



How Security Can Help Financial Institutions Mitigate Risk Amid Evolving Security Threats

by Dana Little

Director, Business Intelligence

Diebold, Incorporated

The dichotomy of today's criminal activity, in which we must thwart a rise in conventional robberies and burglaries, while at the same time learn to mitigate emerging threats such as electronic fraud and organized crime, makes security more important than ever before.

Today's financial institutions have more business objectives than any time in their recent history: evolving banking services, gaining market share, enabling sustainability, securing assets, enhancing infrastructure, achieving compliance, transforming the branch and even ensuring survival. And during a time when the fight for survival often trumps all else, financial institutions may feel compelled to temporarily sideline critical operational initiatives such as security. But the dichotomy of today's criminal activity, in which we must thwart a rise in conventional robberies and burglaries, while at the same time learn to mitigate emerging threats such as electronic fraud and organized crime, makes security more important than ever before. Financial institutions can't afford to be anything less than vigilant in their efforts to secure their facilities, protect their employees and consumers, and safeguard their physical and information assets.

Today's top security threats for financial institutions include:

- BANK ROBBERIES
- ELECTRONIC FRAUD
- HACKING AND VIRUSES
- IDENTITY THEFT
- INTERNAL THEFT
- ORGANIZED CRIME
- TERRORISM

Renewing the Focus on Security

Financial institutions were among the pioneers of a variety of security tools. From the first safes and vaults to the adoption of electrical alarms to the first surveillance systems, banks and credit unions have always been leaders in the development of a more secure business environment. In a world of evolving threats, increased regulatory requirements, consumer expectations for security and intense scrutiny of the bottom line, financial institutions must once again take the lead to develop security strategies that will protect their assets and those of their consumers while delivering value to the entire enterprise.

Understanding the Threats

Conducting business on a network, providing consumers with online access to banking services and participating in the mobile information revolution have subjected financial institutions to a plethora of new security threats. High-tech threats including fraud, identity theft, hacking and malicious software remain a primary concern for financial institutions. And with good reason. In the November 2008 study, "Report on the Underground Economy," information security and management leader Symantec identified financial accounts as the second-most common category of goods and services advertised in the online underground economy. [1] The study revealed that while the asking price for stolen bank account information runs between \$10 and \$1,000, the average account balance of the advertised accounts is nearly \$40,000. While perpetrators of these crimes are cashing in their profits, financial institutions are subjected to insurance claims, regulatory citations, legal activity and the scorn of consumers who are victims of these crimes.

According to Symantec, criminals can sell stolen bank account information for \$10 to \$1,000 in the online underground economy. And it's a lucrative purchase — the average account balance of the advertised accounts is nearly \$40,000.



Renewing the Focus on Security

Understanding the Threats

High-tech threats aren't the only new worries on the minds of leaders of financial institutions. Criminal strategies to commit fraud at the branch level have become more sophisticated as well. And the criminals are often part of organized crime rings that have much to gain by infiltrating the financial institution. According to a May 2007 story in *Bank Systems & Technology*, "...fraud has become the domain of organized crime rings with vast resources that often are out of reach of domestic law enforcement." [2] From complex check-cashing schemes to use of fraudulent identification documents to open new accounts or transfer funds, these elusive criminals are exploiting the vulnerabilities of financial institutions.

The vulnerabilities of the business environment were never more apparent than on 9/11. The role financial organizations played in this tragedy has led many financial institutions to introduce ongoing homeland security and emergency management planning and training. Terrorism remains a concern in the financial industry and is seen as a threat, especially for institutions in major cities. In the last seven years, it has prompted collaboration from a variety of municipalities and financial institutions. ChicagoFIRST (www.chicagofirst.org) and FloridaFIRST (www.floridafirst.org) are but two nonprofit associations that were founded post-9/11 to address homeland security and business continuity issues and, ultimately, protect the financial community.

