management consultancy services | security division

Bank Robbery Deterrence

Bramston & Associates

we are driven by our aspiration to set the highest standards, to provide the best experience and to remain inspirational in the security field by sustaining our core principles - innovation, quality, service and value.

'Passionate about Security'

contents

Risk Assessment

Our goal is to provide your institution with a methodology to evaluate your robbery risk…

page 07

Robbery Deterrence

Robbery Deterrence provides you with a review of the various deterrence options that are available. Combined, these tools are designed to help you match your relative risk with the appropriate deterrence measures. Using the finest deterrence measures available, unfortunately, does not prevent you from being robbed...

page 12

Training and Education

Employee Training and Education provides a series of procedures to consider before, during, and after a robbery occurs....

page 22

BRAMSTON & ASSOCIATES
SECURITY DIVISION
Bramston & Associates
III D 007 Andrakaja Ambohidratrimo
Madagascar
Tel: +261 (0)32 68 12626
E-mail:mg@bramston.co
www.bramston.co/security

Foreword

When it comes to fighting crime, bankers are already carrying a hefty load. They are improving their fraud-fighting capabilities, cracking down on money launderers and now even helping in the search for terrorists. Unfortunately an old nemesis - bank robberies - appears to be making a comeback. Bramston & Associates provides this document as an highlight of our approach to assist bankers in evaluating their current bank robbery deterrence efforts. Financial institutions have had physical security programs in place for years, and have always recognized, first and foremost, the need to maintain the safety of their customers and employees during a robbery attempt. The industry has also always

- ☒ This brochure contains a set of resources to help you meet bank robbery deterrence challenge.
- ☒ It includes information on how Bramston & Associates conducts a robbery risk assessment, enhance your robbery deterrence strategies, train employees in what to do during a robbery, fine-tune your pre- and post-robbery procedures and communicate with the public and the media about robberies.
- ☒ We always keep in mind that during a robbery, a bank's number one priority is the safety of its customers and employees.

recognized the value in maintaining an active and ongoing partnership with law enforcement and other members of the community to deter bank robberies. Robbery deterrence efforts on the part of financial institutions have always been a balancing act between ensuring that the customer has an inviting environment in which to bank and putting in place the measures necessary to limit an institution's vulnerability to robberies.

Robbery Deterrence provides you with a review of the various deterrence options that are available. Combined, these tools are designed to help you match your relative risk with the appropriate deterrence measures. Using the finest deterrence measures available, unfortunately, does not prevent you from being robbed.

Employee Training and Education provides a series of procedures to consider before, during, and after a robbery occurs. The tool contains a robbery response kit that can be amended to suit your financial institution and community. It includes a checklist of things to do following a robbery, as well as a description form that captures the characteristics of the robber and the robbery.

Communicating About Robberies, recognizes that such protection measures do not end when the robbery is over, and that there is a role for your employee assistance program to ensure that your employees recover from any trauma they might have experienced during or after the event.

