



Navigating the Security Minefield

Managing Security and Operations Risk in a Global Financial Services Marketplace

Karen Massey, Senior Research Analyst, Banking Practice
Maggie Scarborough, Research Manager, Banking Practice

January 2007

A Financial Insights White Paper

Sponsored by



Financial
Insights[™]
An IDC Company

FINANCIAL INSIGHTS OPINION

Securing a financial institution and the non-public consumer and corporate information it houses is far from simple, particularly because today's distributed technology environment is more complex, and security must extend beyond an institution's boundaries to encompass service providers, remote partners, and customers. In addition, the global regulatory environment is constantly evolving, burdening financial services with significant costs of operations risk compliance to the tune of Gramm-Leach-Bliley and Sarbanes-Oxley. Under this consideration, Financial Insights observes the following:

- **Financial institutions are increasingly the target of malicious security attacks, security breaches, and fraud.** Financial services organizations are challenged with the increasing frequency and severity of attacks against them. This rapidly evolving environment is changing the way financial institutions approach security and operations risk management.
- **Financial institutions must do better than the historic "secure the boundaries" approach** since today's heightened security and regulatory environment has changed the rules. Financial institutions must protect non-public consumer and corporate information both within and outside their walls, mandating an enterprise approach that also extends beyond the institution.
- **Smart organizations will look to international best practices leveraging holistic solutions to data security and operational risk challenges.** Financial institutions should seek solutions

that encompass the broad spectrum of security concerns, including data, application, and network security; physical security of organization and service provider locations; identity, authentication and credential management; and business continuity. All of these elements are critical to a comprehensive security and operations risk management strategy.

IN THIS WHITE PAPER

In this paper, Financial Insights examines the challenges global financial institutions face regarding security and operations risk management as they strive to safeguard both corporate and consumer non-public information, all while balancing risk exposure. Also explored is how financial institutions are responding to increasing security threats, both external security attacks and internal fraud and unauthorized access, to avoid succumbing to the many risks associated with data breaches, including legal, brand, reputational, and financial. This document also discusses how these security threats fall under the larger umbrella of risk mitigation, and more specifically relate to operational risk guidelines included in the Basel II directive.

SITUATION OVERVIEW

Financial institutions are the keepers of a wealth of sensitive non-public information, entrusted to them by their consumer and corporate clients. The safety and soundness of the financial industry depends on institutions' ability to ensure that information about their customers and their business is accurate and protected. And security matters are further complicated by Basel II mandates related to operational risk management.

Basel II is a global agreement to better define for large financial services firms capital requirements and the methods of measurement. Basel II assigns operational risk as a distinct risk category with not only a minimum capital requirement, but also spotlighting it for regulatory review. For Basel II purposes, operational risk is defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people, and systems, or from external events. What this means to financial institutions is that how well they demonstrate the effectiveness and sufficiency of their operations and attendant IT support could impact how much capital they must carry in reserve for operational risk.

Managing security, fraud, and operations risk is top of mind for financial services executives across the globe. However, we see that security and risk mitigation practices vary by organization and geographic location in terms of intensity and strategy. The extent of protection a financial institution adopts depends on many factors:

- Budget allocation for security priorities
- Past experiences with security issues
- Culture and management preferences
- Cost versus perceived benefits of deploying a given solution
- The availability of adequate solutions
- Regulatory requirements

Recent developments have highlighted the need for financial institutions to increase their security and risk management measures and practices. Well-advertised instances of data loss and security intrusions along with

increased legislation and terrorist activities are now making it mandatory that financial institutions revisit their information security strategy or, in some cases, develop such a strategy.

The importance of security and operational risk management in the financial services industry has grown tremendously over the last few years due to several converging factors:

- **Growing regulatory requirements.** Basel II directives on operational risk management were enacted to address growing financial losses resulting from operational risk, such as fraud, physical losses, and business disruption. Financial institutions are therefore charged with assessing current operational risk mitigation practices and augmenting them as necessary.

Additionally, in the United States, the Gramm-Leach-Bliley Act's section 501B mandates an information security program to protect customer information, and the Sarbanes-Oxley Act requires effective controls over the financial reporting process, which include controls to ensure information integrity.

- **Increasing security risk from data theft, destruction, or manipulation from insiders** due to the greater availability of electronic information and the increased mobility and access of information via networked computers spanning the enterprise and the globe. This threat includes those from external service providers.
- **Growing number of data security breaches** as broadly reported by media outlets when data tapes are lost in transit or laptops that should or should not have contained non-public customer information are stolen or lost.

- **Increasing number and severity of security attacks** in the form of email fraud, viruses, worms, and other malicious code against financial institutions and their customers. These attacks often lead to the acquisition or destruction of confidential customer information.