Even amid the new high-tech and sophisticated threats that face financial institutions today, the industry is witnessing a resurgence of conventional robberies. Internal theft that comes from disgruntled or downsized employees is also a concern. It is suggested that we'll see an even greater increase of bank robberies in 2009 as many people are feeling the effects of the down economy. By the first quarter of 2008, robbery statistics were already showing a slight increase. According to FBI data, financial institutions were victim to 1,604 robberies between Jan. 1 and March 31, 2008, a two percent increase from the same period in 2007 [3]. A June 2008 story in *USA Today* reported: "Bank robberies are up in cities across the USA this year and, although the reason is unclear, the down economy is suspect." [4] The FBI confirmed this suspicion in a November 2008 story in *Desert News*. When asked about the threat of bank robberies during the holiday season, FBI Special Agent Juan Becerra told *Desert News*: "We anticipate the desperation factor to play a part in the thoughts of individuals who otherwise normally would not do something like this." [5]

Even amid the new high-tech and sophisticated threats that face financial institutions today, the industry is witnessing a resurgence of conventional robberies.



Renewing the Focus on Security

Meeting Consumer Expectations

Consumers have an expectation that their identities and account data will be protected by their financial institutions.

Meeting Consumer Expectations

As threats continue to rise, so too do consumer expectations for security. Consumers have an expectation that their identities and account data will be protected by their financial institutions. Consumer perception of security influences loyalty and helps assign value to one of the financial institution's most valuable assets: its brand. An August 2008 story about identity theft in *Security Management* summed up the brand threat: "...it is also important to realize that some incidents of identity theft can create reputation-damaging headlines and lawsuits for enterprises ranging from government to healthcare to financial and college organizations." [6]

Even so, identity theft and the fraudulent transactions that often result are on the rise. According to Javelin Strategy and Research, a firm dedicated to researching financial service areas, nearly 8.4 million consumers fell victim to identity theft in 2007. These thefts led to \$49.3 billion in fraudulent charges. And the average victim spent at least 25 hours trying to resolve the issues related to the theft. [7]

Consumer respondents ranked having their personal, identifying information stolen as one of their top concerns. In fact, concern over theft of this information was ranked higher than concern about other personal life issues such as bankruptcy, having medical information stolen and even separation or divorce.

In a 2008 survey released by Diebold, consumers were asked about their expectations for security in five different industries, including financial, hospitality, retail/pharmacy, information technology and government. Of all the industries included in the survey, consumers perceived that the financial industry puts the most effort into protecting their personal information. In the same survey, consumer respondents ranked having their personal, identifying information stolen as one of their top concerns. Concern over theft of this information was ranked higher than concern about other personal life issues such as bankruptcy, having medical information stolen and even separation or divorce. [8]

A September 2008 story about financial institution spending, which appeared on www.bankinfosecurity.com, suggests consumer trust will be a critical driver of the investment in security in the financial environment. In the article, Christine Barry, research director for financial services research and advisory firm Aite Group LLC, says: "As banks try to build the trust of their consumers, they are going to continue to make an effort to make sure that their consumers both feel and actually are secure. That their identities are secure, as well as their account information. So we will see a continued investment in that [security] as well." [9]



Renewing the Focus on Security

Considering the Big Picture

Considering the Big Picture

A renewed focus — and investment — in security may be a hard sell, especially with the current challenges facing the financial industry. That's why security must be viewed not just as a tactic, but as part of the overall business strategy.

Compliance is a big-picture issue within the financial institution that garners much focus and continued investment. From the alphabet soup of SOX, FACTA, GLBA and PCI to the Identity Theft Red Flags Rule and more, financial institutions are required to comply with a wide variety of standards. Moreover, compliance is often contingent upon the implementation of enhanced security measures, especially when it comes to confidentiality and the protection of data. In the story "The Five Essentials of Banking Security in Tough Times," www.bankinfosecurity.com recognized regulatory compliance as the No. 1 financial industry initiative requiring a security investment, even in the current financial environment. [10] Such investments can be leveraged to deliver value not only for risk management, compliance and security, but for the entire enterprise.

Today's security leaders should strive to be included in the organization's most important discussions about its priorities, its objectives and its future.

