



▶ EDITOR'S COMMENTS.... 1



▶ Biometrics To Go 2



▶ An Eye on It All... 3

▶ Security Technology Needs Human Guidance 4

▶ Branching Out Security..... 5

▶ Looking for Driving Safety Tips?..... 8

○ ISSUE 1 | ○ VOLUME 5 | ○ August 2007

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

Welcome to the fifth issue of **SECURITY SOLUTIONS**. It seems that every week when you open the newspapers or listen to a news program you learn of horrific accidents on the roads. There is now widespread concern about the number of deaths that result from these vehicle accidents. At Amalgamated we see our role as helping to keep you secure from all types of harm. In this issue we have included an article that provides [Driving Safety Tips](#).

It is now widely accepted that businesses must control access to and within their premises. This is however seen as a security issue but the new generation of Access Control can help improve a company's profitability. [Biometrics To Go](#) gives examples of the bottom line improvement experienced by one type of business.

Who knows when your alarm

has been triggered? Over the years the answer has become, your monitoring station. We are now moving towards, Who sees when your alarm has been triggered? The article, [An Eye on It All](#), shows how monitoring stations are now incorporating video into their service offerings.



Terrorism in all its forms is making us rely increasingly on explosives detection devices. The article [Security Technology Needs Human Guidance](#) identifies some of the new technologies.

[Branching Out Security](#) addresses some of the issues that financial institutions must consider in their security planning.

If any additional persons in your organisation would like to receive this email newsletter, just send an email to newsletter@assl.com with the words "Subscribe Newsletter" in the subject line and the email address, name and organization in the body. To opt out of the mailing list send an email with the words "Unsubscribe Newsletter".

Brian Ramsey
Editor

Biometrics To Go

By: *Bashar Masad*



CONTRARY to using badges, sign-ins or other ways of tracking employees, a biometric reader ensures no employee can punch in for another, eliminating time fraud and reducing payroll costs. Because every person's biometric features—hand, fingerprint, eye or face—are unique, a biometric time clock provides a quick, accurate and reliable way to record in and out punches for each employee. That's why so many companies, including fast food restaurants, now employ biometrics.

A biometric reader ensures payroll accuracy by simply requiring each employee to be present—no cards or other credentials are needed. Losses due to buddy punching are eliminated. Using scheduling restrictions, unauthorized early-in and late-out punches are eliminated. The hardware also is typically less than 10 percent of the overall cost for a time and attendance system so biometric readers can be affordably placed in multiple locations. With biometrics, many companies report savings of up to 5 percent of total payroll cost.

Sweet Paybacks

Alliance Management in Avenel, N.J., a Dunkin' Donuts franchisee with stores in Middlesex, Mercer and Cherry

Hill counties, is using biometric readers in 27 of its stores, with three more pending, to record time and attendance information for more than 300 employees. The readers automate time recording and control labor costs.

"We were using timecards, but had numerous problems with them, including employees losing cards. Plus, our time clocks were old and had to be replaced," said Margaret Hanna, office manager for Alliance Management. "The new HandPunch readers have made payroll much easier. We have saved money and received payback within months."

"This Dunkin' Donuts franchisee wanted more accurate, automated record keeping and to control labor costs," said integrator Fred Overbeck of Automated Time Concepts of Glen Head, N.Y. "The stores have lower-paid employees with a high turnover rate, and the franchisee was concerned with buddy punching."

Overbeck said he believes in hand geometry technology.

"Hand geometry readers are the most reliable and easy to use," he said. "Finger-scan readers are not consistent, plus the HandPunch is more tolerant to subtle changes such as sugar- or dough-coated hands."

Now, instead of filling out or punching timecards, employees at Dunkin' Donuts shops simply place their hands on the HandPunch. It automatically takes a 3-D reading of the size and shape of the employee's hand and verifies the user's identity in less than a second. Employees use the units twice a day to punch in and out. Store managers edit punches and forward pay files to the company's in-house payroll department, which uses QuickBooks. Payroll is done bi-weekly.

