



Keeping Your Eye on the Ball:  
**Maintaining a Focus  
on Facility Security  
in the Age of the  
Electronic Channel**

*by Randy Benore*

*Director, Physical Security  
Product Management  
Diebold, Incorporated*

*and Larry Black*

*Director, Financial Security Solutions  
Diebold, Incorporated*



# Table of Contents

page 3	<b>Why Security Should Start At Home</b>
3	<i>Renewed Threats</i>
5	<i>The Need for Consumer Trust</i>
5	<i>The Fight for Talent</i>
6	<b>Evaluating Your Facility Security Program</b>
6	<i>Where Are We Headed</i>
7	<i>Does Our Security Program Include The Right Solutions</i>
7	<i>What is The Cost of Poor Security</i>
7	<i>Are We Fostering a Culture of Security</i>
7	<i>Can We Make Fundamental Changes Today That Will Improve Security and Save Money?</i>
8	<i>Have We Identified and Protected Our Hot Points?</i>
8	<b>Identifying Hot Points from the Outside In</b>
8	<i>The Perimeter</i>
9	<i>The Drive-up</i>
10	<i>After-hour Depositories</i>
10	<i>Employee Entrances and Parking Areas</i>
11	<i>The Lobby</i>
11	<i>The Teller Area</i>
12	<i>Vaults / Cash Room Safes</i>
13	<b>The ATM</b>
13	<b>Maximizing Your Investment by Leveraging Technology, Service and Information</b>
13	<i>Employing New Technology</i>
15	<i>Supplementing the Security Program with Security Services</i>
15	<i>Finding New Uses for Information Generated by Security Tools</i>
16	<b>Trust a Security Partner to Enhance The Protection of Your Facility</b>

Even in the age of the electronic channel, the protection of bank and credit union facilities remains a critical component of a financial institution's security program.

Today's sophisticated banking delivery options have revolutionized the way consumers and businesses interact with their financial institutions. But although they're leveraging advanced ATMs, 24/7 call centers, online banking and mobile account alerts, customers and members still view the branch as the face of their financial institution. That's why, even in the age of the electronic channel, the protection of bank and credit union facilities remains a critical component of a financial institution's security program. A fresh, holistic approach to facilities security can help financial institutions stay ahead of would-be criminals to protect their assets, their customers and members and their employees.

Protection of the facility — the proverbial home of the financial institution — should be at the heart of any bank or credit union's security strategy

### **Why Security Should Start At Home**

Protection of the facility – the proverbial home of the financial institution – should be at the heart of any bank or credit union's security strategy. And that means all facilities – from the corporate office, to the hub that is the central branch, to the spoke of local branches, to remote ATM sites, in-store branches and all other facilities that are encompassed by a financial institution.

Today's economy is driving renewed physical threats. And it's making the need for consumer trust and the fight for talent more important than ever. At the same time, new tools and more sophisticated processes mean facilities security can be both more effective and more meaningful to the overall operation. Embracing a cohesive security strategy that includes considerations for all facilities will help mitigate threats, win the competition for customers and members and deliver cost savings for the entire enterprise.

As the struggling economy leads consumers to become more desperate to make ends meet, many experts believe 2009 will be one of the most active years for bank robberies in recent history.

### ***Renewed Threats***

The allure of profitable, high-tech crimes hasn't eliminated conventional attacks against banking facilities. As the struggling economy leads consumers to become more desperate to make ends meet, many experts believe 2009 will be one of the most active years for bank robberies in recent history. According to a story posted to [www.cnn.com](http://www.cnn.com) on Dec. 31, 2008, bank robberies already were on the rise in 2008 in many cities across the United States. In New York City, robberies grew by 54 percent leading the city's police commissioner to conclude that criminals have "turned [banks] into virtual cash machines."<sup>[1]</sup>



# Why Security Should Start at Home

## Renewed Threats

By Jan. 23, 2009, Tulsa had already fallen victim to seven bank robberies – 50 percent of the reported incidents during the previous year. A story in *Tulsa World* recounted a robbery, reporting: “It was Tulsa’s seventh bank robbery this month, bringing the total during the first 22 days of the year to half the number in all of 2008.” <sup>[2]</sup>