Getting a seat at the table when it comes to compliance is only the first step to injecting security into the big picture. Security strategies and solutions should support the organization's overall vision, mission and values. Today's security leaders should strive to be included in the organization's most important discussions about its priorities, its objectives and its future. In addition, security plans should fundamentally support the initiatives of the enterprise.

An enterprise approach requires security to be measured by the return on investment it will bring to the organization. At its most fundamental, security can be viewed in terms of the cost savings it will deliver through thwarted robbery attempts, the prevention of network breaches, the replacement of keys and more.

An even more progressive view of security for the financial institution entails leveraging security tools and technology to deliver value for other parts of the organization. Devices such as cameras, which traditionally enable monitoring of various hot points to detect potential security issues, have capabilities beyond their role in security. Cameras can also be used to monitor consumer traffic/flow, assess the result of training initiatives and help measure the effectiveness of marketing initiatives.



Renewing the Focus on Security

Considering the Big Picture

Security monitoring solutions also have utility reaching far beyond the security program. Some innovative financial institutions are already leveraging these solutions to enhance their sustainability initiatives. Similar to traditional security monitoring services, energy management monitoring utilizes devices that send signals to a central station. These signals enable the tracking of facility resources such as lighting and heating, ventilation and air conditioning (HVAC). Just as traditional monitoring responds to signals that indicate events such as intrusions, energy management monitoring responds to signals that indicate variances in facility temperature, illumination of lights or other energy-related measurements. It enables organizations to utilize that information to control the cost of energy and meet their overall goals for sustainability. And when used effectively, it can save an organization an estimated 15 to 20 percent in energy costs.

What these two examples have in common is data. Convergence has led the way for integration of building automation and security systems. And because many of today's systems reside on the network and possess an IP address, they can send and receive information security professionals couldn't have imagined even five years ago. Initiatives such as Physical Security Information Management, or PSIM, demonstrate the benefits of leveraging and repurposing this information. In a March 2008 column in *SDM Magazine*, Dan Dunkel, president, New Era Associates, defined PSIM as an "enterprise software that acts as a proactive collection point for all devices on the network, generating information and providing a holistic view of security operations and their related interactions." [11] PSIM could further transform the way we look at security by not only generating information, but also enabling response to various data within the business environment. That's the key to security's role in the big picture, in the larger enterprise. Security must transcend its traditional role to become an even more valuable, more powerful business tool.

To build a modern security strategy — one that will mitigate, detect and respond to traditional and emerging threats while adding value for the enterprise — financial institutions must consider more than just technology. They must blend technology with more effective management and the efficient use of manpower.

Blending Management, Manpower and Technology

To build a modern security strategy — one that will mitigate, detect and respond to traditional and emerging threats while adding value for the enterprise — financial institutions must consider more than just technology. They must blend technology with more effective management and the efficient use of manpower. In the converged security landscape, effective programs include physical and logical security and security management, but also people, process and technology.

Effectively Managing Security

Demonstrating ROI for the enterprise requires measurement, and measurement requires effective management. The management of a security program should begin with the development of security policies, procedures and practices. These elements will not only set expectations for what the security program is expected to achieve, but they will also enable employees throughout the enterprise to understand their role in keeping the financial institution secure. Training programs can help ensure understanding of the policies, procedures and practices that drive the security agenda, and they can also instill a culture of security that reaches far beyond the security team. A culture in which all employees are security aware and committed to protecting the financial institution's assets will not only elevate the visibility of the security program, it will help contribute to its success.

A webcast posted to www.cio.com illustrates how Intel evolved its corporate culture to “turn its workforce into a security force.” According to the webcast, one of the company's transformational tools is a forum for employees to plot how to hijack shipments of microprocessors, sell Intel's intellectual property to competitors, blackmail their coworkers, hack their networks and more. And, yes, there are incentives to attend the meeting in the form of pay and meals. Referred to as “War Gaming,” Intel's approach to creating a security culture involves employees at a variety of levels, from a multitude of disciplines, engaged in these types of exercises that help them understand the criminal mind. These activities foster understanding, and ultimately, help employees better protect the company's assets. The philosophy? Effective security is the responsibility of the entire enterprise, and all stakeholders can serve as “security agents.” [12]

Once employees get involved and understand their role in security, they're more likely to have a vested interest.



