

# REMOTE VIDEO MONITORING



**A solid foundation for effective security measures in the financial industry**  
Safeguarding assets, meeting regulatory compliance and reducing operating costs for financial institutions

By Jacqueline Grimm,  
Director of Security Solutions  
Global Security Division,  
Diebold, Incorporated

## Introduction

Reducing risk through effective security measures is at the top of any business's list of priorities, but its importance in the financial industry goes without saying. While phishing, identity theft, malware and hackers are capturing the headlines, physical threats to financial institutions (FIs) are steadily rising, propelled by the economic downturn. The Federal Bureau of Investigation's (FBI) most recent bank crime statistics report 7,272 thefts against federally insured FIs in 2006 — up from previous years — resulting in more than \$70 million in lost cash, checks and property. Acts of violence and use of firearms are also on the rise, according to the FBI, and the most likely targets are branch offices of metropolitan banks.

But FIs have access to effective weapons that can help them to avoid becoming part of these statistics. One of the most reliable tools is remote video monitoring, which can be incorporated into existing security systems, unifying an institution's security components in a custom-designed system that operates quickly, efficiently and in real-time.

# The financial industry must remain diligent in employing the most effective security tactics available.

Remote video monitoring is even more valuable because of the changing criminal profile. In a struggling economy, desperate, ordinary citizens are committing burglaries, robberies and larceny, competing with seasoned veterans who traditionally orchestrate and carry out planned assaults. This shift has made identifying potential criminals a moving target. As part of this shift, the nature of crimes against FIs has become opportunistic and spontaneous, according to a 2007 U.S. Department of Justice study. The study identified three factors contributing to rising robbery rates, including the increased numbers of branches and banking outlets offering longer hours, the belief that FIs are a lucrative target, and the perception that robberies are quick, low-risk crimes. The FBI reports that crimes against FIs also are changing geographically, with increasing numbers of violent crimes taking place in rural areas, with community branches as targets.

2 Considering these shifting influences, the financial industry must remain diligent in employing the most effective security tactics available. This white paper explores the security challenges facing today's financial industry and focuses on how remote video monitoring can play a vital role in helping financial professionals safeguard assets and comply with regulatory mandates, while also realizing operational efficiencies.

## The Need for Proactive Security Measures

The threat of burglary, robbery, larceny, fraud, money laundering, and a host of other crimes at FIs is constant. While an FI certainly needs to protect its assets and investments, the FBI reports that more than 25 percent of physical security breaches also involve a firearm or other weapon. This means an FI is also responsible for protecting the safety and security of its customers and employees. Furthermore, a financial institution depends on its intangible reputation to protect and secure customer assets; security breaches can negatively impact an FI's image within the community and amongst customers.

FIs must therefore implement proactive security technologies to help protect their assets, people and reputation. By effectively monitoring activities 24/7 and in real-time and capturing vital video and

audio surveillance, FIs can create a proactive, integrated security system that protects their most important investments.

## How Remote Video Monitoring Can Help

One of the many benefits of remote video monitoring is that it can make use of existing security equipment in a new and more effective fashion, helping FIs to leverage existing security investments. This also helps institutions meet self-imposed profitability metrics and apply a powerful, more integrated approach to their current security systems.

With remote video monitoring, FIs can tie their most essential security components together through cameras and alarm triggers that can be positioned virtually anywhere and cued to communicate with a central monitoring station. Providing high-level security for vital areas, ranging from access control to off-site ATMs to processing centers monitoring, remote video monitoring embodies one of the financial industry's most effective, new security technologies.

## What is remote video monitoring?

Remote video monitoring takes video surveillance a giant step forward. It is composed of two-way, interactive audio technology that combines existing DVR technology and video surveillance systems with monitoring processes to provide real-time voice and video images to a central monitoring station for alarm verification and action.