The heightened awareness of bank robberies is inspiring would-be criminals to find new ways to avoid apprehension. In Monroe, Wash., a suburb of Seattle, a creative crook leveraged Craigslist to find decoys to unknowingly help him get away with the crime he was planning. According to a story from Seattle NBC affiliate King 5 News, the suspect in the October 2008 robbery of an armored car parked outside of a Bank of America branch ran an ad on Craigslist, an online resource for local classifieds and forums for more than 550 U.S. cities. The ad offered a wage of \$28.50 per hour for “construction work.” Those who were hired were instructed to report to their first day on the job to a location just outside the bank branch. And they were asked to wear clothing that resembled the suspect’s, including a yellow vest, safety goggles, a respirator mask and a blue shirt. According to the story “...the robber had planned ahead. In case anyone was hot on his trail, he had at least a dozen unsuspecting decoys waiting nearby, which he recruited on Craigslist.” <sup>[3]</sup>

Attacks against financial institution facilities aren’t limited to the teller-line hold ups often depicted on television. According to the FBI’s Bank Crime Statistics for the first quarter 2008, other institutional areas involved in crimes included the vault/safe, safe-deposit area, office area, drive-up/walk-up, night depository and ATM. In a story on Dec. 5, 2008, about a recent symposium focusing on bank security issues, [www.securityinfowatch.com](http://www.securityinfowatch.com) reported that security directors at financial institutions said they are especially concerned about security at the ATM. The story identified larger, full-service ATMs that can accept deposits, count money and dispense cash as a primary target for attacks. “Those units...cost more than many nicely equipped sports cars and are filled with cash stores...and the loss of such an ATM is incredibly expensive to the bank – both in lost time of service, lost cash from within the unit and the cost of replacing this high-end piece of electronic machinery.” <sup>[4]</sup>

In addition to increased physical vulnerabilities throughout the facility, financial institutions must also be cognizant of various forms of fraud. While most of today’s fraud takes place online, old-fashioned check fraud and new account fraud still exist. In fact, a December 2008 story on [www.bankinfosecurity.com](http://www.bankinfosecurity.com) forecasted that check fraud will be one of the greatest risks to financial institutions in 2009. <sup>[5]</sup> According to the American Bankers Association Deposit Account Fraud Survey Report – 2007 Edition, attempted check fraud at the financial institution more than doubled from 2003 to 2006. The study, which is conducted by the organization every three years, revealed that the value of attempted check fraud against deposit accounts totaled \$12.2 billion in 2006. Perpetrators caused a total of \$969 million in actual loss for the financial institutions, compared with \$677 million in the previous study. The top three types of check fraud included return deposit items (38 percent), forged signatures and endorsements (30 percent) and counterfeit checks (28 percent). The study showed that approximately \$1 of every \$4 in check fraud losses were linked to new accounts. <sup>[6]</sup>



# Why Security Should Start at Home

## *The Need for Consumer Trust*

In the age of rampant mergers and acquisitions and the collapse of some of the country's largest and most well-known financial institutions, the fight for wallet share is fierce. Financial institutions must work harder than ever to facilitate the loyalty that will lead to customer and member retention. After all, it takes fewer resources to retain and grow a current relationship than to establish a new one. According to a February 2007 story in *ABA Banking Journal*, the cost differential is substantial. The story reported: "To put some numbers to it, the Council on Financial Competition estimates it costs between five and 10 times more to attract a new customer than to keep an existing one...Customers who are loyal believe the bank acts in their best interest on a regular basis and are most likely to remain with the bank to make additional purchases and become advocates." <sup>[7]</sup>

**Consumer trust is a core component of loyalty. And a financial institution's security — or lack thereof — can have a significant impact on that trust.**