Blending Management, Manpower and Technology

Effectively Managing Security

Once employees get involved and understand their role in security, they're more likely to have a vested interest. Various tools such as security assessments and performance evaluations can be used to measure their engagement, verifying their compliance with policies, procedures and practices. Such tools can also help monitor fulfillment of the regulatory requirements that are commonplace in the financial environment.

Financial institutions should develop proven, documented processes for the assessment of their security technologies.

Management of the many technologies that are part of the security program is also critical. Financial institutions should develop proven, documented processes for the assessment of their security technologies. Such processes will verify performance and influence the long-term maintenance, ensuring the devices operate properly when needed.

Discovering Manpower Alternatives

Creative approaches to security staffing can enable financial institutions to overcome shrinking budgets and limited manpower. Similar to the emerging view of the security function, in which security must extend beyond its traditional role to deliver more value for the organization, the approach to security manpower must also be more global in nature.

Any review of a financial institution's profit-and-loss statement reveals the investment being made in its people. As much as 50 percent of a branch's expense can come from personnel. With such a significant investment in talent, it's vital that staff resources are used as efficiently as possible. By embracing a security culture, a financial institution is opening the door to including the entire organization in security initiatives. Staff can take on duties that broaden the security program and reinforce the value of security across the enterprise.

Outsourcing security-related services can help deliver cost savings, streamline operations and increase ROI for the financial institution.

Partnerships with security integrators also serve to extend the capabilities of the security team. Outsourcing security-related services can help deliver cost savings, streamline operations and increase ROI for the financial institution. By incorporating outsourced solutions, financial institutions can utilize personnel more effectively, enabling employees to focus on core competencies. Outsourcing typically embraces an operating model that allows for the addition of new security solutions with continually updated technology, without the traditional upfront expense. The elimination of such capital investments is yet another way security can contribute to the big picture and the bottom line.

Even technology can help bolster manpower. Small security teams can be virtually expanded by leveraging new technologies. And that expansion can help increase the productivity, efficiency and efficacy of security staff.



Blending Management, Manpower and Technology

Incorporating Technology

Financial institutions should select technology that will also enable them to achieve specific business objectives.

Incorporating Technology

Whether opting for technology applications to enhance manpower, improve security or enable convergence, investments in technology should stay true to the big-picture approach to security. Financial institutions should select technology that will also enable them to achieve specific business objectives.

Modern security technology is designed for integration. No longer must physical and information technologies operate in the silos to which they have historically been relegated. Security integration requires unprecedented collaboration between the security and information technology roles. This collaboration is the only way to ensure that the incorporation of new technologies will pay dividends for the entire enterprise. In a January 2008 column in *SDM Magazine*, Dunkel asserts that creating a collaborative dynamic between physical security and IT professionals is critical. Dunkel says: "First, the IT department is getting more involved in deploying enterprise physical security solutions and, second, the IT department has long-standing buying relationships with the IT manufacturing, distribution and integrator communities. It makes sense to leverage these relationships ..." [13]

Leveraging IT expertise can help ensure successful deployment of new technologies. New digital security standards embrace open architecture with which the IT professional is familiar. And similar to standards in the computer industry, they're driving solutions that move away from the proprietary foundation of the past and toward a plug-and-play model. This mode will ultimately protect the long-term security investment, ensuring interoperability between various systems, including existing legacy systems and new security investments. That interoperability enables security to play a role in the larger enterprise.

Key technologies that are working to enhance the financial institution's security while increasing ROI for the enterprise include:

INTELLIGENT VIDEO

Intelligent video leverages technology to enhance video surveillance. While traditional video captures and records activity, it doesn't have the power to analyze or review the activity taking place. That analysis is left to a security staff that couldn't possibly review every frame. Video that isn't reviewed may contain events, activities or suspicious behavior that could help detect potential security threats. Intelligent video enables the surveillance system to analyze all video that's captured. It has a wide variety of applications for the financial environment, and it's more reliable and flexible than traditional systems. It also lessens the burden for security staff, which have historically relied on manual video review.



