the forced reliance upon the host's cameras and recording system
- Height of teller counters
- Installation of bandit barriers
- ATM replenishment procedures
- Armored carrier cash delivery
- Selection of emergency evacuation sites
- Emergency evacuation tests
- Use of security guards
- Use of a floor-to-ceiling gate to secure the branch during non-business hours

In addition to the institution's normal security practices, "in-store" security training should also include:

- Orientation and periodic retraining regarding the host's facility and security practices
- Orientation and periodic retraining regarding evacuation sites, the use of any specialized equipment and opening and closing procedures

First published on BankersOnline.com 4/19/04

Teller Safety Issues

Answer by Dana Turner, BOL Guru

[Guru BIOS](#)

Question: For a Bank Drive-thru that is separate from the building (connected only by the drive-thru lanes) should there be two full time tellers in that building at all times? What about storage of those tellers' cash. Should there be a vault located in that separate building or the money transported to and from the main building?

Answer: General guidelines for this type of operation include the safety practices that you use for the branch:

- Opening and closing procedures -- using two (2) employees -- are followed;
- The building is equipped with a telephone, robbery alarms and cameras;
- Money must be delivered and retrieved by an armored carrier;
- Daily work (except money) may be transported to and from the building by one (1) employee; and
- Except for opening and closing, one (1) employee may conduct transactions as long as the building is secure.

More specific practices may need to be developed, based upon the building's configuration, operating hours and use.

First published on BankersOnline.com 3/1/04

Using Actual Video Of Robbery In Training Session

Answer by Andy Zavoina, Hussam Al-Abed and Dana Turner, BOL Gurus

Question: Would you advise using a video tape from a bank robbery of a sister bank in a training session for employees?

Answer by Andy Zavoina:

[BIO AND CONTACT INFO](#)

Opinions will differ and it certainly depends on what is in the video. Personally I like the realism which may be gleaned from this. "Yes, it can happen to you...". The shock and awe effect can be meaningful, so long as it isn't to a point where the employees are scared to do their jobs because of the violence shown.

Training includes instilling the confidence to handle the situation.

Answer by Hussan Al-Albed:

[BIO AND CONTACT INFO](#)

I am looking for such a video myself; an effective Training should include case studies and what is better than an actual case of armed robbery!.It can be used to study the scenario of the armed robbery and how each employee acted upon it. If they received armed robbery Training before:

did they apply any of it during that actual robbery?

The video it self should receive a complete analysis by the Trainer before it is shown to Trainees, Trainer should study The robbers Moves on their way in and out of the bank, How the staff reacted, were they Observant during the robbery? Did they fill the cards after the robbery was over? Did they handle with care what ever the robbers touched? Did they activate the alarm? If yes: when? What a bout other customers whom were at the bank when the robbery took Place? Did any one leave? If yesdid someone take his or her contact info. ? Did the staff discuss descriptions of robbers among them selves?Such a video is highly recommended in Training On the Other hand it should be mentioned that armed robbery is a “ Minutes Crime “ More Like “ Grab & Run “ such a short time Might let the robbers act More violent to ensure discipline and there demands are met quickly, for that reason Training should include a List of Doe’s & Don’ts during the robbery to ensure safety of every one at the bank and at the same time grabbing the descriptions of The robbers.

Answer by Dana Turner:

[BIO AND CONTACT INFO](#)

Captured "live events" make excellent training supplements -- often for both the "do" and "don't" actions that may be highlighted.

Using such a videotape with the rightful owner's written permission (obviously a corporate "sister" bank needs no such permission) shouldn't be a problem -- in most cases. It may matter very much, however, if the videotape is to be used in a court trial. If the employees who were robbed viewed the event, their testimony at time of trial might be compromised. Check with the responsible law enforcement or prosecuting agency before showing the tape.

First published on BankersOnline.com 7/21/03

Mock Robberies

by Dana Turner

[BIO AND CONTACT INFO](#)

QUESTION: We'd like to do some robbery training using mock robberies, and our HR people are objecting violently. Is there a problem doing mock robberies?

