



White Paper

Centralized Communications Increase Security and Reduce Fraud

***Integrated network platforms secure multiple
branches from a central locations***

Date created: 8/18/2010
Date modified: 2/16/2011

Table of Contents

1. Introduction	3
2. Balancing Increased Security and Strict Budgets	3
3. Finding Value in the Network	3
3.1 Advancements in IP Video Surveillance	4
3.2 IP Offers Affordable Access Control Solutions	4
4. Completing the Puzzle: Integration From the Ground Up.....	5
5. The Use of Analytics to Manage Video	4
6. Centralized Management	6
7. The Power of Voice Over IP	6
8. Conclusion	6

1. Introduction

Financial institutions rely on a variety of technologies to increase security and reduce fraud. On an annual basis, this market sector invests millions of dollars in complex security systems to limit risk exposure to robberies, fraud, theft, violence and more. Technologies include video surveillance to monitor real-time activity and record events for investigation, access control to monitor who enters and exits the building and other sensitive areas such as vaults, video analytics which alert operators to events such as tailgating, and alerts that go off in the event of an incident such as a break in.

The security industry has grown more sophisticated in recent years with the invention of IP-based technology. Yet, unfortunately most security systems still fall short in fully protecting against potential threats because they do not correlate critical data between the subsystems listed above. Without the ability to share critical data between these systems, security officers do not have a comprehensive view of their operations.

In response to this shortfall, fully integrated IP-based systems have started to emerge that incorporate the separate subsystems into one platform, available to the user right out of the box. Because all components are provided in one package, the unified approach is cost effective and easier to install, use and maintain.

This whitepaper will examine the features and benefits of the integrated approach to security and show the specific applications that will help financial institutions gain greater insight not only into security operations but business and marketing initiatives as well.

2. Risk Profile and the Current Financial Sector Environment

Fraud and theft are growing at a rate that financial institutions cannot keep up with. The American Bankers Association Deposit Account Fraud Survey collects information on various types of payment fraud losses. A 2009 study showed that check-related losses amounted to an estimated \$1.024 billion in 2008, up from \$969 million in 2006. The number of fraud cases also increased with 80 percent of banks reporting check fraud losses in 2008. The report also found that industry losses from debit card fraud — POS signature, POS PIN, and ATM transactions combined — reached an estimated \$788 million in 2008. ‘Friendly fraud’ in which the bank falls victim to fraud from its own customers is also gaining momentum in recent years. Customers will accuse a teller of not providing the correct dollar amount of a withdrawal or claims that a different amount was deposited into an ATM than the amount shown on the receipt. The number of robberies has remained consistent. The FBI’s 2008 bank crime report found that there were nearly 7,000 robberies reported in 2008, almost exactly the same number reported in 2007. In 2008, robberies cost the nation’s banks \$61.9 million in losses and 21 deaths. As bank networks evolve, so too does the risk profile. Recent studies show that customers rely more on ATMs to conduct transactions than typical brick-and-mortar branch locations. Banks are also placing kiosks and teller windows in grocery stores and shopping malls. With a changing of the way banks operate business comes new threats.

Yet while financial fraud and theft are on the rise, many security budgets have been slashed in recent years in response to a downturn in the economy. The number of on-duty security personnel has diminished and many institutions are looking to automate security operations in order to “do more with less.”

3. IP Technology Advances Security But Falls Short

IP based technology revolutionized the security industry. Two systems, in particular, experienced significant changes with the introduction of network-based technology: video surveillance and access control.

3.1 IP Video Surveillance

Video surveillance is the most critical component of an intelligent security system. It provides eyes into bank branches and corporate offices and can help manage the volume of people that enter and exit these facilities on a daily basis. IP video offers greater advancements over traditional analog systems such as:

- ▶ Real-time video monitoring from any location to enhance safety, protect assets and verify alarms.
- ▶ Centralized video monitoring of multiple cameras and branches from one location
- ▶ Higher quality images and feature sets
- ▶ Advanced data encryption
- ▶ Long-term savings in infrastructure and operational costs because financial institutions can leverage existing network infrastructure
- ▶ Future-proof systems enable easy expansion

With the recent introduction of megapixel and HD cameras, IP cameras far surpassed analog cameras in terms of image quality. When video management is operated over the network, remote video monitoring is possible, which enables operators to view video from numerous cameras from a single location. When coupled with video analytics, operators can react more efficiently if an alert is raised. If facial grabbing is enabled, banks can identify known perpetrators before an incident occurs.

3.2 IP Access Control Solutions

Fully networked access control systems offer enhanced security and flexibility over traditional lock and key sets. It is far easier and less costly to de-activate digital access cards from an online database than it is to replace keys and locks. Because the financial sector is moving through a consolidation period, this is critical because new access cards can be programmed from a central location rather than sending a team in to install new locks and new keys cut. Networked access control also identifies break-ins faster and has the ability to record a timestamp event when a door lock has been tampered with.

