

# **Diebold Bylined Article for *Security Products Magazine***

## **COMPETITIVE ADVANTAGE THROUGH COMPREHENSIVE SECURITY SOLUTIONS IS IN REACH FOR FINANCIAL INSTITUTIONS**

**By Vincent Lupe, Director Global Product Management and Planning**

Worldwide events have forever changed our concept of security. Today we look at our personal safety with a new perspective, and organizations view their security issues with a new urgency. Organizations understand they can no longer continue approaching security in a largely reactive manner. Instead, to protect their people, resources and data from new risks, organizations must adopt a proactive approach. The challenge now is to aggressively find ways to anticipate security problems and keep them from happening.

Organizational change, particularly on this scale, is undertaken deliberately, and the move from a reactive to a proactive security approach still remains a work in progress for many industries and institutions. A 2006 survey by PricewaterhouseCoopers bears out this notion. Surveying nearly 8,000 respondents in 50 countries across all industries, including private and public sector organizations, the study found some security practices improving but, overall, slow progress.

Many leaders within the financial market know that a well-managed comprehensive branch security program – one including a convergent philosophy by way of the interoperability of physical and logical security – can result in lower risk, fewer losses, a brand reputation for consumer safety and, ultimately, a competitive advantage. For many professionals across the industry, investigating and implementing progressive, proactive security strategies is a daily mission.

### **INDUSTRY IN TRANSITION**

The industry as a whole, however, remains in the midst of transition. Some financial institutions may struggle with showing the value or competitive advantage that physical security solutions provide to their organizations. And though most correctly choose to

outsource security services, the practice of bidding instead of partnering with security vendors can result in disparate systems, decentralized accountability and does not provide for optimal integration.

Security systems are still essential for guarding cash, but are just as important in the achievement of regulatory compliance and protecting employees. While traditional crimes against branches – robberies, for example – are down, branches are increasingly the target of other types of malicious security attacks, including brutal attacks on ATMs, security breaches and fraud.

Amid this changing landscape, the financial services industry continues its attempts to approach security and operational risk management in new, more proactive ways. Success can be found by managing with a layered approach.

## **SECURING THE BRANCH FROM THE OUTSIDE IN**

Guaranteeing the security of a branch is becoming ever more complex. While branch and ATM banking offer benefits such as improved proximity to customers and greater organizational flexibility, they also add security concerns such as fraud threats and remote asset risks. An effective approach is to secure branches from the “outside in,” employing a layered approach consisting of six elements:

- Perimeter surveillance
- Interior hardening
- Access control
- Intrusion detection
- ATM security
- UL Certified Central Station

## **PERIMETER SURVEILLANCE**

With the exception of the ATM site, the traditional branch surveillance mindset has typically been concerned with interior perimeter coverage. However, it is just as important to recognize that there are several factors relative to external perimeter security that raise concerns for financial institutions, including parking lot activity, people

approaching the branch at night, and loitering or vagrancy in the ATM vestibule, just to name a few.

In today's world, digital technology provides a new approach to how surveillance can enhance both interior and exterior perimeter security and address these types of concerns. Some financial customers are leveraging this technology with software analytics to transform a typical camera from an image-capturing device to a security sensor that now provides an enterprise-level of integration to an event monitored solution.

### **INTERIOR HARDENING**

Notwithstanding the effectiveness of video surveillance, a layered approach to security demands further interior hardening. Vaults, day gates, safe deposit boxes, chests, night depositories and bullet- and fire-resistive barriers are critical to comprehensive branch security.

Advancements in barrier technology include concrete or super-strength modular vault panels and new composite chest designs. They are lighter and thinner than site-poured concrete vaults and therefore maximize floor space. They are also expandable. Some are available in virtually any shape or size, making them an attractive choice for keeping pace with changing needs for security.

Emerging technology for locking systems includes Internet Protocol (IP) and biometrics, which provide enhanced asset protection, operational efficiencies and electronic access control features at the container level.

### **ACCESS CONTROL**

A comprehensive branch security plan must also acknowledge that not all threats come from the outside. Therefore, modern vaults, safes and safe deposit boxes should be combined with electronic access control technology for maximum security. Much like video technology, access control technology can be used to grant or deny access and log who was where, and when. When integrated with building automation or HR

software, electronic access control can be utilized to enhance business operational efficiencies.

Emerging biometric technologies coupled with electronic access control also offer increased data protection, single sign-on capabilities, identity protection and fraud deterrence and detection. Electronic access has moved beyond the door and has matured into a modern day access environment.