Blending Management, Manpower and Technology

Incorporating Technology

IP DEVICES

Internet Protocol, also known as IP, enables computers to “talk” to one another, regardless of their location. IP security employs the same idea. In this case, however, physical security devices — such as digital video recorders, cameras, card readers and motion detectors — are among the components communicating. Using IP, security professionals can deploy and operate these devices across facilities and geographies to accomplish video surveillance, access control, intrusion detection and other forms of physical security.

BIOMETRICS

Biometric systems analyze specific behavioral, biological or physical traits to verify individuals’ identities. Such systems offer increased security due to the inherent difficulty of mimicking one’s physical identity. Behavioral biometric traits include signature and voice. Physiological biometrics are more commonly used in the financial environment for applications such as access control and login authentication. They use physical traits — fingerprints, hand geometry, iris or retina scans, facial recognition and more — to authenticate a person’s identity.

IDENTITY AND ACCESS MANAGEMENT/FRAUD MANAGEMENT

Identity and access management enables a financial institution to establish an identity for an employee or consumer and grant permission for that employee or consumer to access various physical or information assets according to that identity. This complex security practice helps manage fraud by implementing stronger identity verification and authentication processes. Moreover, it enables continued management of the identity and related permissions throughout its lifecycle. For consumers, processes ensure the person accessing accounts or other assets is who he or she claims to be. For employees, processes ensure they access only the physical and information assets for which they have permission.

While the environment in today's financial market presents an untold number of threats and challenges, it also offers unique opportunities to develop a security program that mitigates these threats and adds value to the enterprise

Planning a Holistic Security Strategy

While the environment in today's financial market presents an untold number of threats and challenges, it also offers unique opportunities to develop a security program that mitigates these threats and adds value to the enterprise. In December 2008, the ASIS Foundation's Urban Institute Justice Policy Center released "Planning for Change," a report on security managers' perspectives on future demographics, crime and technology trends. While the security managers who participated in the report were realistic about the challenges that lie ahead, they were also optimistic. The executive summary of the report reflected this optimism: "As the security industry looks ahead toward its next 10 years, security professionals are challenged with adapting current protocols and technologies, and developing new ones in response to emerging demographic and crime trends. In anticipation of these changes, leaders in the security industry could take a more proactive role anticipating likely impacts, facilitating conversations around these issues, and planning and advocating for changes that offset threats ... while capitalizing on the benefits. This approach holds promise for achieving significant gains for the safety and security of employees, consumers and the public." [14]

This promise holds true for the enhancement of security for financial institutions. While the security needs of each financial institution vary, banks and credit unions of all sizes have common assets and common items of value they seek to protect. Security programs should ensure the protection of the five key assets of the financial institution:

- Facility
- Network/data
- Staff
- Equipment
- Customers/members

The best course of action is to implement a holistic security strategy that integrates robust physical and logical security solutions. The steps to achieving such a strategy include:

Identify areas of the financial institution that are most vulnerable.

Assess and prioritize which real-world threats would have the most significant impact on the institution's physical and critical information assets. Determine the likelihood of each risk occurring within the institution.

Develop a holistic security strategy designed to integrate physical and logical tools to protect the institution's assets.

Deploy efficient solutions and mitigation strategies that will keep assets safe and demonstrate an ongoing commitment to reducing risk.

Manage and monitor the overall maintenance of the security program.

Integrate, manage and monitor physical and logical security operations.



Planning a Holistic Security Strategy

The integration of logical and physical security solutions is critical to a holistic, interoperable security strategy.

The integration of logical and physical security solutions is critical to a holistic, interoperable security strategy. Physical security solutions should focus on the hot points within the financial institution. Typical hot points include:

- Perimeter
- Drive-up
- After-hour depositories
- Employee entrances and parking areas
- Lobby
- Teller area
- Vaults/cash room safes
- ATMs

Security programs should protect five key assets:

FACILITY
NETWORK / DATA
STAFF
EQUIPMENT
CUSTOMER / MEMBERS

While physical security solutions focus on the hot points within the financial institution facility, information security solutions should protect sensitive information and the infrastructure on which it resides. To protect data, systems and networks must be safe, secure and compliant. Any network is an easy target for unauthorized users who are eager to steal consumer identities, account information or proprietary information, or those whose goal it is to deploy remote-control programs, Trojan horses or other malicious code. Hackers may attempt to overcome firewalls, take advantage of improperly configured applications and crack encryption to access data. And with only simple protections in place, a financial institution is vulnerable.

