



## **Incorporating Information Security into a Holistic Security Plan**

*by B. Scott Harroff*  
*Chief Information Security Architect*  
*Diebold, Incorporated*

Insider and external threats to financial institutions are prompting the need for bank executives to more closely examine all current security structures and develop robust, holistic integrated security programs that effectively protect the institution's network, systems and data.

Financial institutions have always faced numerous security threats. But today, the threats have changed in character. Gone are the days when the most dangerous threat to a financial institution was physical in nature. The threat of hackers, malicious software and insider sabotage has become more prevalent as technology improves and economic conditions worsen.

Often the impact of the theft of information is far-reaching and long-lasting, so executives must deploy an information security plan that protects sensitive data and the infrastructure on which it resides. A recent article in National Journal Magazine reports that economic damages from fraud could exceed those caused by any act of terrorism.<sup>[1]</sup> Insider and external threats to financial institutions are prompting security professionals to more closely examine all current security structures and develop robust, holistic integrated programs that effectively protect the institution's network, systems and data. Such a comprehensive approach complements a financial institution's business objectives, while enabling it to identify vulnerabilities, assess and prioritize threats, deploy efficient mitigation strategies and manage the information security program.

### **Identify The Risks to Your Information Assets**

Potential threats to your information security assets run the gamut from fraud and identity theft to hacking and malicious software. While nobody wants to imagine the tumult these security breaches cause, it's imperative that security leaders do just that in order to understand the financial institution's vulnerabilities. Once the vulnerabilities are identified, steps can be undertaken to protect a bank or credit union's numerous information assets.

**Consider this:** The Federal Trade Commission's publication, *Consumer Fraud and Identity Theft Complaint Data January-December 2007*, shows the complaint database developed by the commission received more than 800,000 complaints of consumer fraud and identity theft in 2007 alone. That was the eighth consecutive year identity theft was ranked as the No. 1 consumer complaint, with 32 percent of reports directly related to identity theft. Furthermore, losses from fraud and identity theft were reported at more than \$1.2 billion, amounting to a median per-person monetary loss totaling \$349.

**2007 was the eighth consecutive year identity theft was ranked as the No. 1 consumer complaint, with 32 percent of reports directly related to identity theft.**

Not only do fraud and identity theft create a nightmare for the consumer – they also wreak havoc on the financial institution, significantly and negatively impacting its bottom line. The FTC reports that credit card fraud was the most common form of identity theft in 2007, with 23 percent of consumer respondents from the study reporting it had occurred to them. Credit and debit card fraud forces banks and credit unions to cancel and reissue thousands of cards, resulting in thousands to tens of thousands of dollars in loss for the financial institution, as well as the loss of numerous hours of employee time.<sup>[2]</sup>



## Identify The Risks to Your Information Assets

Credit and debit card fraud forces banks and credit unions to cancel and reissue thousands of cards, resulting in thousands to tens of thousands of dollars in loss for the financial institution and the loss of numerous hours of employee time.

Bank account data is among the most commonly advertised items for sale online, according to a report by Internet security firm Symantec. The report, cited in an April 8, 2008, article in Security Management, states that 22 percent of goods and services for sale by cybercriminals are bank account details. Prices for bank account information range from \$10 to \$1,000 — a cheap price tag considering the access it could deliver to bank accounts with high balances, business accounts and European Union accounts. Cybercriminals are stealing this information simply because it's easy for them to acquire and there is a lack of fraud detection technology that's been implemented on credit cards.

Symantec reported Trojan horse programs increased by 86 percent during the last half of 2007.

Not only are cybercriminals stealing and then selling bank account data for profit, they also are developing Trojan horse programs to capture confidential banking information. Symantec reported Trojan horse programs increased by 86 percent during the last half of 2007. <sup>[3]</sup> The destructive programs pretending to be benign applications are so named because they are similar to the horse in the Greek myth about the Trojan War. Seemingly unthreatening, the program can be destructive and devastating to logical assets.

### Understand Insider Threat

With the economy in recession and the unemployment rate skyrocketing, it's quite possible fraud, identity theft, malicious software and hacking, as well as insider crimes, will continue to rise as people look for a quick fix to their money woes. Information security encompasses much more than protecting against the external risks of fraud, identity theft, hacking and malicious software. It also includes protecting your financial institution against potential insider threats. Such threats are a growing concern. And according to an article on [www.bankinfosecurity.com](http://www.bankinfosecurity.com), security experts believe there is an increased risk of insider threats occurring during this tumultuous economic time of mergers, acquisitions and employee layoffs.