ANSWER: Mock robberies using employees as PARTICIPANTS is particularly hazardous. Even when employees are prepared, they often experience a multitude of adverse reactions. And if these employees are injured -- physically, mentally or emotionally -- they often sue (and win against) the institution.

Mock robberies using law enforcement officers as PARTICIPANTS and employees as OBSERVERS is an appropriate training tool. The cops win because they are better trained. The employees win because they can observe -- safely -- how they should react.

First published on BankersOnline.com 9/3/01

Robbery Training

by Dana Turner

[BIO AND CONTACT INFO](#)

QUESTION: Anything new we should be covering in our robbery training?

ANSWER: Bankers traditionally address a couple of robbery variations during training meetings: the stand-up robber with either a gun or a note. There are actually several robbery variations and

robbery training should address each one. The actual mechanics of each type of robbery differs from the other ones and the types include:

1. Stand-up robber with a gun;
2. Stand-up robber with a note;
3. Stand-up robber with a threat of having a gun;
4. Stand-up robber with a bomb, or the threat of a bomb; and
5. Take-over robbery with multiple offenders.

First published on BankersOnline.com 9/3/01

Robbery Training & Mock Hold-ups

Answers by Andy Zavoina, Barry Thompson and Dana Turner

QUESTION: Do you have any ideas for how we can make our robbery training interesting without it being scary? Do you think it's a good idea to include a mock holdup?

ANSWER by Barry Thompson, BOL Guru

[BIO AND CONTACT INFO](#)

The usual Bank Security training program begins with groans from all required participants, but how do you make it enjoyable? Here are three ideas I have used successfully many times.

One of the greatest training vehicles I have used in my twenty-two year career as a Bank Security Officer was to capture employees. Main Office and Branch personnel pay lip service to the morning warning system, but how many really observe it? For my security training, I would go to the targeted office before opening and change the morning warning signal. (If you are doing the training and you can't gain entry to the building, wait for your first team to arrive and then change the system.) I would then start taking staff members "hostage" as they entered work. The most effective thing to say is "Bang!"; your victim always grimaces. Many never forget the experience of being verbally shot when entering the financial institution.

Taking someone hostage when they ignore the standard morning warning system will provide you a basis to deal with someone who doesn't want to be trained. "Remember, Joe. I seem to have caught you last week, didn't I?" It's hard to argue about attending training when you have demonstrated through your own actions that you need it.

Another useful way to train is to do it regularly when you have to visit the teller line. Walk up to the teller who is going to perform your transaction and hand her a check. Ask the teller to point out the items that make it a check.

You can also bring a check you know is bad and hand it to the tellers and have them tell you what's wrong with it. This is an effective means of making training fun on a quiet day in your financial institution.

Above all, no matter what training methods you use, keep them enjoyable. It's easy to remember something that was fun to learn in the beginning.

ANSWER by Andy Zavoina, BOL Guru

[BIO AND CONTACT INFO](#)

Mock hold-ups can be useful, and very real. If orchestrated in advance, those participating can be convincing without being scary. Those watching can still learn. I have seen mock hold ups that were intended to represent a horrific gang robbery, but my experience indicates that many robberies are not that way. There is a single person with a note who says they are armed. They may or may not show a weapon. Staff needs to be prepared for this as well.

ANSWER by Dana Turner, BOL Guru

BIO AND CONTACT INFO

Contact your local law enforcement training center (police academy) about having an academy class conduct mock robberies -- at the academy. The officers "play" both the "good" and "bad" people. Your employees act only as observers -- not participants -- and then they critique the exercises later. Your employees benefit from the more exciting training scenarios and the cops benefit by "pre-living" the best responses to "real-life" events.

In my opinion, "Mock robberies" that are used for employee training without the employees knowing they are not real -- that use actual employees on the institution's premises -- have been the subject of too many lawsuits, already. Professional Security Officers stopped using them several years ago. By linking the cops to your training needs, you can increase the level and quality of law enforcement service while you decrease the potentially harmful side effects to your employees. First published on BankersOnline.com 2/5/01

Robbery Prevention

by Bart Frazzitta

[BIO AND CONTACT INFO](#)

QUESTION: What steps can a branch manager take to prevent robberies?