"Problems we were having with the timecard system at Dunkin' Donuts have been alleviated,"

Hanna said. "The first and last thing an employee does each day is go to the HandPunch. All employees use it, including office administration. We now get our time sheets and time reports all on one sheet. The biometric system is much easier to use. More importantly, we've had no complaints or problems with the readers."

Biometrics Goes Global

In Venezuela, 85 McDonald's restaurants are cutting payroll costs by up to 22 percent annually after incorporating biometric terminals. More than 3,400 employees have been enrolled in a biometric time clock system in the past four years. On average, the system generates more than 7,500 transactions each day, resulting in 2.5 million punches annually.

"McDonald's moved to biometrics because officials wanted to verify that the employee clocking in was really that person," said McDonald's Brenda Morales. "Students make up about 90 percent of the McDonald's workforce in Venezuela. They were frequently punching one another in to cover for exams or other school-related events."

"A card only verifies a card. We have used finger scanning for other applications, but we believe that hand geometry is more effective and produces fewer errors when there are larger employee populations. With hand geometry, a larger area is scanned than with finger scans, and the template is updated after every scan so it remains current."

As fast food restaurant managers have discovered, biometric-based systems have many benefits. There are no badges to issue, replace when lost or stolen, or recover when an employee leaves or is terminated. Their hand is their badge. The system helps curb problems of employees buddy punching for friends. After a biometric reader is installed, many companies are stunned to discover how much buddy

punching actually costs them. And there is no more data entry errors when calculating payroll or recording attendance. A plug-and-punch feature enables some readers to be installed in less than 15 minutes.

Supervisors at each McDonald's franchise, who also clock in and out each day on the terminals, now use the HandPunch terminals to authorize and verify employee time and overtime on a computer located at the store. The hours are sent to a central payroll processing center via a phone line.

"Most supervisors at McDonald's are promoted from within, and many find it difficult to impose rules and restrictions on their fellow workers," Morales said. "The use of biometrics ensures that everyone is treated the same and fairly. McDonald's employees are satisfied with the HandPunch because payroll information is processed quickly and without mistakes. They receive regular reports with information about time and attendance."

According to Morales, language is not an issue because the software is in Spanish, and the readers accommodate several languages.

As fast food restaurants have found, biometrics ensures that employees earn a day's pay only when they are present to do a day's work. Whether the restaurant franchisee has 50 or a thousand employees, biometric-based time and attendance terminals produce more accurate payrolls and reduce labor costs. The technology also cuts operating costs and increases employee convenience by eliminating the need for badges—all while enhancing the bottom line.

About the author: Bashar Masad is a senior product manager at Ingersoll Rand Security Technologies. He is a member of the International Biometric Industry Association

Security Products June 2007

An Eye on it All

By Bill Fitzhenry

IN an age when the need for increased security services is at an all-time high, managing security information has become more efficient, flexible and powerful. Monitoring companies continue to deliver products and services to address those needs.

"The world of security is changing, and HSM's eServices are playing a key role in the 21st century security industry. Our customers and the marketplace have told us that. And by partnering with customers to understand their specific security needs—across the entire spectrum—we are better equipped to enable them to better manage their security efforts," said Tony Byerly, senior vice president of sales and national accounts for HSM.

HSM Electronic Protection Services, for example, has introduced eVideoManager video monitoring services and eVideoData real-time online access to video recordings and associated alarm event data. The two products are designed to help manage risk, reduce costs and increase the efficiency of a company's security operations.

Felix Gonzales, vice president of strategic initiatives and business development at HSM, said the company continues to focus on services that help customers better and more profitably run businesses.