Though damaging, insider threat may not always be deliberate and premeditated. Oftentimes, sensitive company data is unintentionally made vulnerable through the use of a variety of prevalent consumer technologies such as instant messaging, smart phones, USB flash drives and many other smart devices that have the ability to move large amounts of data. Unfortunately, while the convenience of these systems has proven to be a necessary part of life for executives in today's data-driven and mobile world, sometimes transferred information can simply fall into the wrong hands. Sensitive data transferred via messages can end up on multiple, unsecured servers where they can be accessed by those who should not be reading them. Intentions may not have been malicious, but the end result often is.



## Understand Insider Threat

Purposeful, calculated insider theft is a completely different matter. Deliberate insider threats fall into three categories: insider IT sabotage; theft for business advantage; and theft for financial gain. In a [www.bankinfosecurity.com](http://www.bankinfosecurity.com) article, Dawn Cappelli, senior member of the computer emergency response team (CERT) at Carnegie Mellon University's Software Engineering Institute, said the motivation for insider sabotage is typically revenge. "Usually, the employee is upset about negative work-related issues and wants to take revenge by disrupting the company's systems and network. These work-related issues can range from the employee being denied a promotion to not getting along with his/her supervisor, or having issues with low salary or total compensation package," the article states.

In a 2008 study conducted by security research group Lextant for Diebold Security, consumers ranging from Baby Boomers, to Generation X and Generation Y, all ranked identity theft as one of their top three life concerns.

Surprisingly, theft for business advantage is often motivated by the desire to develop a competitive edge, rather than financial gain. In this circumstance, the employee may have been hired by a competitor or is looking to launch a new business and wants to bring the information with him or her. Meanwhile, in cases of theft for financial gain, the motive is completely focused upon cash. Theft for financial gain is the most prevalent among financial institutions, according to CERT crime data from 1996 to 2007 cited by Cappelli. Sixty-eight percent of theft of information takes place within and just after three weeks of an employee leaving his/her job.<sup>[4]</sup> Protecting logical assets from external and insider threats also protects the financial institution's brand. The impacts of a security breach extend far beyond those consumers directly affected. Consumers place high importance on privacy and security, and a breach can have immeasurable negative consequences for a financial institution's brand reputation. In a 2008 study conducted by security research group Lextant, Baby Boomers to Generation X and Generation Y respondents all ranked identity theft as one of their top three life concerns.<sup>[5]</sup> The importance consumers place on the security of their personal information validates the need for financial institutions to mitigate threats to consumers' information. Otherwise, they will risk losing them as customers while simultaneously forging an uphill battle to gain back positive brand reputation.

### Mitigate Risks to Your Information Security Assets

But what strategies should be employed to mitigate risks and protect a financial institution's systems against insider and outsider threat? A firewall simply is not enough of a defense to protect data. To adequately safeguard systems, the bank or credit union needs to recognize where it is most vulnerable. If your financial institution has not yet identified its weaknesses, be proactive and conduct a risk assessment to gain knowledge of existing opportunities for your information technology systems to be compromised. An assessment will help determine how well critical systems are protected by providing a detailed and full analysis of external and internal threats. In fact, assessments should frequently take place to ensure systems are protected and deployed strategies are proving to be effective.



## Understand Insider Threat

Conduct a risk assessment to gain knowledge of existing opportunities for your information technology systems to be compromised.

If the financial institution is a large organization, resources may be available to take on the assessment internally, with the chief information security officer (CISO), chief security officer (CSO) or another high-level security employee serving as the point person for the task. However, because of compliance issues, complexity of information systems and lack of employees with the highly technical skills needed to complete the assessment, many financial institutions choose to outsource the assessment. A trusted security provider can ensure that all potential threats are identified, while providing an in-depth analysis to determine the best possible course of action to minimize or eliminate them. Furthermore, a security integrator can make recommendations, based upon assessment findings, as to what next steps the institution should take to develop a proactive security strategy.

To conduct a thorough assessment, first determine what should be studied. Some questions to ask may be:

- Are computers up to date?
- Are unapproved programs on your systems?
- Is the network adequately secure, disabling unauthorized access?
- Should those with access be limited?
- Is the network both safe and compliant?

After the assessment is completed, prioritize which identified real-world threats would have the most impact upon your financial institution, and determine what action(s) should be undertaken to mitigate the identified risks.