With an Underwriter's Laboratories required reaction time of 45 seconds or better, central station dispatchers can quickly and remotely view and monitor a site when an alarm is triggered and communicate with anyone on-site. In an event-driven situation, dispatchers can send out assistance if the event is a detectable situation or prevent a false dispatch if no security breach has occurred. Once a situation is diagnosed, the dispatcher responds using a customized response plan that has been designed to meet the unique monitoring requirements of each FI location.

## How video monitoring works

No matter what the facility — a branch, off-site ATMs, check processing center or an FI's headquarters — any critical area at that facility is considered a contact point,

Through video monitoring, the number of opportunities to combine security events is greatly enhanced, which translates into greater opportunities to help prevent crimes from taking place.

which can be wired to a zone on a central alarm panel and paired with a video camera. Consequently, any contact point can be monitored 24/7 and programmed to immediately trigger an alarm signal that alerts the central monitoring center that a security event occurred at that specific contact point. Vital contact points include access sites for employees and customers, safes and vaults, server rooms, teller lanes and ATMs, as well as off-site facilities such as check processing centers.

Triggers can be set to trip alarms for doors opening or closing in restricted areas, people entering restricted areas, glass breaking, or any number of other events to include motion or heat. Because every facility's needs are different, contact points and triggers vary, resulting in the need for custom-designed security systems. Additionally, video monitoring technology is compatible with many manufacturers' control panels, allowing connection to existing systems often without the need to purchase new equipment and normally with only minor upgrades.

Through video monitoring, the number of opportunities to combine security events is greatly enhanced, which translates into greater opportunities to help prevent crimes from taking place. This technology allows for the immediate identification of the true nature of an event, which has a powerful impact on reducing the number of false dispatches as well as in helping capture and preserve vital information to assist law enforcement in tracking criminal activity and protecting critical assets.

### THE FINANCIAL INDUSTRY'S TOP CHALLENGES

Ask any number of financial professionals to identify their top challenges and the majority will agree on the following:

- Safeguarding assets
- Reducing false alarms
- Complying with industry regulations

### Safeguarding assets

Remote video monitoring helps FIs keep oversee interior and exterior operations any time of the day or night, and its presence alone can serve as a valuable deterrent to criminals. It also can provide a strong sense of safety for employees, which can translate through customers interaction. With remotely-monitored, strategically placed cameras at vital contact points, central station dispatchers can monitor the most important areas of a facility and, if a breach were to occur, provide accurate information to law enforcement to generate a quick and appropriate response.

Unfortunately, employees have been identified as common source for information leaks in many instances, both intentionally and unintentionally. The National Association for Bank Security lists some of the top ways these internal breaches can occur:

- Lost or stolen laptops, PCs or computer storage devices
- Backup tapes lost in transit
- Employees allowing access to information
- Employee theft of information
- Internal security failures
- Improper disposal of information

By placing cameras in sensitive areas, such as server rooms, offices, delivery areas, employee break areas, and throughout the parking lot, a FI can discourage the mishandling of customer information. Simply knowing live operators are randomly looking into a facility can encourage professional employee code of conduct. Remote video monitoring can also help to prevent costly mistakes that could result in released confidential information, by monitoring doors that are left open or laptops left unsecured.

Employee carelessness is only one way that personal information is leaked. In the financial industry, identity theft, network intrusions and other information breaches can be devastating for an institution's reputation. With cyber crime, it's important to understand that they usually begin with a physical security breach, which can be captured with remote video monitoring. With video monitoring equipment positioned to monitor specific, strategic contact points within a facility, a dispatcher can immediately be alerted if an unauthorized individual enters a secured area — a computer or server room, or offices where computers containing valuable

## The fees associated with false alarms can be overwhelming and vary by geography, but many FIs have reported fines upwards of \$10,000 per month.

information are stored — and if equipment leaves that area. Motion detectors paired with video cameras provide a powerful level of security by identifying who or what tripped the alarm when a contact point is triggered.