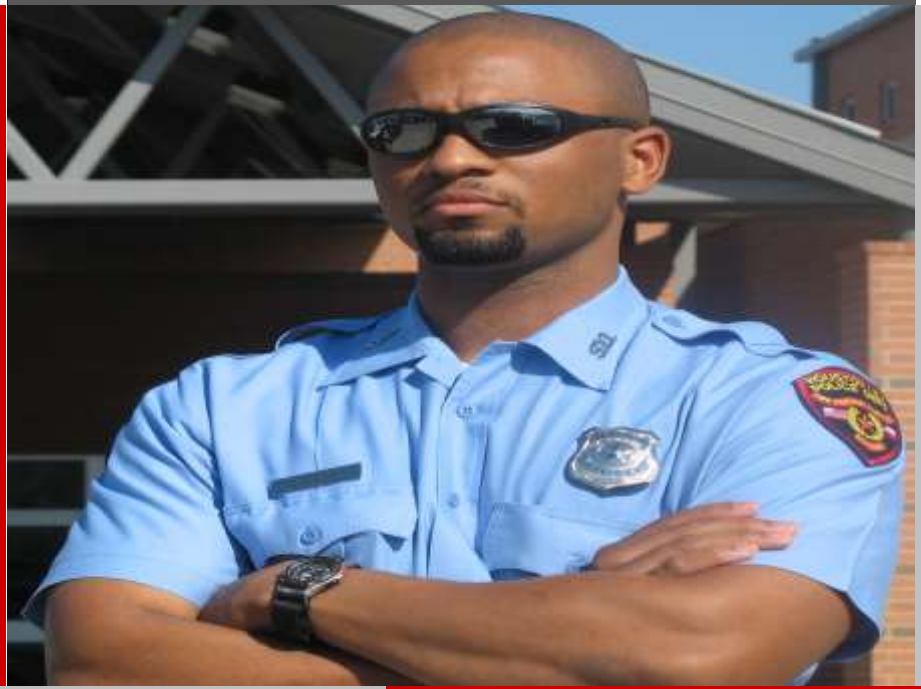
07

ASSESSING ROBBERY RISK

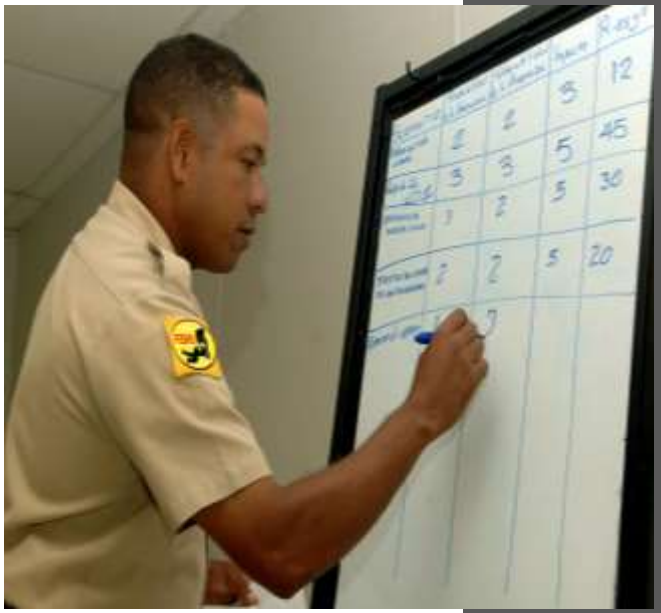
Physical Security Checklist and Inventory

Any assessment of robbery risk begins with an evaluation and inventory of the measures you are already taking as a financial institution. The following checklist and inventory provides your institution with some factors to consider when evaluating your security measures. This approach should be modified to suit your institution's particular needs.

For institutions with multiple branches, your institution can utilize the risk assessment provided within this document to develop a suggested survey frequency.



08



1. Windows

Are all windows secured in a manner that prevents staff from opening them from within the facility?

Are all windows properly latched and tamper proof/resistant?

Is the risk of intrusion low enough at this site that screens and/or bars are not needed on the windows?

2. Hatches and Vents

Are exterior hatches and vents secured to prevent unauthorized external entry? Note the type of lock in the comments section (padlock, etc).

Is the risk of intrusion low enough at this site that no external hatch requires alarm protection (i.e. door contact)?

Describe location of all key locks and alarm contacts that exist currently in the comments section.

3. Doors

Are all outside doors equipped with adequate locks to prevent unauthorized access after-hours?

Do all outside doors with external hinges have a security pin or screw?

Is the risk of intrusion low enough at this site that no latch guards are required to prevent tampering?

Are alarm contacts used on external doors, as necessary? Describe areas of missing protection for inclusion in final recommendation.

For solid doors or doors with blind spots, are cameras and a door monitor in place or is

a global “peep hole” installed?

4. Cameras

Black & White Video System/Color Video System or Mixed: b/w and color

Digital Recorder / VCR Recorder / 35mm Hard-Film System / 70mm Hard-Film System

5. Camera Coverage Areas Number

Entrance Doors / Exit-Only Doors / Teller Work Stations / Cash Work Rooms / Teller Cash Dispenser Chests / Teller Lines / New Accounts Desks / Drive-Up / ATM Transaction / ATM Chest Door / Night Depository and Room / Blind Areas at Remote Structures / Exterior

6. Adequacy of Camera Coverage

Are all cameras free from obstructions to their field of view? For instance, is there furniture, marketing, plants, etc. that block a camera's

view of the intended subject area?