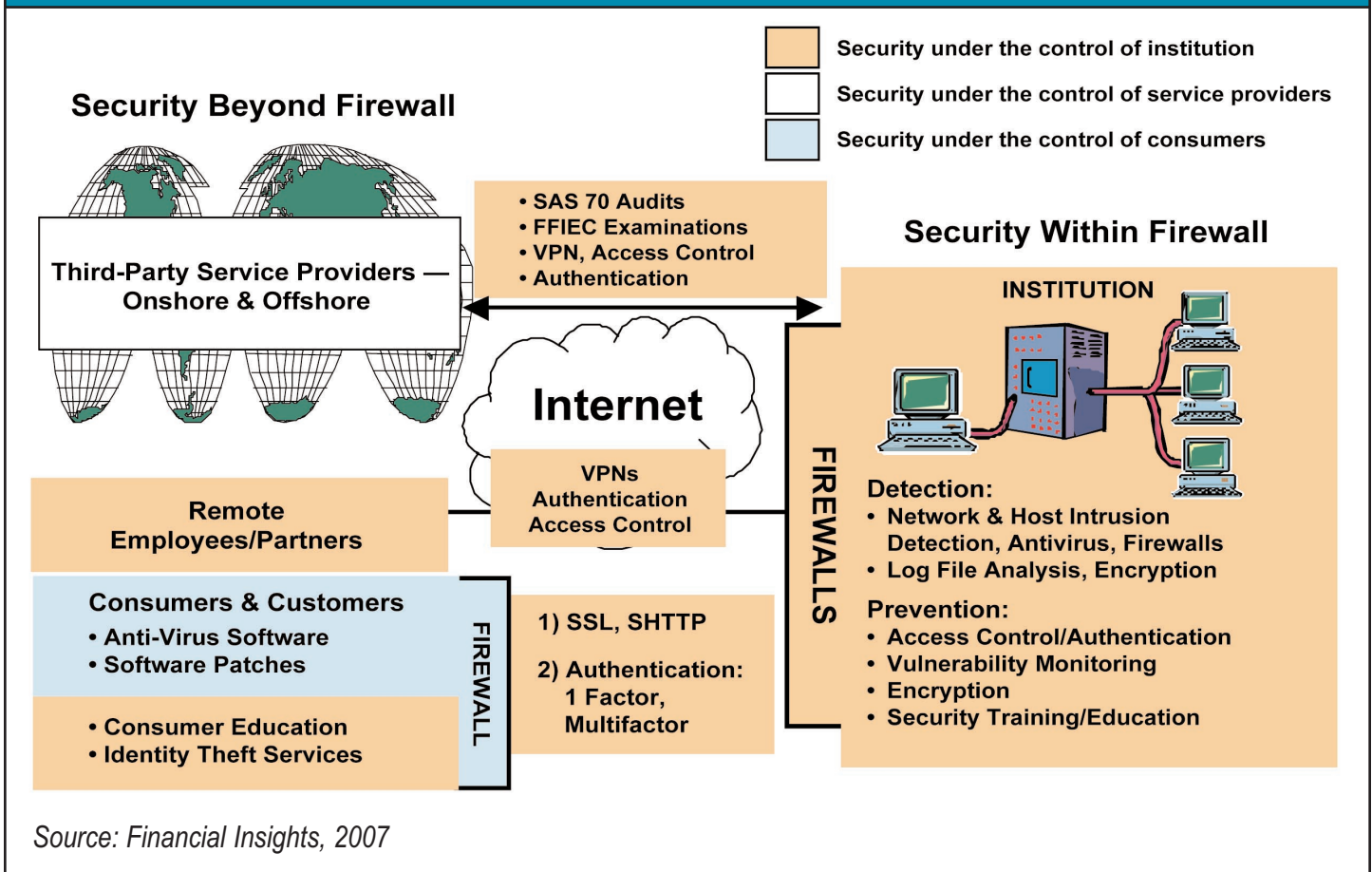
Security

Financial services firms must be concerned with security on many different levels, some of which is beyond the direct control of the institution. Figure 1 illustrates the breadth of security required to safeguard the institution's information, portions of which are under the control of either the organization's service provider or the consumer.

As Figure 1 demonstrates, financial institutions are responsible for customer and corporate security on three levels:

- **The financial institution** — Includes network, infrastructure, and environment, as well as all employees and agents with access to customer and corporate data.
- **Service providers** — Financial institutions can outsource the function, but not the management responsibility regardless of what is contained in the service level agreement (SLA).
- **Consumer** — Financial institutions must educate consumers on the need to keep confidential passwords, log-ins, and other identifying data safe. Vulnerabilities in a consumer's network or Internet connection can also open a financial institution to attacks.