Protecting access areas also ranks high among the industry's security challenges — the presence of video monitoring can be critical. The FBI's statistics identify 9 a.m. to 11 a.m. as an FI's most vulnerable time, making video monitoring an essential component of opening any financial facility. Remote video monitoring can record and help identify exactly who enters the facility and at what time, and can capture such anomalies as someone "piggybacking" on an employee's credentials at an access portal or an employee entering under duress. If an employee has a problem entering the facility because of a lost or defective access card, a dispatcher at the central monitoring station can communicate with the individual, make an ID through an access code and provide entry, in many cases also avoiding a false alarm.

### Remote guard tours and look-ins

For the financial industry, an invaluable feature of video monitoring is the ability to perform round-the-clock proactive site monitoring through video-monitored guard tours, which can virtually mimic an on-site security guard making after-hours rounds. This eliminates the high wages associated with armed guards while providing eyes on multiple areas at once. During a video guard tour, central station dispatchers remotely walk through the facility, including its exterior, using a DVR and cameras to confirm all is as it should be. This type of monitoring is especially effective in safeguarding locations such as processing centers, which are usually located away from more trafficked areas. Guard tours can be programmed for specific times of the day or night, depending on each site's needs, and allow FIs to boost security without adding staff.

A similar video monitoring capability is remote look-ins. Again, configured to a custom-designed schedule, video look-ins can randomly move around a site during open hours as often as needed. This service can help keep employees alert and honest and have a similar

effect on customers. While neither guard tours nor remote look-ins are driven by actual security events, with cameras correctly positioned to protect the most critical areas, video monitoring has proven effective in curtailing robberies and securing sites, while reducing staffing costs.

For the financial industry, it's imperative to not only look in on an event taking place, but to ensure it is recorded. If a security breach were to occur, the availability of high-quality digital video and audio evidence can provide vital information that can assist local law enforcement in potentially catching the criminals. Video monitoring technology also enables video clips and sound bites to be digitally captured and shared with other law enforcement entities as the FBI or used as evidence in the courtroom.

### Reducing False Alarms

The fees associated with false alarms can be overwhelming and vary by geography, but many FIs have reported fines upwards of \$10,000 per month. Cincinnati, Philadelphia, Kansas City, Orlando, Dallas and Baltimore are just a few of the major U.S. cities introducing ordinances to recoup the costs of police dispatches for false alarms. According to the Center for Problem-Oriented Policing, police in the U.S. responded to about 36 million alarm activations at an estimated annual cost of \$1.8 billion, with false alarms accounting for 10 to 25 percent of all alarm calls to police.

Moreover, research performed by the Alarm Industry Research & Educational Foundation found that about 80 percent of all false dispatches are due to human error rather than robberies or burglaries. The foundation's survey results included a recommendation that commercial alarm systems be monitored by an industry central monitoring station, and for good reason. When an alarm occurs at an FI, police are automatically dispatched because robbing a bank is a federal offense, unless verification can be provided confirming a nonevent. During the day, when people are on site, verification is more readily available; but without remote video monitoring, FIs can pay dearly for recurring false alarms after-hours.

Moreover, research performed by the Alarm Industry Research & Educational Foundation found that about 80 percent of all false dispatches are due to human error rather than robberies or burglaries.

And, there are myriad of events that can trip after-hours alarms. In the financial industry, it's not uncommon for non-employees such as real estate representatives or financial advisors to meet at a site, driving up the potential for alarms to be triggered by the visitors mistakenly entering off-limits areas or setting off motion detectors. Additionally, after-hours workers such as employees, cleaning crews and maintenance companies can accidentally fail to disarm a security system upon entering.

Alarms also can be tripped after-hours by such innocuous sources as a large truck rattling the facility's doors and windows as it passes, or a forgotten balloon from a branch's special event floating by a motion detector. At just one false alarm per week, an FI with 10 sites can pay out more than \$5,500 a month. Implementing video monitoring services facilitates an immediate and appropriate response that can verify the false alarm, potentially reducing them by 30 to 50 percent.