Is the current surveillance coverage adequate? If not, note missing coverage.

Is there a routine for testing individual camera coverage?

During a robbery do all cameras accelerate coverage, or does one camera lock into the area of alarm trigger?

7. Alarm Activators

Is an alarm activator present at every location with access to cash (teller work stations, cash desks, etc.)?

Are there an adequate number of alarm activators on desks in the facility?

Are an adequate number of wireless pendants available for staff and in use (3 minimum)?

Is there a silent “panic” alarm or telephone in the main vault?

Is there a routine for testing individual units?

8. Perimeter Alarms

Exterior Door Contacts / Motion or Sound Detectors / Glass Break Sensors / Ceiling Sensors / Other

10

ASSESSING ROBBERY RISK

Robbery Risk Assessment Questionnaire

This questionnaire is designed to assist you in documenting the varying degrees of robbery risk that exist within your branch network. Each location, by its very nature, has a different risk profile. Developing an orderly approach to differentiating between your branches, in conjunction with inventorying your existing physical security measures, will allow you to determine if the level of security you have in place across your branch network matches your varying risks. In addition to surveying your own locations, security officers should visit other financial institutions in the area as well and discuss local crime concerns with the appropriate local law enforcement agency.

1. What is the total amount of monetary assets stored at this location?

2. Where is the financial institution office located?

3. Is the financial institution located in Restricted access area (specialty), Industrial District, Business/ Commercial District, Rural Area?

4. Is the location within ½ mile of a major thoroughfare highway?

5. Is the location within line-of-site of a governmental site?

6. Does this location have two or more public entrances:?

7. What is the visibility into the branch from the exterior, i.e., mirrored windows, number of windows and similar:

8. What is the comparative distance from the access point to the branch to the teller stations?

9. What is the comparative distance from the access point to the branch and a platform associate (FSR, commercial banker, etc.)?

10. How many psychological or physical barriers exist between the access point to the branch and the teller stations?

11. Is there a clearly marked transition zone between the public and private areas of the branch, i.e., clearly defined borders?

12. How many robberies has this location had in the past 12 months?

13. How many robberies has this location had in the past 36 months?

14. Have there been more than four reported incidents, (ATM robbery, assault, vandalism, night depository robbery) during the past 36 months at this location?

15. Has an injury occurred at this location as a result of a crime?

16. Is there obvious gang activity within 1000 feet of the facility?

17. Is there obvious illegal narcotics activity within 1000 feet of the facility?

18. Is there obvious vandalism and graffiti within 1000 feet of the facility?

Deterring Robberies

Individuals are primarily deterred from robbing a financial institution by the fear of failure, the fear of apprehension, or both. Deterrent factors can be successfully implemented against the vast majority of potential robbers. Some robbers, however, are not to be deterred for any reason and this section is not geared toward those. The best reaction to those situations is found in other sections of this document on training, coordination with law enforcement, and post robbery procedures.

Our ability to present deterrent

factors is extensive. We can reach the potential robber in a variety of ways – through the building or amplification of their existing knowledge and information, or by creating/giving them new knowledge and information. Past or existing knowledge would be the publicized accounts of failed robberies, capture, prosecution and incarceration of a perpetrator. New knowledge or information would be that which we give them as they approach, or enter, our branches. Consider the path the potential robber takes as he approaches a branch – first making observations outside of the branch and then the information he or she receives as they enter and are inside a branch, all of which we control.

☒ This material is presented from the approach a potential robber might encounter the information or stimulus. Using this method, we can progressively present the many potential deterrents demonstrating the cumulative effect they can have.