Real-Time Reaction

In direct response to customer demand for video monitoring services and real-time access to security information and video images, more monitoring products are popping up in the marketplace. Services used in a UL- and FM-approved monitoring facility with a disaster recovery backup facility are better equipped to respond when needed. A portfolio that includes video alarm verification, video guard tour, video opening/closing services and video escort can provide a real ROI for its customers. There's always a need for increased security and safety from real-time, live support services, and a means to reduce false alarms. Monitoring services can help reduce guard costs and improve guard patrol efficiencies. Some tools also are designed to reduce inventory shrinkage/loss and improve employee productivity.

To ensure a compatibility with existing CCTV systems, some services can be used with existing customer intrusion alarm systems while compatible with most customer communication paths, including DSL, cable, LAN, Ethernet, dial-up or cellular.

Online access to video recordings for monitoring services such as alarm verification, open/close services, guard tour and escort allows customers to view what they want when they want. Video recordings are displayed with the associated alarm event data and are stored in an IT database available online from anywhere to customers.

"The days of paper or data-only reports are gone. eVideoData allows the customer to see data and view associated video clips of events, all in an online format stored on HSM's network," Gonzales said.

eVideoData offers alarm event reports that provide alarm data and a recorded video of the associated event and real-time access to video recordings on the same screen--a means to store and organize video recordings and alarm data and view and share the information.

Managing Video

Customers using monitoring services will see benefits such as reduced false alarm dispatches and increased security by having video monitoring specialists viewing activity in real time.

"Our customers asked us if we could develop a service that enhanced the power and benefits of eVideoManager by making recorded data and images available together and on HSM's existing eServices platform," Byerly said. "Thus the creation of eVideoData, which now takes video monitoring and online data to a new level--it's as simple as point and click from anywhere, anytime."

Customers see value in the added time and cost savings granted by monitoring services. Many services, for instance, are easily accessible via the Internet. Gonzales said that HSM's eServices platform allows customers to view alarm data and embedded video recordings of events online while still having all that information stored in HSM's IT network.

Continuing to Improve

Many companies in the monitoring business are constantly expanding their product offering, tweaking and perfecting existing services while planning for innovative, new products.

"The customer appetite for these type of offerings is huge once they see the plenitude of information available in an easy-to-understand and accessible format," Byerly said.

"Our customers wanted the capability to view their video recordings and alarm data together," Gonzales said. "eVideoData will put an end to searching your computer for e-mails or files for video and alarm events. Available online and at their fingertips, customers will now have everything they need to review or investigate an event."

Customers need an efficient way to view, share, store and retrieve video recordings with the added convenience of embedded alarm data on the same screen online, anytime and anywhere. Current monitoring services are designed to enhance conventional alarm monitoring process by providing real-time, live monitoring support for alarm

verification and open/close services. Moreover, monitoring services augment the traditional guard service process by providing a means to document activity, improve patrol efficiencies and reduce guard costs.

Reprinted from Security Products

February 2007

Security Technology needs Human Guidance

Diverse, accurate methods for detecting bomb material and improvised explosive devices (IEDs) are entering the marketplace, but even when fully automated or integrated with each other, these technologies offer little protection without personnel trained to think like the adversary, say industry and research experts.

"The advances we're seeing in detection technologies are impressive, and it's an area where people are trying to fully automate the process, but, at the end of the day, security is human-based," says Amotz Brandes, a former Israeli soldier and currently director and managing partner of Chameleon Associates, Canoga Park, Calif., a security consulting firm.

"Automation and integration of these technologies? That's great -- go for it. But in most cases it doesn't work [to prevent a security breach or event] without the human dimension and a shift in thinking toward the possible incident as opposed to the historic one," he told Defense News.

Brandes and other experts addressed

a one-day conference of government and industry security officials to review the latest techniques for detecting bombs and their perpetrators.



"A lot of new technologies have been coming onto the market and we need to look at them," says Yves de Mesmaeker, secretary-general of the European Corporate Security Association.