#### HERE'S HOW IT WORKS:

A central station dispatcher receives an alarm signal from a monitored site. The dispatcher can quickly visually inspect the site and if necessary, listen in through two-way audio, which can assist in preventing a false alarm dispatch. Additionally, if there are workers or other individuals on-site who accidentally tripped the alarm and are instructed to not answer the telephone after hours, the audio system is broadcast over speakers, facilitating communication. By using the two-way audio system, the dispatcher can verify who is on-site with a personal code and circumvent a false alarm.

#### Complying with Industry Regulations

Incorporating remote video monitoring not only helps FIs meet the security challenges of today, but also ensures a security system robust enough to tackle new security issues as they arise. This means the ability to comply with evolving regulatory mandates, which according to Deloitte Touche Tohmatsu's 2007 Global Security Survey, is a top concern for industry professionals. In the survey, which included responses from thousands of financial professionals in more than 40 countries, security regulatory compliance is the only category that has ranked in the top five priorities for respondents in all five years since the survey's inception.

The industry's longest standing rules were published in the Bank Protection Act of 1968, which established the minimum standards for a security program, including mandating alarms and surveillance systems. Regulations were also established through such rules as Title V of the Gramm-Leach-Bliley Act, which developed Interagency Guidelines for Safeguarding Customer Information. Under this act, financial institutions are required to implement and maintain administrative, technical and physical safeguards for protecting customer information, which covers a range of banking operations from access controls to firewalls. In addition, the international Basel Committee, which formerly focused on an FI's loan portfolio, recently implemented the New Capital Accord, or Basel II. Basel II applies a scorecard approach that allocates capital based on an assessment of the quality of an FI's physical security, access control and other operational risks measured against established Basel II standards. Failing to comply can result in huge liabilities and significantly greater costs in the long run.

In light of these regulations, FIs must be prepared to show that their physical security systems are as effective as the security systems that have been developed for their online banking models. Adopting remote video monitoring significantly enhances an existing system by unifying the security components under a central monitoring station to provide a more integrated approach that can substantially strengthen the institution's overall security system.

# To help meet these challenges head on, remote video monitoring offers the next step in integrated security.

## Summary

Although cyber crime is capturing headlines, law enforcement data shows an alarming rise in physical threats against the financial industry in a broader geographical area and by a larger criminal demographic, attributed at least in part to the floundering economy. In addition, regulatory requirements continue to evolve that requires the integration of physical and logical security measures to safeguard FI assets and information.

To help meet these challenges head on, remote video monitoring offers the next step in integrated security. This service offers FIs the ability to integrate fully customized, alarm monitoring into existing security systems, to monitor all facilities in real-time, resulting in a proactive security strategy. Remote video monitoring is also invaluable in reducing false alarms, which are some of the top challenges financial professionals face. Offering numerous additional benefits, video monitoring provides the live audio and video necessary to secure any critical area of a financial institution, while capturing vital information to assist law enforcement.

## Authored by Diebold, Incorporated.

Diebold, Incorporated has been at the forefront of the security industry for nearly 150 years, and has been recognized as Frost & Sullivans 2008 Global Physical Security Systems Integrator of the Year for its expertise in physical, logical and electronic security. Diebold's event monitoring center, now in its twentieth year, has been named a Five Diamond, Level II 100 percent Operator Certified Central Station, which is a prominent designation awarded by the Central Station Alarm Association to less than one percent of U.S. security companies. Diebold also received the 2007 Central Station of the Year award by CSAA for its commitment to security monitoring excellence.

**For more information about Diebold, Incorporated and its monitoring capabilities for financial institutions, please visit [www.monitorsmarter.com](http://www.monitorsmarter.com) or call 1-800-248-2460, ext. 2566.**

Call on Diebold for the latest in product, service and security solutions.  
Since 1859, Diebold has put the customer first.

Contact Information:  
Diebold, Incorporated  
5995 Mayfair Rd  
North Canton, Ohio 44720

E-mail: [globalsecurity@diebold.com](mailto:globalsecurity@diebold.com)  
[www.diebold.com](http://www.diebold.com)

© Diebold, Incorporated, 2008. All rights reserved.  
Litho in USA. 04.08

**DIEBOLD**<sup>®</sup>  
SECURITY