### Identify Staffing, Technology and Processes

Staffing is crucial to the successful deployment of security solutions. Be sure to identify who within your organization will be responsible for mitigating threats and deploying strategies to safeguard logical assets. What staffing is needed to effectively and efficiently implement and manage new or existing technology that will be used for securing systems? Determine whether your financial institution must purchase new technology or if existing technology can be utilized to achieve desired results. Processes — and training to learn those processes — must be in place so all employees understand rules, roles and responsibilities.



# Develop a Holistic Information Security Strategy

The ultimate goal of a financial institution's security team should be to develop a holistic information strategy to protect consumers, employees and the organization. Such a strategy should incorporate technologies that are interoperable with the institution's physical systems. As people grapple with the economic headwinds the current recession has delivered, the need for a robust, integrated security program is vital. Individuals who would never have considered theft for information are attempting to do so because of the economy.

A holistic program may include elements such as identity management and access control.

We've already established that data sometimes is transferred over multiple, unsecure servers, often without the sender realizing the potential for sensitive information landing in the wrong hands.

## ***Identity & Access Management***

The use of identity management tools can reduce the number of employees with access to the sensitive data, thus helping to mitigate the risk of a security breach through data transference. The true benefits of identity management systems extend far beyond the credential that enables authentication and verification. Identity management enables the enterprise to establish a unique corresponding credential for each employee, and then use that credential to control access to both physical and logical assets depending upon set permissions. A security provider can work with you to centralize identity management, implement the tools to produce credentials and leverage those credentials to facilitate a more secure approach to protecting the financial institution's information assets.

The development of an identity and access management system that enables the creation of a single, vetted, unique identity and corresponding credential to mitigate risk is one such solution. Credentials can be used to govern access to your institution's physical assets, such as facilities, rooms within facilities and supplies, while also managing access to data and information assets. A credential is any item or token that is uniquely bounded to a user's identity. Credentials fall into four categories of personal identification that can be used to establish identity:

- Something you are
- Something you know
- Something you have
- Something you are assigned



# Develop a Holistic Information Security Strategy

## *Identity & Access Management*

Biometrics is covered under the “something you are” category. A fingerprint, iris, retina, face, voice, DNA or handwriting are all examples of biometrics unique to one’s identity. “Something you know” is specific knowledge you possess that others would not easily know. For example, this could be a password or an answer to a security question such as, “What is your mother’s maiden name?” A card granting access to facilities and rooms is an example of something you have, but a number of other items also may fall into this category. Finally, “something you are assigned” can include one’s Social Security number, address or other biographical information.

In addition to streamlining the process, single sign-on allows users to gain access to multiple resources and software systems through just one password and one login.

### ***Single Sign-on***

A credential — falling into one of the aforementioned four categories — can be used to enable single sign-on (SSO), allowing users to complete a single login to gain access to multiple resources, applications and software systems, minimizing existing and potential password vulnerabilities. There is no longer a requirement for individuals to remember multiple, complex passwords. And SSO can be tied to both biometrics and card access for improved functionality. Additionally, SSO eliminates the risk of human error and the loss of credentials. Individuals today have passwords for multiple technologies currently in their possession. Calling to mind the appropriate password for the corresponding technology can be difficult, often resulting in a call to the IT department and an increased cost to the financial institution for IT support. Not to mention, many employees write down their passwords so as not to forget them. Unfortunately, these passwords may be stored in or around their work stations, resulting in an increased vulnerability to a non-permitted user finding the unsecured passwords and signing on with the employee’s credential. SSO mitigates the likelihood of this occurring.

Once the decision is made to invest in single sign-on, an internal framework should be established to support the interoperability of multiple systems that can leverage the credential for logical access control. To effectively implement the system, financial institutions can incorporate a provisioning model to ensure that each employee maintains one identity, eliminate disparate documentation and processes and make certain employees are only granted access to physical and logical systems for which they are permitted. Provisioning creates more efficient communications between various systems across organizations or departments. Ideally, a single, unique identity could be provisioned for physical and logical access control throughout a financial institution’s multiple locations. The identity management system or server would store identity information, allowing financial institutions to leverage the user interface to make updates to the identity, manage authorization for the use of that identity and seamlessly onboard and offboard users. Provisioning can help keep a financial institution’s systems consistent, contributing to a successful security solution.