Consumer trust is a core component of loyalty. And a financial institution's security — or lack thereof — can have a significant impact on that trust. It all comes down to the experience customers and members have with their financial institutions. An April 2008 story in *Bank Systems and Technology* cited a report by TowerGroup Senior Analyst Rodney Nelsestuen that identifies key enablers for customer retention. Nelsestuen asserts: "If banks remain mindful of key enablers, they should see a marked increase in net customers and expanded relationships with existing ones." One of those key enablers is the customer experience, "the customers' view of all interactions with the financial institution – including product, delivery channel, people, process and technology — across the entire relationship." <sup>[8]</sup> If delivery channels aren't secure, the relationship will be fractured, the experience will be compromised and ultimately, there will be consequences when it comes to trust and loyalty.

The security of the financial institution can also impact the value of one of its most important assets: its reputation. And that reputation is something that carries weight when consumers are selecting financial institutions. A 2008 survey of more than 1,600 consumers conducted by Compete, a Web analytics company that provides online competitive intelligence, ranked "past experience/reputation" as the third most-important factor in consumer selection of a financial institution. <sup>[9]</sup>

### ***The Fight for Talent***

Even in today's marketplace, the fight for the best talent is at a fever pitch. And with Baby Boomers set to exit the workforce at a rapid rate as they enter retirement, the competition will only intensify.



# Why Security Should Start at Home

## *The Fight for Talent*

Hiring the right people to deliver exceptional service is critical to the consumer experience. So the recruitment and retention of the best employees also helps ensure the retention of your customers or members. And while security may not always be considered in terms of workforce strategy, an employee's comfort with the safety and security of his or her work environment plays an important role in recruitment and retention.

Most employees have the expectation that their workplace will offer a safe environment in which to do business. This is true even in the branch environment, which is more vulnerable to violent attacks than other office facilities. That's why ensuring the security of a financial institution's employees should be a central component of security strategy, as well as one of the measurements used to evaluate the security program's ROI.

## **Evaluating Your Facility Security Program**

Just like any security function, a facility security program should be an ongoing, ever-evolving effort to protect a financial institution's assets. Such an ongoing program requires constant evaluation to identify vulnerabilities, assess the efficacy of the program and determine relevant enhancements or upgrades. A fundamental element of the security program, evaluation should begin with a few basic questions.

### ***Where Are We Headed?***

Security leaders should understand and plan for short- and long-term security needs. Creating a road map for the security infrastructure that anticipates and prepares for the evolution of the security program during a two- to four-year period can help ensure a financial institution makes the most of its security investment.

The first step in developing such a road map is the identification of clear, measurable objectives for the security program. Security objectives not only enable financial institutions to identify successes, they also provide the data needed to communicate return on investment to the organization. Gone are the days when security could operate in an organizational vacuum. In today's business environment, security should be addressed in terms of the ROI it will bring to the entire enterprise.

Articulating security ROI is one way to help ensure a continued investment in security. Financial institutions must view security not just as a tactic, but as part of the overall business strategy. Ultimately, security strategies and solutions should support the organization's overall vision, mission and values.

### **A few essential questions can help a financial institution evaluate its facility security program:**

Where are we headed?

Does our security program include the right solutions?

What is the cost of poor security?

Are we fostering a culture of security?

Can we make fundamental changes today that will improve security and save money?

Have we identified and protected our hot points?



# Evaluating Your Facility Security Program

## *Does Our Security Program Include the Right Solutions?*

Understanding the financial institution's security objectives and long-term road map will enable evaluation of the current security program. Security strategies and solutions should be aligned with identified objectives and should enable the financial institution to stay on track with its road map.

Many of today's security solutions are built on open architecture that enables the integration of a variety of technologies, allowing scalability and customization as a financial institution's security needs evolve.

### ***What Is the Cost of Poor Security?***

Skimping on security to minimize the operational budget isn't likely to deliver cost savings in the long run. Inadequate security measures could add cost for the organization in terms of lost assets, damages to the facility, injuries, lost productivity and impact on the financial institution's reputation and brand.