ANSWER: The question as to whether a branch manager can or cannot prevent a robbery is arguable in and of itself. What a branch manager can do is take proactive steps to create an environment that deters criminals from considering whether to rob a particular branch in the first place. Some of these measures include:

1. Limit the number of entrances to a branch. Instead of allowing customer access through two doors, use one door. (Additional doorways for staff can be secured with access control systems)
2. Consider designs that have teller counters to the rear of the branch. This acts as deterrent because a robber will have to cover a greater distance to exit the branch.
3. Employees who are well-trained and vigilant in robbery procedures
4. Numerous security cameras that are clearly visible
5. Establish an emergency action plan in case of robbery, and review it periodically to keep it current
6. Branches need to periodically test security systems for effectiveness and reliability

Bartholomew J. (Bart) Frazzitta, Vice President and General Manager, Physical Security Division, Diebold, Incorporated

Bart Frazzitta is vice president and general manager of physical security for Diebold, Incorporated. Based in Canton, Ohio, Bart is responsible for the development, sourcing and manufacturing of all Diebold physical security and facility products. This includes vault doors, modular vault walls, safe deposit boxes, drive-up pneumatic systems, safes, bullet-resistive products, work station furniture, fire-insulated products and other related items.

Frazzitta joined Diebold in 1972 as a sales representative in western Pennsylvania. He has since held various positions with Diebold, including regional sales manager, division vice president of sales, and vice president for Marketing. In 1991, Frazzitta was elevated to his present position of corporate officer and vice president, which entails all of the physical security and facility products that Diebold now offers globally. Frazzitta also serves as a board member for the company's subsidiary in Mexico - Diebold Mexico and Diebold China.

Prior to joining Diebold, Frazzitta worked for the Dover Elevator Corporation in Pennsylvania, Tennessee and Illinois. A native of New York metropolitan area, Frazzitta earned his bachelor's degree in Business Administration from the City College of New York in 1965.

Diebold, Incorporated is a global leader in providing integrated self-service delivery systems and services. Diebold employs more than 11,000 associates with representation in more than 80 countries worldwide and headquarters in Canton, Ohio, USA. Diebold reported revenue of \$1.7 billion in 2000 and is publicly traded on the New York Stock Exchange under the symbol 'DBD.' For more information, visit the company's Web site at www.diebold.com.

CONTACT: Bart can be reached at (330)490-5562.

First published on BankersOnline.com 10/1/01

Robbery: Advice For Tellers

Answers by Andy Zavoina and Dana Turner, BOL Gurus

QUESTION: What does a teller do in the case of a bank holdup?

ANSWER by Andy Zavoina:

[BIO AND CONTACT INFO](#)

Stay calm, cooperate, give him/her the money, be observant and sound the alarm after the robber has left the scene. At that point your internal procedures should kick in to notify law enforcement, management and to protect the crime scene.

ANSWER by Dana Turner:

[BIO AND CONTACT INFO](#)

A comprehensive policy and procedure statement/training guide -- one for staff and one for management -- is available in "[Bankers Tools](#) - Policies, Procedures & Position Descriptions".

First published on BankersOnline.com 12/3/01

Post-Robbery Procedures

Answer by Barbara Hurst and Dana Turner

QUESTION: What are the major problems for police investigators after a bank robbery, and different ways to prevent future robberies?

ANSWER by Barbara Hurst:

[BIO AND CONTACT INFO](#)

Major problems: (1) Not protecting areas the robber may have touched - counters, door handles, glass on doors that may have been pushed. (2) Too much conversation and comparing of visual "notes" before description of robber(s) is written down. Memory fades quickly with conversation. (3) Forgetting to try to get the license number and direction of the getaway vehicle.