# Develop a Holistic Information Security Strategy

## *Physical Access Control*

Physical access control is the most basic element of a strong security strategy for your financial institution and should be effectively managed. Integrated systems may incorporate the latest in biometrics and card reader technology, integrated or stand-alone badging systems, door hardware and systems software. The system will provide you with complete reporting of employee activity, including who is entering facilities, rooms and vaults and at what time. Additionally, the system may be tied to event monitoring services to provide managed access control, which combines PACS with systems that can be remotely managed and monitored. This allows for localized control, accountability and convenience to the financial institution. With managed access control, you can further define authorized individuals' access by both time and location, ensuring that individuals are not entering buildings during unauthorized hours. Integrating both physical access control systems (PACS) and logical access control systems (LACS) results in improved efficiencies, less cost and improved ROI.

Here's a real-world example. The South Carolina Federal Credit Union (SCFCU) determined it had too many security issues that were created by an overly complicated and inflexible system that left too much room for human error. A security integrator was hired to alleviate these concerns by implementing a managed access control solution. The SCFCU reported that the new system enhanced security while creating a simpler operation. Both the risk manager and the security officer said they appreciated the ease of the access control interface and the flexibility of the remote monitoring system. The solution "empowers us to do our jobs. It's more efficient and simplifies our lives," according to SCFCU Risk Manager Janece Van Wert.

But the effectiveness of a new holistic suite of security solutions relies in part on employee buy-in and understanding of the system. Make certain that each individual is aware of security, understands his or her role and responsibility for mitigating risk to your financial institution and is committed to providing protection. Once each individual understands he or she has a role to play to improve and ensure security, he or she will be more likely to have a vested interest.

Meanwhile, you must also be sure that those within your organization responsible for securing assets — whatever title he or she holds — understand all processes and functionality of the fully integrated system. Make certain to determine the level of support to be received from the security provider should one be hired so questions may be answered and issues rectified as they arise.



# Implement a Holistic Information Security Strategy

The addition of a proactive, positive model is the first step to developing a holistic information security strategy. In tandem with antivirus software, which monitors for known software on systems and intrusion detection systems, which monitor for malicious, network-based issues, a positive model solution should be integrated into your system. Proactive, positive model solutions provide protection by allowing only pre-approved behaviors for system users, applications and data access. Positive model programs do not rely on detection of an intrusion before flagging a process. Rather, positive model programs create rules that define allowable activities and restrict all else. This embraces a philosophy that fewer allowed permissions yield the least opportunity for threats.

With this architecture in place, the system's connectivity can be shut down if an action falls outside the normal scope of operation. Be sure to remove unnecessary applications from systems and monitor for unapproved network traffic as these often prove to be the vectors for compromise of your financial institution's infrastructure. Regularly review your system's configurations to determine whether there are opportunities to enhance its security posture. For systems with critical data, application security assessments should be performed either internally or with an experienced security integrator. Operating systems should be hardened and applications need to be reviewed and patched against vulnerabilities on a regular basis to ensure breaches are consistently remediated. Routine assessment will help determine areas of the system that need to be stronger and more secure.

## Partner With an Experienced Security Integrator

The protection of your information assets is vital to the success of your institution. Benefits from hiring a security partner are many. A security integrator can help your financial institution remain committed to security during this time of unprecedented uncertainty in the financial market. Relying on a security partner to meet the many challenges faced today as a result of a weakened economy, smaller budgets and increased threats to your informational data can help ensure the success of a robust, holistic suite of security solutions.

Partnering with the right security integrator is critical. An experienced security integrator should have a broad range of capabilities, offer solutions tailored to the needs of your bank or credit union and be a company for which you can trust to help you manage your information security solutions. A security integrator will support you during each step of the process – assessing your needs, developing the solutions and finally implementing them into your institution.

Consider partnering with a security integrator as your institution continues to mitigate risk and enhance security of its networks and data. Such a partnership could play an integral role in the future success of your financial institution.

## END NOTES

- [1] Harris, Shane. "U.S. Intelligence Officials are Worried that Financial Institutions are Vulnerable to Hackers." *National Journal Magazine*. Oct. 18, 2008.
- [2] "Consumer Fraud and Identity Theft Complaint Data January-December 2007." *Federal Trade Commission*. Feb. 13, 2008.
- [3] Harwood, Matthew. "Bank Account Details Most Popular Item for Sale by Cybercriminals." *Security Management*. April 8, 2008.
- [4] Gupta, Upasana. "Tackling the Insider Threat." [www.bankinfosecurity.com](http://www.bankinfosecurity.com). Nov. 6. 2008.
- [5] Lextant. "Information Security Surveys." Aug. 11, 2008.