During a time when cost cutting is a top priority for many in the financial industry, security should be considered in terms of the cost savings it will deliver through thwarted robbery attempts, disabled fraud, elimination of the need for key replacement and more.

### ***Are We Fostering a Culture of Security?***

To ensure success in today's facility, security must go beyond the security department. Security management can be enhanced by fostering a security culture in which all employees are security aware and committed to protecting the company's assets.

A facility security program that engages all employees must include the development of security policies, procedures and practices; training programs; and tools to measure compliance.

### ***Can We Make Fundamental Changes Today That Will Improve Security and Save Money?***

A variety of enhancements to a financial institution's security program can deliver immediate efficiencies and cost savings, while improving security.

The first example can be found in the multiple combination locks used at the teller line, on safes and chests and in vault interiors. Today's branch utilizes as many as 30 combination locks in these locations. And many financial institutions invest in a third-party provider to periodically change combinations. They can lower costs by managing combination changes internally, or by upgrading to electronic locks.



# Evaluating Your Facility Security Program

*Can We Make Fundamental Changes Today That Will Improve Security and Save Money?*

Even with today's modern security technologies, many financial institutions still use keys to control who has access to their facilities and other assets. Keys are easily lost, stolen or retained by people who are no longer employed by the organization. Each of these circumstances would prompt the rekeying of the facility, and the resulting costs can add up fast.

Access control systems can eliminate the frustration of managing keys and the cost of rekeying facilities, while at the same time improving overall security.

Finally, many financial institutions still dedicate personnel to serve as vault attendants. While consumers expect their safe deposit boxes to be secure, they can be frustrated by the need to wait for a vault attendant to access their boxes. The implementation of self-service for safe deposit can add value for the branch and for consumers. Personnel who formally attended the vault can focus on value-added tasks, while consumers can gain immediate, secure access to their safe deposit boxes.

## ***Have We Identified and Protected Our Hot Points?***

Understanding hot points within the facility and building a security program that protects those hot points is integral to making the most effective, efficient use of a financial institution's security investment. Even the most robust technology deployments won't be effective if they're not being applied to the most vulnerable areas of the facility.

## **Identifying Hot Points from the Outside In**

Every bank or credit union facility has its own unique set of security threats and opportunities. Even so, a number of "hot points" are consistent from institution to institution, market to market, location to location. While a financial institution's individual needs may impact the way it secures these hot points, a variety of best practices can help guide the development of the security strategy. From outside at the perimeter to the variety of internal areas, people and devices that require protection, effective facility security is all about safeguarding the hot points from the outside in.

### ***The Perimeter***

Because there is less control of the environment surrounding a facility, the perimeter is often more vulnerable to criminal activity than other building zones. Even so, when it comes to protecting the perimeter, it's all about the basics.

#### **Common Financial Institution Hot Points Include:**

- The Drive-up
- After-hour Depositories
- Employee Entrances and Parking Areas
- The Lobby
- The Teller Area
- Vaults/cash room safes
- The ATM



# Identifying Hot Points From The Outside In

## *The Perimeter*

Taking a strategic approach to lighting, facility planning and equipment placement — aesthetic elements that might otherwise be overlooked — can help enhance security. Appropriate lighting can be a deterrent to criminal activity, and it can also help improve consumers' perception of security around the perimeter. In a story on [www.securityinfowatch.com](http://www.securityinfowatch.com), retired police commissioner Paul Evans talked about the impact lighting can have on security: "Better lighting reduces crime by up to 20 percent." <sup>[10]</sup> Exterior lighting should meet or exceed lighting specifications, which are governed by regulation in most states.

The configuration of the perimeter, as well as the placement of equipment, can also have an impact on security. Physical obstructions around a facility's perimeter can help harbor those with malicious intent. Points of entry and exit, as well as the areas surrounding ATMs and night depositories, should be free of such obstructions.