Diebold's identiCenter™ offers an example of modern access control. identiCenter is a biometric security solution for financial institutions that uses an individual's fingerprint to quickly, securely and accurately identify account holders within a financial institution. Diebold's identiCenter uses proven fingerprint-reading hardware and software to address the threat of identity theft among consumers and financial institutions, a concern that affects 10 million Americans at a total impact of \$50 billion annually

In addition, identiCenter's full system can streamline branch traffic and improve customer service. Adding an optional kiosk and monitor enables an enrolled consumer to "check in" upon entering the branch by verifying his or her identity and selecting transaction options in advance of reaching the teller. The financial institution, in turn, provides customers or members with information about approximate wait time, their place in line, instructions about how to prepare for the transaction and more efficient, personalized service.

Diebold's PassVault™ offers another example. PassVault brings biometric innovation to vaults, enabling self-service safe deposit area access.

## **INTRUSION DETECTION**

Intrusion detection systems are often the last line of physical and logical detection. A variety of intrusion-detection technology is available ranging from magnetic contacts, glass-break detectors, passive infrared dual technology, activation devices such as bill traps and holdup buttons, smoke, sound, seismic and heat detectors, display devices such as sirens, bells, strobes and annunciation displays, to speakers, keypads and intercoms, and wireless devices.

Intrusion detection systems are moving from telecommunications networks to IP or network communication technologies, enhancing the layered security approach. The implementation of this type of security technology can also include an attractive return-on-investment proposition by lowering telecommunication expenses.

## **ATM SECURITY**

Attacks on ATMs have proliferated in recent years, both in sophistication and brutality. Criminals have grown smarter and more daring to defeat existing security measures, costing financial institutions millions of dollars.

Some ATM providers view security as just another add-on feature. Diebold is an example of a provider that has taken a different approach, starting with a thorough and exhaustive look at the different ways criminals attack ATMs. We listened to our customers and tracked the activities of criminals around the world. Then it designed a network of defenses to guard against each type of attack. Included are guards against some of the most sophisticated fraud attempts.

These defenses work together as a complete, integrated system that secures a financial institution's assets, protects its customers and prevents crime before it begins. Examples include:

- Intelligent card reader sensors
- Digital video transaction recording
- Digital security protection for the operating systems
- Video Analytics
- PIN encryption
- Physical-attack hardening of installed ATMs
- Consumer safety enhancements

## **SECURITY MONITORING**

For customers, monitoring ties a comprehensive system together. Monitoring provides continuous review of the effectiveness of any integrated security solution. Virtually any condition – the status of an alarm, safe, vault door or access control device – can be

monitored remotely over a robust communications network.

Monitoring services also provide continuous coverage with appropriate action plans for the huge volume of signals generated by openings and closings, night depository access, electrical failure and other events at both branches and ATMs. Central station monitoring reduces demands on support staff and helps reduce security costs.

Diebold's CSAA Five Diamond Certified Event Monitoring Center offers nationwide coverage in the United States, Canada and Puerto Rico. By partnering with Diebold, financial institutions have access to the latest alarm monitoring and video verification technology.

In addition, Revisor <sup>SM</sup> Online, a Web-based customer service application, enables Diebold's alarm monitoring customers to view and administer security operations at their convenience. These data allow customers to have tighter security controls over their account information and alarm activities. Customers are able to use these data to leverage false alarm fines, thereby allowing them to control costs more accurately and efficiently. The data help reveal a number of activities:

- Burglary
- Vandalism
- Holdups
- Employee duress
- Chest access
- Interruption in operation or unattended equipment

### **COMPETITIVE ADVANTAGE**

The world of security will continue to be dynamic. Financial institutions that deploy a well-managed, comprehensive branch security program built on a convergent philosophy can experience a competitive advantage. Financial institutions that carefully implement a layered security program will benefit from reduced risk, fewer losses and a brand reputation for consumer safety – a key ingredient to financial customer and member satisfaction.

**About Diebold**

Diebold, Incorporated is a global leader in providing integrated self-service delivery and security systems and services. Diebold employs more than 15,000 associates with representation in nearly 90 countries worldwide and is headquartered in North Canton, Ohio, USA. Diebold reported revenue of \$2.9 billion in 2006 and is publicly traded on the New York Stock Exchange under the symbol "DBD." For more information, visit the company's Web site at [www.diebold.com](http://www.diebold.com).