A. DETERRENCE TOOLS FOR OUTSIDE THE BRANCH

- ☒ Utilize the local law enforcement community through communication, cooperation and coordination to provide key deterrent factors, as noted below.
- ☒ Consider police & security patrols, both walking and vehicular as part of your deterrence program.
- ☒ Coordinate a weekly walk-in with the local force. It will not only create a visible presence, but also foster better communication, and cooperation.
- ☒ Vehicular patrols in the immediate proximity to a branch can be requested, supplemented with parking of off duty or, “out of service” cruisers in the vicinity of a branch.
- ☒ Notable security experts recommend the use of police officers as guards, following the doctrine that the best deterrent is the law enforcement officer.
- ☒ Supporting this consideration is the observation that while more costly, the deterrent effect is commensurate with that cost, and potential liability may be reduced due to the level of training, skill and experience the police officer will have.

Branch Site Selection, Layout and Design

- ☒ Choosing a site in a locale where the crime rates are better than other sites should help reduce the risk of robbery.
- ☒ Formulating a risk assessment of current and proposed branch sites by gathering crime rate data, as well as opinions from local law enforcement personnel.
- ☒ Investing in a geographic/socio-economic analysis of the locale can help with evaluation of sites.
- ☒ Designing a branch with the entrance in the front and full visibility including unobstructed glass panels and low shrubbery helps discourage robbers.
- ☒ Teller stations should be positioned far from entrance doors, possibly in the rear of the branch, forcing robbers to parade through the platform exposing their visual identity to many institution employees.

GUARDS: ARMED & UNARMED, LOCATION, APPEARANCE, COST

There are several factors to consider regarding the placement of armed or unarmed guards outside financial institutions, as noted below.

There are several regions where armed guards are considered necessary and have been in use for many years. It is usually in response to the violent nature and volume of robberies in those regions. This approach is effective against a vast majority of potential robbers.

The greater number of guns present in a particular area simply increases the probability of a gunfight occurring. In such cases, the possibility of serious injury and death becomes a reality.

Unarmed guards provide another level of deterrence, and may be more available, or versatile as a greeter while controlling costs.

The presence of unarmed guards will more likely lead to a de-escalation of violence.

Finally, the responsibility and liability issues significantly increase with the presence of armed guards. Some private contract guard companies simply will not provide armed guards.

SIGNS: ATTIRE, REWARD & COOPERATION PROGRAMS, ENFORCEMENT

- ☒ Signs at the door requesting the removal of identity-obscuring attire such as hats, hoods and sunglasses are increasing in popularity and use. A potential robber never wants to bring any additional attention to them by being the only person in a branch with a hat, hood, or sunglasses.
- ☒ Some institutions also do not allow backpacks or musical instrument cases inside the location.
- ☒ Other signage in use notifies patrons and potential robbers that the institution participates in reward programs in conjunction with law enforcement. Regular customers may become more observant while in the branch and those in the institution with knowledge of criminal activity may take advantage of the tip-line to earn a reward.
- ☒ Sign design, and location will determine effectiveness of this tool.
- ☒ While enforcement of such a policy can remain soft, simply the approach of a greeter, branch employee, or guard to address the issue should serve as a deterrent. If only one person is deterred then this low cost measure is considered effective.
- ☒ Finally, if a robber complies by removing disguising or covering articles, but follows through on their robbery, identification is greatly enhanced by the quality of photos. This can also be effective in witness identification that can be used to make a case.

B. DETERRENCE TOOLS FOR INSIDE THE BRANCH

Police: Employees, Roles

- ☒ The use of off-duty officers as part-time employees may have several benefits. These officers can recognize key robbery indicators, such as suspicious activity or behavior preceding a robbery regarding particular individuals.
- ☒ Additionally, such officers can provide immediate crime scene control for evidence preservation in the post robbery environment.

- ☒ Guards inside serve as a significant deterrent to potential robbers, while adding other useful elements of safety and security.
- ☒ Positioning internal guards is key. Placing them near the primary door, or lobby area so a potential robber must see and pass them can ensure their visibility.
- ☒ The guard inside can be used as a slightly more customer friendly presence through welcoming and/or enforcing branch policies regarding attire (e.g., hats or sunglasses).
- ☒ The location of these guards also affords them the opportunity to make observations should a robbery occur.
- ☒ Most considerations regarding the use of armed vs. unarmed guards also apply when guards are positioned inside rather than outside.