Strategically placed cameras around the facility's perimeter not only enable monitoring services and the capture of video that may be critical for the prosecution of criminals, they also help thwart criminal activity. Evans agrees, saying the addition of cameras can reduce crime by 3 or 4 percent. <sup>[10]</sup> Prime locations for exterior cameras include:

- Main entrance/front door to the financial institution
- Parking area closest to main entrance
- ATM locations
- After-hour depositories
- Drive-up lanes
- Remote employee entry/exit points
- Employee parking areas

## *The Drive-up*

Today's drive-up remains a primary form of convenience for both consumer and business banking. And it continues to be a hotbed for would-be criminals who aren't brazen enough to take their activities into the branch. Tools such as bullet-resistive (BR) products and two-way video can help enhance security in the drive-up.

BR products can help reduce the risk of burglary, holdup and vandalism at the drive-up. BR windows are designed to protect tellers who are in consumers' line of sight. And when used in conjunction with BR windows, BR drawers and pass-through trays can further enhance the security of the drive-up environment for both consumers and personnel.

Financial institutions can further mitigate risk to drive-up tellers by relocating them from the drive-up window to more secure locations within the branch. The introduction of two-way video can enhance security for tellers without sacrificing their level of consumer service. Installation of two-way video in each drive-up lane provides tellers with video of drive-up consumers while giving those consumers access to live video of the teller. Video capabilities also enable recording of drive-up transactions and can be leveraged to deliver on-screen marketing messages to consumers during down time, such as while they're waiting for tellers to complete their transactions.



# Identifying Hot Points From The Outside In

## *After-hour Depositories*

In today's 24/7/365 business environment, the night depository continues to be a vital component of business banking. Unfortunately, it also remains a prime target for robberies and other malicious activities. The use of cameras and alarm capabilities can help protect this vulnerable area from attack.

The use of cameras in conjunction with after-hour depositories can help discourage criminal activity and capture critical video in the event of a security breach. Dual cameras can offer views of both the depository chest and the surrounding exterior scene. Surveillance can record images from the front of the depository and from within the unit as envelopes or bags fall into the chest, creating permanent, visual transaction records. Connection to the facility's video monitoring capabilities can enable around-the-clock evaluation of activity at the depository.

After-hour depository alarms can be integrated into a financial institution's existing alarm system. A wide variety of alarm options are available, including door contact alarms, heat thermo alarms and seismic detectors. These devices can detect a wide variety of attacks, such as external prying, torching, hammer attacks and jamming of the drum assembly.

### ***Employee Entrances and Parking Areas***

Safety is a critical employee concern and one that has immeasurable impact on recruitment and retention for financial institutions. Adequate lighting and video analytics in key employee areas can help ensure optimal security.

Employee entrances/exits and parking areas can be primary targets for potential robberies, internal theft and other crimes. Similar to exterior consumer entrances and self-service areas, adequate lighting in key employee areas will not only deter potential criminal activity, but also foster a perception of security among the employee population.

A technology that is emerging for security applications, video analytics can be applied to help detect suspicious activity in employee areas. Utilizing parameters identified by the financial institution, the technology uses sophisticated software to analyze live or recorded surveillance video. Analysis detects differences between actual activity and activity that is identified as normal or allowed. It can then alert the financial institution to events of interest through actions such as triggering an alarm, alerting personnel via pre-defined protocols or gathering data for later review.

**Safety is a critical employee concern and one that has immeasurable impact on recruitment and retention for financial institutions.**



# Identifying Hot Points From The Outside In

## *The Lobby*

A financial institution's lobby is a key starting point for crimes that take place inside the facility. Interior cameras, strategically placed personnel and new technologies such as video analytics can help deter and detect crime in the lobby.

Interior cameras should be an integral part of a facilities security strategy. Key camera and monitor locations include:

- Lobby overview, including a lobby view monitor
- Each entry/exit door
- New accounts desk/area
- Monitor for view of lobby activity located in employee break rooms

The presence of personnel in key lobby areas often serves as a deterrent to criminal activity. Ideally, a security officer or greeter should be in place in the facility's lobby to provide ongoing observation of entry into the facility, as well as activity at the teller line. Similar to its utility for key employee areas, video analytics can be used to detect suspicious activity in a financial institution's lobby.