The technologies reviewed during the conference, according to Defense News, ranged from the mundane, such as systems for scanning the undersides of vehicles, to the exotic, such as an analysis of human convection plumes -- the small cloud of heat a body releases -- to new uses for older technology like X-rays and microwaves. For instance, GE Security has developed a stand-off vapor-based trace detector that gets around the civil rights problem of taking direct-contact samples from people. "Vapor detection is designed to move [the sampling problem] away from the person toward fingerprints, items and clothing," says James Copeman-Bryant, GE Security's technical services director in Europe for Homeland protection.

His company's new Ion Track detection station extracts and vaporizes minute particles from a human convection plume, and uses spectrometry to determine their composition -- all within a few seconds per scanned person. Due to its high sensitivity and ability to detect both positive and negative

ions, the procedure analyzes a wide range of vaporized explosive materials, "about 95 percent of what's out there," he told Defense News.

Asked by de Mesmaeker what the remaining 5 percent was, Copeman-Bryant says it included material such as gun pellets or smokeless powder. "But a terrorist would have to carry a lot of that stuff to bring down an airplane or border post," he says.

Other new IED- and explosive-detection systems combine advanced computer power with conventional technologies to produce similar rates of accuracy.

SecuScan, manufactured by Signalbau Huber of Munich, scans the underside of moving vehicles to produce images with detail down to 5 mm. Paired with license-plate data generated by partner TopGuard of Eindhoven, Germany, it compares a returning vehicle's newly scanned image with its previous one to detect alterations. SecuScan is deployed in Afghanistan and sites across Europe.

Another example of squeezing better results from older technology is terahertz (THz) imaging. "There's been a lot of confusion about THz capabilities," said Mikael Karlstrom, vice president for product engineering at ThruVision, near Oxford, England. "U.S. agencies concluded that THz-based imaging doesn't work, but that's because they mainly looked at laser-based THz imaging." Karlstrom said the THz range used by ThruVision's system instantly produces a passive scan of the human body from up to 12 meters away that detects threats under clothing layers, but without seeing through people or revealing anatomical detail. Before the end of 2007, he said, the company should offer a ruggedized version with a

stand-off detection capability in the 15- to 50-meter range. Despite the increasingly sophisticated science deployed in detection systems, Brandes reiterated his warning about over-reliance on technology to diminish terrorist threats. "One can still reshape TNT into a statue of Jesus or a dinner plate. Your machine might detect the material, but someone has to recognize the threat," he said. "Don't forget that the adversary is not standing still. They're probing these systems and new technologies all the time to find the vulnerabilities. You have to think like they do."

Reprinted from

DefenseNews.com

June 2007

Branching Out Security

By Vincent Lupe

WORLDWIDE events have forever changed the concept of security. Today, people look at personal safety with a new perspective, and organizations view security issues with a new urgency. Organization officials understand they can no longer continue approaching security in a largely reactive manner. Instead, to protect 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 the issues from occurring.



Organizational change, particularly on a large 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 public and private sector organizations, the study found some security practices improving—but overall slow progress.

Many leaders within the financial market know a well-managed, comprehensive branch security program—one including a convergent philosophy 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 seeing the value or competitive advantage physical security solutions provide. 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 helping the facility maintain 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 From the Outside In

Guaranteeing branch security is becoming more complex. While branch and ATM banking offer benefits such as improved proximity to customers and greater organizational flexibility, it also adds 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 perimeter surveillance, interior hardening, access control, intrusion detection, ATM security and a UL-certified central station.

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 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.

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

Even with 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. The design is not only lighter and thinner than site-poured concrete vaults but it also maximizes floor space.

In addition, the vaults are expandable and some are available in virtually any shape or size, making it an attractive choice for keeping pace with changing security requirements.

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

Blocking Access

A comprehensive branch security plan also must acknowledge not all threats come from the outside. 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, deny or log user access. When integrated with building automation or HR software, electronic access control can be used 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/detection.