Preventive measures: (1) Robbers almost always (99% of the time) case a branch before robbing it. If staff there is careless - ignores customers - does not make eye contact - is lazy and distracted - That's the branch they'll hit, every time. The one across the street with a greeter, people paying attention, interested in getting you in, business done, and out, is protected by its employees' behavior. (2) Equipment. Cameras - very visible, Man traps, bullet resistant glass in front of the tellers area. Any anti-robber equipment possible, short of arming the tellers! (3) Carefully adhered to security procedures when opening and closing the branch, servicing the ATM, or receiving a cash delivery. Robberies are on the down turn, a feather in the cap of our front line people and security officers and procedures.

ANSWER by Dana Tuner:

[BIO AND CONTACT INFO](#)

In addition to Barbara's reply -- and as an experienced robbery investigator -- there are some additional pitfalls:

1. Poor video quality resulting from the overuse of the videotape (3 times maximum);
2. Poor video quality resulting from the inappropriate placement of cameras (typically 30-50 feet is the maximum for identification purposes, otherwise the camera simply tracks movement);
3. Lack of an internal "crime scene commander" (someone needs to take command of the scene, coordinate internal resources, act as the intermediary for the police and secure evidence);
4. Lack of an approved "corporate investigative policy" and report template (the bank needs to conduct its own investigation, in addition to the police's); and

5. Lack of an approved "media relations policy" (let the police make all statements to the press).

First published on BankersOnline.com 10/1/01

Robbery Deterrence: Security Guards vs. Equipment and Procedures

Answers by Andy Zavoina and Dana Turner, BOL Gurus

QUESTION: I am the Security Manager and our branch office, located in a small rural town, has been robbed three times in the past nine months. In the first robbery, the robber wore a disguise and a gun was displayed. In the second robbery, no weapon was displayed AND the robber became nervous and just grabbed money from a customer and fled. In the third robbery, the robber wore a disguise, a knife was displayed and the robber went behind the teller line. There were at least a dozen customers in the branch at the time of the robbery. In all three robberies, the staff followed banking procedures, and there were no injuries.

Senior management and branch personnel want to hire an unarmed security guard for 3 to 6 months. I expressed my concerns that a security guard may provide the staff with a false sense of security, escalate the situation toward more violence rather than controlling or deterring the situation, and present many liability issues.

I have recommended the below listed action steps to deter a future robbery:

1. Install additional cameras (2 exterior and 1 at the rear entrance) and a monitor at the rear entrance. Approved by senior management.
2. Repair the locks on the doors leading behind the teller line. (The Branch never informed Maintenance the locks were broken.) Approved by senior management.
3. Consider renovating the interior of the branch to allow branch personnel to view customers entering via the rear entrance. (Currently, when individuals enter the rear door, they must walk down a hallway before they can be seen by branch employees. All three robbers entered via the rear entrance.) Senior management is currently considering this request.
4. Install dye packs at the teller stations. (We currently have just a motion triggered vault pack.) - Approved by senior management.
5. Close the rear entrance to customers. Require customers to enter via the front door. - This recommendation was flatly refused by senior management.

Note: We did meet with the local and state police to discuss possible action steps. Unfortunately, the police informed senior management they felt a security guard would act as a deterrent.

I am having a difficult time convincing senior management not to hire a security guard.

Your thoughts on this matter would be greatly appreciated.

Also, if you have any articles or statistics regarding the use of guards, I would appreciate receiving a copy.

ANSWER by Andy Zavoina:

[BIO AND CONTACT INFO](#)

I believe that a guard does act as a deterrent, although ours are armed.

Ensure that the guards are properly trained and they should avoid the lobby confrontations you are worried about.