**A financial institution's teller area remains one of the most targeted — and the most vulnerable — areas of its facility.**

### ***The Teller Area***

A financial institution's teller area remains one of the most targeted — and most vulnerable — areas of its facility. Financial institutions must remain vigilant in their efforts to secure this area from traditional and emerging threats.

Location is fundamental to securing the teller area. Teller lines should be removed from front door entry points. And tellers should have visibility to access and departure routes to and from their lines. Branches with high cash and/or transaction volume should consider cash dispenser technology, which can reduce the overall cash exposure at the teller line.

The use of gates can help segregate and secure the area behind the teller line. In addition, cameras can deter criminals, as well as provide a reviewable record of activity in the event of a breach. A minimum of one camera is recommended for each teller station.

It is imperative that tellers have the ability to activate an alarm when needed. All teller stations with cash must have the ability to trip the alarm system in a safe and discreet fashion. Wireless hold-up buttons and bill traps can provide additional flexibility when securing the teller area. And hold-up buttons can also enhance security when installed at desks and in offices near vulnerable areas of the facility.

In the event of a hold-up, robbery or burglary attempt, a financial institution should have the ability to detain the perpetrator. All branches should offer a remote lock-down feature that enables the remote locking of front doors without requiring personnel to approach the doors.



# Identifying Hot Points From The Outside In

## *The Teller Area*

Security strategies can also be leveraged to thwart fraud at the teller line. Policies and procedures should be developed and enforced for verifying the identity of both consumers who are affiliated with the financial institution and those who are not. The use of biometric technologies — such as fingerprint programs or facial recognition — can be employed for verification and assistance in flagging suspicious consumers. According to a December 2008 study by Unisys, a worldwide information technology services and solutions company, consumers acceptance of such technologies is on the rise. <sup>[11]</sup> The biannual, global study into consumer attitudes about a wide range of security-related issues found that a majority of Americans are comfortable using common biometric technologies for authentication. More than 70 percent of respondents in a survey said they would trust banks and government agencies to ask them for their biometric data for identity verification. Respondents ranked fingerprint technology as their most-preferred authentication method, with personal passwords close behind.

### ***Vaults / Cash Room Safes***

While vaults and cash room safes may be more challenging targets for criminal activity than other areas of the facility, the sheer magnitude of the assets they protect mean they still require fundamental protection.

Because a vault is typically the only piece of equipment in the branch that will never be replaced, it's critical to select a vault that will meet the long-term needs of the financial institution. The efficacy of a vault is measured in terms of how long it would take to penetrate. Experts recommend a minimum of a Class II vault, which could keep a perpetrator at bay for 60 minutes — more than twice the duration of a Class I vault. Class II vaults that are UL-certified can store up to \$5 million.

Vault doors should be equipped with time locks that are regularly serviced. The time lock is critical to ensure no one can gain access through any lock manipulation whether manual or robotic.

Both vault doors and safes require alarm devices. At a minimum, they should be protected by door contacts and thermostat alarms. Additionally, cameras should be positioned at vault entrance/exit locations to enable monitoring of vault activity. If a walk-in vault is visible from the exterior, lighting can help thwart and detect criminal activity.

Financial institutions should consider self-service solutions — such as electronic vault attendants — to simplify the management of safe-deposit vault doors. Such solutions provide added convenience for consumers, and they eliminate the expense of a vault attendant, enabling branch personnel to focus on core competencies.



# Identifying Hot Points From The Outside In

## The ATM

**Three critical points of protection at the ATM should be considered as part of any facility security plan:**

Secure the consumer

Secure the ATM

Secure cardholder and transaction information

In today's financial environment, the convenience of the ATM has become a consumer expectation. And while ATM availability makes banking services more accessible for consumers, it also presents criminals with opportunities for attacks. Three critical points of protection at the ATM should be considered as part of any facility security plan.