Greeters: Employees, Policy Enforcement

- ☒ Greeters also have a deterrent effect in that potential robbers do not want to have any interaction with someone who might be able to identify them. There are several ways to implement a greeter program, as noted below.
- ☒ Internally posted guards, as previously noted, have a significant deterrent effect, while also having the ability to enforce branch policies regarding attire.
- ☒ Employees may serve as greeters, and certainly would be more customer friendly. Employees can be assigned on a rotating basis instead of giving the responsibility solely to a platform representative. Employees encourage compliance with bank attire policies.

VIDEO MONITORS: TYPE, USAGE

Teller line monitors are positioned inside to display the customers standing in line, or approaching tellers, or platform personnel. The customer is reminded that they are on camera and a clear image of him or her is being obtained.

Teller line monitors should be wired to recorders whenever possible. Although there might be some cost savings with a closed loop, conversely if the camera is wired to a recorder there is an additional image of the potential robber.

Initial tests of these monitors suggest that when placed in sites consistently robbed, there is some reduction in robbery activity.

BARRIERS: ACCESSIBILITY, FULL & PARTIAL, FIXED & MOVABLE

- ☒ When considering various types of barriers, fully assess legal compliance with any Disabilities Act, accessibility, as well as the appearance they present to customers.
- ☒ Full bandit barriers are expensive and effective. Their emplacement creates not only greater security for personnel but also provides a sense of safety for them.
- ☒ When barriers are in place there is adherence to robbery procedures, such as early alarm activation.
- ☒ Ensure you determine whether your institution requires bullet resistant materials and evaluate whether the counter is resistant if you are adding bullet resistant barriers from the counter up.
- ☒ Evaluate the areas both above and below the teller counter when considering bullet resistant barriers to ensure maximization of safety and security.
- ☒ Partial barriers are a cost-effective approach to providing some additional security and deterrence where none might have previously existed.
- ☒ Fixed barriers are most common, and cost effective.
- ☒ To help with customer acceptance ensure that acoustics are sufficient for smooth communications by thorough testing.
- ☒ Movable barriers can be steel walls that rise in a teller area to segregate and protect employees.
- ☒ Those devices have had some success in somecountries.
- ☒ Some security professionals in the states have been somewhat concerned about the safety of those units that propel upwards quickly from the counter.
- ☒ These types of devices also represent costly, high-end solutions.

ACCESS CONTROL DEVICES

- ☒ There is currently much growth in their acceptance and use.
- ☒ Moderate and high-risk areas have been the primary recipients of these types of devices.
- ☒ Operationally, they effectively allow only one person to pass through the vestibule at a time.
- ☒ Often equipped with metal detectors they can lock down an individual automatically or manually as the need arises.
- ☒ While costly upon installment, they are obvious to all and serve as a significant deterrent. In comparison, the one-time cost may equal that of the annual cost of one guard.
- ☒ Obviously, when considering this type of device, its impact on customer flow rate into and out of the branch must be assessed.

C. ADDITIONAL TOOLS (FOR RESPONSE)

Common tools

- ☒ Alarms: Location, Testing, Integration
- ☒ Cameras
- ☒ Video Tape: Use, Maintenance
- ☒ Digital Video Recorders (DVRs) .

Dye Packs

The use of dye packs and their potential versus actual effectiveness is often debated. Seek advice from institutions that do use them as well as those that do not. Styles and configurations of dye packs continue to evolve and vendors will happily present a full spectrum of options. New “flex-packs” are quite authentic; however, savvy robbers often intimidate tellers by demanding no “exploding money”.

Locator Devices

There are electronic tracking systems on the market that use radio-transmitters to help locate robbers. These devices typically use a radio triangulation system to pinpoint the suspect’s position. These systems always require infrastructure using radio towers as well as cooperation from responding police, as the tracking devices must be installed in their vehicles. These can be very effective in apprehending robbers, however, the set-up requires cooperation among financial institutions and some financial investment.

Bait / Decoy Money

Used by many institutions to assist in prosecuting bank robbers as providing significant evidence that the currency was stolen from the victim institution. This requires some maintenance including an updated record of the serial numbers and a regular change of currency straps. Some institutions have opted for decoy money, which is not recorded and thus requires less maintenance. This security measure is intended more for loss reduction than for prosecution.

