

# SECURITY DIRECTOR NEWS

THE BUSINESS NEWSPAPER FOR SECURITY DIRECTORS

www.securitydirectornews.com

marketwatch: **finance**

JANUARY 2005 • SECURITY DIRECTOR NEWS

19

## Financial institutions dive into new realm of risk

Today's bank security directors have more on their minds than robbers, forgers — like terrorists, cyber thieves

BY JOANNE FRIEDRICK

For those directly involved in the banking and finance industries, the awareness is great that this sector is not only the mark of robbers and forgers but also a target for international terrorists and cyber thieves.

However, long-standing practices within the industry have put it on the right track for dealing with these security challenges.

In its Best Practices for Government to Enhance the Security of National Critical Infrastructure, the Department of Homeland Security's National Infrastructure Advisory Council gave high marks to the financial services industry, noting the ongoing cooperation among institutions, focus on regulatory issues and speed with which it reacts to challenges.

As a result, the final report and recommendation, issued April 13, 2004, said "the banking sub-sector has multiple strong incentives to promote security" and was unlikely to need additional regulation or oversight from DHS.

Security practices within the banking and finance community cover a wide range of issues, including taking into account regulations such as the Gramm-Leach-Bliley Act, which covers financial privacy; and the U.S. Patriot Act, which calls for protection against terrorist use of financial institutions to move and access funds.

"Terrorism affects banks at many levels," said Francis Tesorero, chairman of the Banking and Financial Service Council for ASIS International, "from physical threats to the security of the institution, money laundering, fraud, travel safety, executive safety and many others."

He said the council, addressing concerns related to terrorism, has served as a liaison to DHS's Financial Services Sector Coordinating Council "where we were instrumental in the creation and refinement of the nation's current alert system."

Tesorero echoed the best practices report's conclusion that the financial services sector "is one of the most prepared critical infrastructures in the nation."

Security directors themselves, Tesorero said, have seen their role expand from one focused on robberies, check fraud and internal theft to a more all-encompassing role tied to both post-Sept. 11 and technology-related threats.

"Computer fraud and computer hacking investigations have opened up new

his input is sought in the prevention and investigation process, he said.

Dealing with the balancing act between making banks welcoming and friendly and making them safe for customers and staff has been the focus of late, said Barry Katsoff, vice president-director of business development for Stanley Security Solutions.

He said institutions want restitution if theft or fraud occurs, which means greater investment in systems that deliver readily identifiable photographs and more cameras per teller.

Darrell Wilson, security director for Truliant Federal Credit Union in Winston-Salem, N.C., said his focus on combating fraud has resulted in the recovery of \$1.5 million and the conviction of 600 individuals.



Darrell Wilson

"Fraud is my security issue," stated Wilson. Because of what he views as a lack of cooperation from police on pursuing fraud cases, Wilson said he has learned to do everything in house, from capturing the fraud on tape to interviewing the suspects and gaining the confession — all on video.

He said the key is to force the perpetrators to come to him, then catch their transactions via camera. "Every time we get a fraud, we pull pictures (from the security cameras)," he explained. ATM transactions are also recorded on digital video, he said, and alerts of fraudulent transactions are quickly transmitted to tellers and managers.

Bank fraud continues to be a top priority among bank security personnel, as does bank robbery, said Michael Smith, president of the New York Bankers Association, which represents commercial, regional and community banks.

Smith said the organization's security task force, made up of about 30 bank security directors and officers, spent 18 months addressing the bank robbery issue. A big part of the solution, said Smith, is the use of technology to not only enhance communication between banks and law enforcement but also to identify criminals and send digital images of suspected thieves throughout the banking system.

ATM and branch security are part of a multi-faceted approach to financial institution security, according to Richard Baggot, vice president-electronic security and currency systems group at Diebold.

Everything from vaults to safe deposit boxes to teller lines have had their security enhanced through new developments

proved camera technology allows banks to send color images to off-site security offices and even to patrol cars while an event is going on so robbery suspects can be identified better and faster, he said.

Cameras installed at ATMs view not only the user but also the area around the ATM in case of a robbery or attack.

Another innovation, said Stanley Security Solutions' Katsoff is the use of the teller cash dispenser, which limits or eliminates the amount of funds in teller cash drawers and adds safeguards, such as supervisor intervention for consecutive transactions, or special hold-up sets with lots of small value bills meant to fool the thief.

But bank security also means covering the corporate headquarters and operations centers, said Baggot, with systems for addressing visitor and employee access control, workplace violence, internal theft and terrorism.

"Everything changed after Sept. 11," said Baggot, especially for high-profile banks. He said most are limiting access to their headquarters and operations centers and have increased camera surveillance both inside and outside facilities.

Katsoff said high-risk companies have added concrete barriers outside to tighten access at bank administration centers and turnstiles for access control to prevent tailgating.

"We're seeing a lot more security for employees and visitor management," he said.

Cyber security is also part of the equation, said Baggot, with access control and biometric systems used to keep people from gaining access to sensitive areas and data. Knowing the legal ramifications is also important, he said: "There is an obligation to provide security."

Both the Gramm-Leach-Bliley Act and the U.S. Patriot Act have mandated certain security measures. Jacky Grimm, director of security solutions for Diebold, said as a result of the GLBA's regulatory compliance issues, Diebold partnered with RiskWatch to offer a security risk assessment tool.

The software covers both physical and logical security risk assessment, explained Caroline Hamilton, president and chief executive officer of RiskWatch. She said the software takes the place of manual risk assessment by going through all the elements of a security risk assessment plan and coming up with a report that serves as a baseline for auditing purposes. It also provides a list of recommendations to get a financial institution compliant with GLBA.

Hamilton said while the new program is focused on GLBA compliance, banks are also aware of other compliance issues, such as the need under Sarbanes-Oxley for bank officers to attest that security measures are in place. **SDN**



Richard Baggot

## the future has arrived



Its performance is unique as its futuristic styling. The WV-CW374 Weatherproof Camera features the best in Panasonic camera technology for the most demanding applications. Plus it's a self-contained system. Complete with a mounting bracket that's simple to install. Take one look at the WV-CW374 and you'll agree — the future has arrived.