3.3 Shortcomings of IP Security

While IP technology elevated the capabilities of traditional security systems, the full power of these networked-based products were not realized until recently. IP-video, access control

and all other advanced security components were each purchased from separate vendors and therefore, operated in a siloed environment. The end-user, then, faced a decision: either operate each system on separate servers and through separate interfaces or contract an integrator to customize a solution so that these systems could communicate and share information. However, integration is both expensive and complicated and, in many cases, results in a loss of functionality. As a result, many banks chose to forgo critical components such as access control or video analytics to reduce capital expenditures.

4. End-to-End Solutions

Today, the security industry is moving toward a new approach to physical security, one in which systems are designed from the ground-up as completely integrated IP solutions that minimize the complexity of customized integration and leverage the power of the network. These integrated, IP solutions combine the essential components of a sophisticated system including video management, access control, video analytics, intrusion alerts and more onto a single platform. Instead of piecing together separate components from various vendors, these components can now be purchased together in a single package, installed all at once and operated through a single user interface. These solutions are also based on open architecture, enabling banks to integrate with other systems, teller transaction systems and ATMs.

Platforms that integrate these traditionally separate components from the ground up enable critical information from connected devices to communicate seamlessly with each other. For example, when a door is forced open, security operators receive an alert but also have the ability to pull up video from a corresponding camera all on the same interface. The security operator can then talk, utilizing VoIP capabilities, to an intercom or audio-enabled camera next to that door. Better yet, the door alert, footage and audio file can all be automatically recorded over the same interface for quick playback during investigations.

4.1 Analytics Effectively Manages Video

For small-to-medium-sized financial institutions such as banks and credit unions with limited resources, adding surveillance cameras is a cost-effective way to gather additional situational awareness and protect the bottom line. Video security provides operators with a window into various environments, both internal and external. However, more cameras lead to an influx in captured data that must be sifted through or monitored to find specific events. Conventional CCTV systems were never designed to accommodate the scale of modern installations, which today can include several hundreds or thousands of cameras. In order to manage the sheer volume of video, today's networked solutions embed various video analytics to help operators identify critical details quickly and effectively.

If 24/7 monitoring is enabled, video analytics automatically alert operators to areas where cameras detect motion or suspicious behavior. Remote control of cameras lets security personnel watch and control cameras in multiple facilities, not just cameras on-site. They can pan, tilt and zoom to get a better look at an incident in progress, such as a break-in or an armed robbery. With traditional CCTV systems, it is more difficult to catch crime as it happens by simply monitoring live video, more so when you take into account the number of

cameras installed and the sheer number of bank branches being monitored. Video analytics makes it easier to monitor incidents, store critical events, and retrieve evidence after the fact for forensic purposes.



Trip wire will alert operators when people or objects enter into a specific field of view.



Video analytics will send an alert when suspicious objects are left behind in a field of view.

Some of the activities video analytics can be used to identify include:

- ▶ Facial recognition to identify known perpetrators
- ▶ Suspicious behaviors in common areas
- ▶ Slip-and-falls to control liability
- ▶ People counting to manage staffing levels
- ▶ Loitering
- ▶ Entry and exit monitoring in secure areas, such as vaults
- ▶ Package left behind
- ▶ License plate recognition in drive-through lines or parking lots

6. Centralized Management

Another benefit to integrated networked systems is remote management, which provides users with the ability to access, configure and monitor all features of a security system from anywhere and at any time through a Web browser. Remote management greatly simplifies a facility's video surveillance operations by providing an interface to easily monitor a business' entire infrastructure from any networked location. A centralized security system enables banks to quickly approach also enables staff to quickly access recorded video, along with remote access to live and recorded video across its branch network from any location.

Furthermore, remote management enables users to access, configure and monitor all features of their security system from anywhere and at any time through a Web browser. Video is stored through remote backup, adding instant recovery capabilities that limit costly downtime.

7. The Power of Voice Over IP

With Voice over IP, operators can communicate with a site or branch from anywhere over the network, enabling them to speak through audio-enabled cameras that have a microphone or

speaker built-in or to an operator working at another audio-enabled monitor. VoIP also allows security teams to record audio files that correlate with video files for increased evidentiary support. Lastly, operators can record an audio file and have it playback through a camera speaker when triggered by an event. Imagine a break-in at a specific branch. The cameras can be set up to playback a message informing the culprit that the police are on their way.

8. Conclusion

Each financial institution whether it be a large mortgage firm, a local bank or a regional credit union has a unique set of security requirements but banks overall can benefit greatly from solutions that leverage the IP network and integrate multiple devices to work together. Fraud investigators can be more effective in solving cases by correlating information from video surveillance, access control, VoIP and video analytics together. As demonstrated, the power of the network and the integration of multiple subsystems offer greater possibilities than an analog system. When networked systems work in concert, it enhances situational awareness and enables operators to respond to situations quickly and more effectively. Incorporating best practices with solutions that are flexible enough to successfully evolve with changing requirements, integrate with existing and future technologies, and scale with evolving risk and needs are ideal for business in the financial sector, those of all sizes and risk profiles.