A robust information security program with detection software and limited user privileges can reduce vulnerability and provide a stronger likelihood of identifying unauthorized activity by:

- Preventing breaches and threats before they happen
- Safeguarding valuable data
- Improving information technology security and compliance
- Implementing appropriate responses in the event of a security breach
- Minimizing vulnerabilities related to identities and passwords

Action steps for a holistic security strategy:

- Identify vulnerabilities
- Assess and prioritize real-world threats
- Develop a strategy that integrates physical and logical tools
- Deploy efficient solutions
- Manage and monitor the program's maintenance
- Integrate, manage and monitor operations

Forming a strategic alliance with a security integrator can help make the implementation and maintenance of a security program that addresses today's threats more manageable.

Relying on a Security Partner

The security challenges of today's evolving financial environment won't wait. To meet these challenges, financial institutions must overcome limited budgets, an overburdened workforce, the need to focus on a variety of other business priorities and more. Forming a strategic alliance with a security integrator can help make the implementation and maintenance of a security program that addresses today's threats more manageable. A successful partnership with an integrator can enable a financial institution to achieve economies of scale, gain efficiencies and realize greater return on investment.

Selection of a security integrator is about much more than price or bells and whistles. To fulfill one of the most critical operational needs of a financial institution, an integrator must foster trust, have a broad range of capabilities and be committed, stable, flexible enough to customize solutions to the specific needs of the organization, experienced in similar projects and skilled in serving as a consultant to its customers.

As you renew your focus on security, consider investing in a partnership that could forever impact the performance and value of your security program. The security of your organization depends on it.

END NOTES

- [1] Symantec Enterprise Security. "Report on the Underground Economy: July 2007 – June 2008." November 2008.
- [2] Bruno-Britz, Maria. "Fraud Techniques Evolve in Parallel with Bank Products and Defenses." *Bank Systems & Technology*. May 5, 2007.
- [3] U.S. Federal Bureau of Investigation. "Bank Crime Statistics (BCS) Federal Insured Financial Institutions: January 1, 2008 – March 31, 2008." October 17, 2008.
- [4] Joyner, Chris. "Bank Robberies Up Around USA." *USA Today*. June 16, 2008.
- [5] Winslow, Ben. "FBI Braces for Bank-Robbery Boom." *Desert News*. November 23, 2008.
- [6] Collins, Jim. "Scoring to Combat Identity Theft." *Security Magazine*. August 15, 2008.
- [7] Kim, Rachel. "2008 Identity Fraud Survey Report." Javelin Strategy and Research. February 2008.
- [8] Lextant and Diebold, Incorporated. "Information Security Surveys." August 11, 2008.
- [9] Field, Tom. "New Year's Resolutions: A Look Ahead to Banking, Security Priorities in 2009." www.bankinfosecurity.com. December 1, 2008
- [10] McGlasson, Linda. "The 5 Essentials of Banking Security in Tough Times." www.bankinfosecurity.com. November 25, 2008.
- [11] Dunkel, Dan. "Security's New Landscape." *SDM Magazine*. March 1, 2008.
- [12] www.cio.com. "War Gaming: How Intel Turned Its Workforce Into a Security Force." www.cio.com. November 19, 2008.
- [13] Dunkel, Dan. "Transformation Trumps Convergence." *SDM Magazine*. January 6, 2008.
- [14] LaVigne, Ph.D., Nancy; Hetrick, Samantha; Palmer, Tobi. "Panning for Change: Security Managers' Perspectives on Future Demographics, Crime and Technology Trends." ASIS Foundation Urban Institute Justice Policy Center. December 2008.