- **Secure the consumer.** Security features such as ATM location, lighting, built-in cameras and mirrors can help protect the consumer from attacks at the ATM.
- **Secure the ATM.** Brute-force attacks against the ATM still take place. From drills to torches to bombs to trucks that can literally tear machines from their locations, resourceful criminals will use any means possible to gain access to the funds inside an ATM. That's why the hardening of the ATM — making it physically stronger to increase resistance to brute-force attacks — is so critical. The stronger the ATM, the more difficult it will be to compromise. The longer it takes a perpetrator to break into a machine, the more time law enforcement will have to respond once a security breach is detected.
- **Secure cardholder and transaction information.** The latest encryption technology is vital to ensuring the protection of PINs and sensitive transaction data.

## Maximizing Your Investment by Leveraging Technology, Service and Information

Employing new technology, supplementing the security program with various security services and finding new uses for information generated by security tools can enable financial institutions to maximize their investment in security.

### *Employing New Technology*

With the proliferation of technology, the threat to information assets posed by hackers, viruses and insider sabotage has become more prevalent. Information security solutions can help mitigate a variety of risks to a financial institution's data, some of which originate at the facility level. And, when integrated as part of a holistic security program, these solutions can also improve the efficacy of physical security solutions, such as those employed to protect the facility.

While physical security solutions focus on the hot points within the financial institution facility, information security solutions should protect sensitive information and the infrastructure on which it resides. Information security solutions can protect data, systems and networks by:

- Preventing breaches and threats before they happen
- Safeguarding valuable data
- Improving information technology security and compliance
- Identifying appropriate responses in the event of a security breach

Employing new technology, supplementing the security program with various security services and finding new uses for information generated by security tools can enable financial institutions to maximize their investment in security.

The next generation of monitoring and access control can enable a financial institution to gain more control over who enters its facilities and accesses its assets, as well as when the access occurs. Managed access control is a full-featured access control solution in which the software is “hosted” by a security provider. The solution not only enhances access control management, but it also reduces monitoring costs by consolidating access control and intrusion alarm monitoring through a single source. Financial institutions can leverage the monitoring and access control administration expertise of the provider and eliminate the need for investment in and detailed training about system software. Managed access control also eliminates the need for software maintenance agreements and full-time, in-house operating personnel.

Managed access control grants and restricts levels of authority and access to cardholders, controlling and limiting employee access to various areas throughout the facility. The solution enhances security by preventing the loss of information, inventory and equipment. And by restricting facility access, it also helps ensure the protection of the premises and employees from intruders and vandals.

In addition to offering financial institutions control of who enters facilities or accesses assets and when, the interoperability of the access control and intrusion alarm system can help reduce false alarms, as well as ensure the most efficient, appropriate alarm response. And with false alarm fees on the rise, alarm verification is critical.

The right camera and video recording technologies enable successful monitoring. And today, financial institutions have a variety of options. To ensure the longevity of the equipment and its ability to meet the facility’s long-term security needs, financial institutions should consider transitioning to IP-based solutions.

Internet Protocol (IP) technology achieves improved security results at a lower cost. IP enables physical security devices — such as digital video recorders, cameras, card readers and motion detectors — to communicate. Using IP, security professionals can deploy and operate these devices to accomplish video surveillance, access control, intrusion detection and other forms of physical security. The advanced technology also enables security practitioners to access security data quickly – from virtually anywhere. Options for how to view, record and analyze video are increased, and security information can be digitized, transmitted and stored via a network.

Regardless of the technology incorporated, the data provided by video cameras throughout the facility can be leveraged for a variety of analyses. Video analytics is used to review video for specific data, behavior, objects or attitudes. The technology can evaluate the contents of video to determine specified information about the content of that video. Such analysis can help identify potential security breaches and other unauthorized activity.



## Maximizing Your Investment by Leveraging Technology, Service and Information

### *Supplementing the Security Program with Security Services*

Outsourcing has become a valuable way for organizations to enhance their workforce. By partnering with a security integrator, financial institutions can take advantage of today's outsourced security solutions to make the most efficient use of their facility security staff and minimize their up-front capital investments, while enhancing security throughout the facility.