ANSWER by Dana Tuner:

[BIO AND CONTACT INFO](#)

It's unfortunate that your branch has become so popular -- for all of the wrong reasons. You also might amend your statement that there were no injuries -- there are likely long-term psychological and emotional injuries. What you're describing is your need to develop a "security environment" -- one that's "offender-hostile" and yet "customer-friendly", with employee and customer safety as the first priority. Please consider these suggestions:

1. An effective security environment has five (5) logical components:
 - Employees and other institution-affiliated parties;
 - Customers and other persons likely to be on the premises, including vendors;
 - Facilities that you own or control;
 - Assets that are tangible and intangible; and
 - Records from internal and external sources.
2. The key to your question is employee and customer safety. The answer to the security guard issue needs to address both employee and institutional needs. Find out from your employees:
 - On a scale of 1 - 10, how safe do they feel after these events?
 - What additional training do they want?
 - What reasonable security enhancements would they like to see you put in place?
3. If your robbery training only deals with a "stand-up" robbery, you've missed several other types. Each type often requires different response procedures, including: (go to BOL's main page for 01-28-02 for the FBI's latest statistics on robberies):
 - Robbery using a weapon;
 - Robbery using a threat only;
 - Robbery using a note;
 - Robbery using a bomb or bomb threat; and
 - Robbery committed by several offenders (take-over).
4. Concerning your recommendations to management:
 - 1., 2. and 3. -- fine;
 - 4. Remove the "bill trap" connection and include a "homing device" if your local law enforcement agency can track it;
 - 5. Your recommendation is appropriate because this is a safety issue. Your senior management may bear personal liability if -- based upon historical issues that demonstrate that leaving this door open contributed to the robberies -- you continue to allow people to use this door.
5. Security guards may provide protection and defense -- but at what cost? Consider that there are three (3) types of contract security guards (four (4) if the guard is your employee):
 - Unarmed: inexpensive, and possibly useful for guarding property only;
 - Armed: moderate cost, and possibly useful for guarding property and persons; and
 - Off-duty, sworn law enforcement officers: expensive, most useful for guarding property and persons, liability borne by the agency and able to enforce the laws of your state while working for you.

I agree with your local law enforcement agency about the use of security guards -- with limits. Unfortunately, the Security Officer is often responsible for implementing unpopular or inconvenient processes -- and it's particularly unfortunate when he/she doesn't agree with the decisions made by others. Another BOL user posed a question to me last week that should be featured in next week's edition. Please check back next week for more information.

First published on BankersOnline.com 2/4/02

Robbery Risk: Multiple Entry Points Into The Building

Answers by Dana Turner and Barry Thompson

QUESTION: My bank's corporate office and branch are combined in one office building. The majority of upper management is located on the second floor of the building. The first floor consist of branch personal, loan processing and the collection department. Currently there is one alarm on the first floor, that is used for the entire building. My dilemma is that upper management would like to have an additional alarm on the second floor and be able to enter the second floor through a back door on the fire escape. I see this as a good way for a morning glory robbery to take place. Not to mention the safety concerns of the fire escape. The first and second floor are connected by an elevator. This would allow a would be robber to accost someone entering the building on the second floor and gain entry to the first floor via the elevator. Personnel on the first floor would enter the building without knowing a robber was inside. I would appreciate any additional points or statistics you could provide.

ANSWER by: Dana Turner

[BIO AND CONTACT INFO](#)

Your concerns are justified. Just for a second, transform your bank building into an airport. Would the airport allow passengers maintenance personnel and crew members to enter the gates just anywhere?

Every employee should enter the building using the same entrance. The second floor door should also be alarmed and covered by a camera, because of the elevator access to the first floor.

ANSWER by: Barry Thompson

[BIO AND CONTACT INFO](#)

Dana is absolutely correct with his answer to you. I once worked with a bank which had a similar problem and the President wouldn't allow us to control the door. In our case the door was inside the building on the second floor and unlocked. The staircase next to the door led down to a customer entrance lobby. Each morning the outside door was unlocked after 8 AM allowing customers to stand inside the building during bad weather. Another set of doors guarded the main lobby of the bank and were opened at 9 AM to allow access to the customers from the entrance lobby.

This was allowed until one irate customer used the staircase and door to enter the bank before opening hours. This incident provided enough incentive for the President to reconsider this security weakness.

First published on BankersOnline.com 11/5/01