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. The product uses fingerprint-reading hardware and software to address the threat of identity theft among consumers and financial institutions—a concern affecting 10 million Americans a

year and a \$50 billion financial impact.

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

Minding the Intrusion

Intrusion detection systems are often the last line of physical and logical detection. A variety of intrusion-detection technology is available, including magnetic contacts, glass-break detectors, passive infrared dual technology and activation devices, such as bill traps and holdup buttons, along with smoke, sound, seismic and heat detectors.

Intrusion detection systems are moving from telecommunication 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 ROI proposition by lowering telecommunication expenses.

In addition, 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.

Some ATM providers view security as just another add-on. It's important to look into the different ways criminals attack ATMs. Listening to customers and tracking the activities of criminals around the world has helped design a network of defenses to guard against each type of attack, including 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 customers and prevents crime before it begins. Implementing intelligent card reader sensors, digital video transaction recording, digital security protection for operating systems, video analytics, PIN encryption, physical-attack hardening of installed ATMs and consumer safety enhancements all help financial institutions strengthen security.

A Monitor's Job

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 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.

Because customers are able to view and administer security

operations at their convenience, the data allows customers to have tighter security controls over account information and alarm activities. Customers are able to use the data to leverage false alarm fines, helping control costs more accurately and efficiently. The data helps reveal a number of activities, such as burglary, vandalism, holdups, employee duress, chest access and interruption in operation or unattended equipment.

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 the author

Vincent Lupe

Vincent Lupe is the director of global product management and planning at Diebold

If you are interested in having First Aid Training or Defensive Driving Training for your staff, contact Amalgamated Security

Looking for some Driving Safety TIPS ?



Driving can be very dangerous at times and the roads are much busier today than they were a generation ago. Nowadays, almost every individual has a car as opposed to just one car per family (as it was in previous decades). With so many cars on the road, there's a significantly increased risk of getting into an accident. To keep you and your family safe, follow these safety tips.

The Cell Phone Issue

When discussing safety tips for safe driving, we have to address cell phone use. Most of us know not to use a cell phone while driving, yet so many of us still do despite how dangerous this practice is.

Some studies have suggested that driving while talking on a cell phone is worse than driving while under the influence of drugs or alcohol. Talking with a headset or with your phone on speaker is really no solution. It's the actual act of talking that presents a problem. When you're on a cell phone while driving, your mind is preoccupied with your conversation.

That being said, cell phones are actually an important part of road safety. If you're driving down a road and witness an accident or run into trouble, your cell phone can be a priceless tool. It's a matter of knowing when (and when not) to use it.

Be Alert

Another important safety tip while driving is to always be alert. Don't drive while you are tired. If you are on a long road trip, you really should stop for about twenty minutes every two hours to use the restroom and get out and stretch.

Many people push the limits and try to drive when they are, in fact, tired. This is a dangerous practice as many car accidents happen when someone falls asleep at the wheel. Don't be a statistic. Be smart enough to know when you're too tired to drive.

You're Not Alone

Another important safety tip is for you to be aware of the

other drivers on the road.
How often do you look both left and right when driving through an intersection?
Many accidents occur because someone has run a red light and hits into the side of a vehicle going across the roadway.

Don't only look in the direction you expect traffic to be coming from, look on both sides of each lane. Sometimes cars do proceed down the wrong side of the road either because they are driving in an unfamiliar area or they are under the influence.

The above road safety tips was designed to increase your awareness of possible dangerous situations that you might encounter (or create, in the case of insisting on using that cell phone) while you're on the roadway. Keep the above safety tips in mind the next time you turn your key in the ignition.

Amalgamated Security provides a full range of security services, which include:

- Cash Services**
- Electronic Security**
- Access Control**
- Data Storage**
- Courier Services**
- Guarding Services**
- Alarm Monitoring**
- Response Services**

If you are interested in having First Aid Training or Defensive Driving Training for your staff, contact Amalgamated Security