**Security outsourcing can help deliver cost savings, streamline operations and increase ROI for the financial institution facility.**

By outsourcing components of the security program to an integrator, financial institutions can utilize their personnel more effectively, enabling employees to focus on core competencies. This is critical in a branch environment in which up to 50 percent of the expenses support personnel. Security outsourcing typically embraces an operating model that allows for the addition of new security solutions with continually updated technology, without the traditional upfront expense. It can help deliver cost savings, streamline operations and increase ROI for the financial institution.

#### ***Finding New Uses for Information Generated by Security Tools***

Security tools and technologies can be leveraged to deliver value for other parts of the organization and ensure a continued investment in security. Devices such as cameras, which traditionally enable monitoring of various hot points to detect security issues, have capabilities beyond their role in security. When enhancing cameras through video analytics, they can also monitor consumer traffic/flow, assess the result of training initiatives and measure the effectiveness of marketing campaigns.

Similarly, data produced by a variety of security tools and devices can be leveraged through operational initiatives such as physical security information management (PSIM). PSIM enables the integration and analysis of information from traditional security devices and systems, and it presents the necessary data to automatically or manually resolve situations, real-time.

Traditional security solutions such as monitoring also can be leveraged to meet other operational needs. For example, energy management monitoring enables an operational focus on sustainability. Like its security counterpart, this solution utilizes devices that send signals to a central station. Those signals enable the tracking of facility resources such as lighting and heating, ventilation and air conditioning (HVAC). Just as traditional monitoring responds to signals that may indicate events such as intrusions, energy management monitoring responds to signals that indicate variances in facility temperature, illumination of lights or other energy-related measurements.

Relying on the same physical security strategies and solutions that have always protected the facility won't be good enough in an age that's seen a resurgence of bank robberies, an increase in attacks against institutional areas beyond the teller line and more sophisticated branch-based fraud.

### **Trust a Security Partner to Enhance the Protection of Your Facility**

Today's intense focus on high-tech security threats and information security may lead to neglect of the tools and techniques that can protect the brick-and-mortar facilities that still serve as the primary face of the financial institution. But relying on the same physical security strategies and solutions that have always protected the facility won't be good enough in an age that's seen a resurgence of bank robberies, an increase in attacks against institutional areas beyond the teller line and more sophisticated branch-based fraud.

A security integrator can serve as a trusted advisor and partner for the financial institution, collaborating with the in-house security practitioner to understand today's risks to the facility, identify hot points and introduce modern security strategies and tools that will ensure the protection of the financial institution's home.

---

#### END NOTES

- [1] [www.cnn.com](http://www.cnn.com). "Is Recession Behind Spike in Bank Robberies?" December 3, 2008.
- [2] Marshall, Nicole. "Another Tulsa Bank Robbed." *Tulsa World*. January 23, 2009.
- [3] [www.king5.com](http://www.king5.com). "Armored Truck Robber Uses Craigslist to Make Getaway." October 1, 2008.
- [4] U.S. Federal Bureau of Investigation. "Bank Crime Statistics (BCS) Federal Insured Financial Institutions: January 1, 2008 – March 31, 2008." October 17, 2008.
- [5] McGlasson, Linda. "10 Faces of Fraud: The Greatest Risks to Banks in 2009." December 9, 2008.
- [6] American Bankers Association. "Deposit Account Fraud Survey Report – 2007 Edition." November 27, 2007.
- [7] Michael, Nancy. "Customer Loyalty: How To Create Advocates." *ABA Banking Journal*. February 2007.
- [8] Bruno-Britz, Maria. "Keys To Improving Customer Retention." *Bank Systems & Technology*. April 28, 2008.
- [9] Marchione, Karen. "Top 10 Reasons Why Consumers Choose Their Bank." *Compete, Inc.* October 22, 2008.
- [10] Kohl, Geoff. "Symposium Sheds Light on Bank Security Issues." [www.securityinfowatch.com](http://www.securityinfowatch.com). Dec. 5, 2008.
- [11] Unisys. "Security Index Biometrics Study." December 9, 2008.