Intranet Sites

Internal Web sites can be set up to provide tremendous amounts of information very rapidly and inexpensively to your branch managers, once the Web site is established. Branch security procedures, employee awareness, bank robber wanted posters, security alerts, and security personnel contact lists can be easily managed through Web page programs.

Reward Programs & Internet Sites

Various clearing-house associations and trade associations offer reward programs. Many operate in conjunction with local or regional Web sites. Others prepare and distribute wanted posters to branches and are funded by the victim banks as a percentage of the individual losses they each experienced. Many “crime stopper” organizations are willing to place bank robbers on their wanted poster campaigns. In these cases, the distribution is widespread and the rewards are much smaller, making them an effective yet inexpensive aid in apprehension.

Employee Training and Education

24

BEFORE A ROBBERY

Before a robbery occurs, training can provide employees with the ability to think through their reactions, mentally prepare them for a robbery, and practice their response. Training should be provided on a regular basis, to ensure that the proper reactions are in place and clearly understood.

The following are topics that should be addressed in training programs offered to all staff working in a branch:

Branch security equipment, including alarms and camera systems, should be tested to ensure that all activation and warning devices are in good working order. Testing should include transmitting an alarm to the monitoring station to ensure that communications are functional as well.

Cash maintained in teller drawers should be kept to the lowest amount required to effectively conduct business. Excess cash should be transferred to the vault or another storage area as frequently as needed to maintain low cash levels.

Transfers of cash should not be on a fixed schedule.

Provide training on the operation of alarm devices. Every employee in the branch should know how to operate every alarm device throughout the branch. Although tellers might normally be working behind a teller line, they may find themselves at a desk in the customer service area. They should know the location of every alarm activation device, and how to properly activate the alarm.

Provide training on the monitoring process used for security alarms. Branch staff should know that the alarm does not create an audible signal within the branch, and know where the alarm is monitored. If the monitoring site calls the branch to confirm a robbery, branch staff should be trained on how to respond to the call.

Provide training on the operation of notification or warning signals. Employees in non-public areas of the branch should have some process to determine that the public areas of the branch are safe to enter. A warning light, for example, near the door of a break room should be interlinked with alarm activation devices. Branch staff should be taught to check the warning light, and be provided a way to determine if a robbery is in progress when the warning light is illuminated.

Prepare bait money, recording all serial numbers.

25

DURING A ROBBERY

Risk Management

- ☒ During a robbery, the following points should be covered with all staff working in the branch:
- ☒ Stay calm. Robberies are usually over very quickly.
- ☒ Comply with demands of the robber(s) and to take no actions that would place themselves or others in danger.
- ☒ Give the least amount of cash possible. Include the bait money previously prepared.
- ☒ Observe the robber(s) as closely as possible, noting their clothes, any jewelry, any scars or tattoos, approximate height and weight, and other identifying characteristics.
- ☒ If a note is used, handle it as little as possible, and set it aside as soon as it is read. Try to keep the demand note.
- ☒ Activate the alarm and camera system as soon as it is safe to do so.
- ☒ Once the robber(s) has left the branch, notify other employees that a robbery has occurred.
- ☒ As quickly as possible after the robber(s) have left the branch, lock all doors to the branch.

  If possible, note the direction of escape for the robber(s), including a description of any vehicle used to escape. Do not pursue the robber

America - Bramston & Associates LLC - 16192, Coastal Highway, Lewes, DE 19958, USA - Tel: +13023193828 - E-mail: us@bramston.co

Europe - Bramston & Associates - 4, Netherfield Road, Harpenden, Herts AL5 2AG, UK - Tel: +447760810487 - E-mail:uk@bramston.co

Middle East - Bramston & Associates - PO BOX 22793, SHARJAH, U.A.E - Tel: +971505583143 - E-mail:sh@bramston.co

Africa- Bramston & Associates - Raffles Tower, Cybercity, Ebene, Mauritius - Tel: +2302592488 - E-mail: mu@bramston.co

www.bramston.associates