Figure 1: Key Security Activities and Areas of Control: Institution, Customer, and Service Provider



The challenge to financial institutions is that of the three factors, they have limited direct control on one or arguably two of them, and they can only influence, but not control, the third.

Even in light of service provider contracts and regulatory measures, security breaches abound. A recent high-profile case in the United Kingdom uncovered a call center worker in India who sold bank account details of 1,000 customers to an undercover reporter. The call center employee, who appeared to not be working alone, stated that he could supply confidential data from in excess of 200,000 accounts per month. Bank account, credit card, passport, and driver's license details were purchased for approximately US\$7.75 each. Institutions impacted were alleged to be HSBC and Barclays, although both institutions have stated that

data had not been leaked by their respective Indian operations during this incident.

Consumers pose additional security threats. Consumers can be careless with authentication devices, such as losing an ATM card or writing down passwords, which leads to unauthorized account access and ultimately asset theft. Additionally, consumers generally do not have proper security on their personal devices, which can result in security breaches in online sessions between the consumer and the financial institution. And if that was not enough, consumers have been trained to not worry about the consequences of their actions because financial institutions have rectified financial losses resulting from fraud, regardless of the root cause.

Table 1. Risk Event Types and Examples

Event Type	Examples
Internal fraud	Employee theft, intentional misreporting of positions, and insider trading on an employee's own account
External fraud	Robbery, forgery, and check kiting
Employment practices and workplace safety	Workers' compensation and discrimination claims, violation of employee health and safety rules, and general liability
Clients, products, and business practices	Fiduciary breaches, misuse of confidential customer information, money laundering, and sale of unauthorized products
Damage to physical assets	Terrorism, vandalism, earthquakes, fires, and floods
Business disruption and system failures	Hardware and software failures, telecommunication problems, and utility outages
Execution, delivery, and process management	Data entry errors, collateral management failures, incomplete legal documentation, and vendor disputes

Source: FDIC Supervisory Insights, Summer 2006; Financial Insights, 2007

Operations Risk Management

The Basel Committee on Banking Supervision has defined operational risk as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. The seven operations risk event types are displayed in Table 1.

It is no coincidence that fraud and security are integral components of the comprehensive operational risk management definition. As important as it is to protect the boundaries of the organization, so is it to ensure that the financial institution has the appropriate policies and procedures in place to protect against catastrophic loss. We experienced several of these losses in the past few years in the shape of terrorist attacks and hurricanes along the Gulf Coast of the United States. But the financial services industry must also protect itself against the not-so-obvious instances occurring on a daily basis.

A well-known example of an operational risk management failure is the collapse of Barings Bank. Barings was driven to bankruptcy by the fraudulent trading activities of one renegade trader. Barings did not establish a sound reporting structure or comprehensive auditing procedures in the establishment of a new regional office, which allowed an individual trader to mask more than US\$1 billion in losses.

Financial Service Firms on the Defense

This rapidly evolving environment is changing the way financial services organizations approach security and operational risk management. Financial institutions have historically taken a

secure the perimeter approach. Complex organizational and sourcing structures and the proliferation of multichannel delivery strategies have led to a collection of point-specific remedies that protect resources as a proxy for information, consequently focusing financial institutions on perimeter defense. While this has traditionally served organizations well, today's heightened security and regulatory environment has changed the rules. Complex silo-focused security and risk mitigation arrangements compromise the IT security organization negatively and impact the institution's ability to effectively respond to emerging threats. Furthermore, the lack of an enterprise-level view of security operations puts firms at risk of non-compliance with existing and emerging regulatory initiatives.

Securing Data Outside The Organization

The expanding geographic boundaries of a financial institution's business create new security risks. The movement of information to outside entities, such as third-party processors and interchange partners, also poses an increased risk to financial services firms. In 2005, Citibank and Bank of America both experienced embarrassing losses. UPS lost tapes containing loan information on 3.9 million Citibank customers. In the case of Bank of America, tapes were lost containing 1.2 million personal accounts for federal employees. In response both organizations now have initiated major business process and technology initiatives to rectify existing information security shortcomings to ensure future risk is mitigated.

Banks, though, often express concern that they are often between a rock and a

hard place. Regulators demand that non-public information be backed up and stored offsite, yet large banks do not have the infrastructure to support the bandwidth required to move all that data electronically. Therefore, tapes must be the storage medium and therein lies the danger.

In regards to business process outsourcing, financial institutions are ultimately responsible for the actions of their service partners, as dictated by privacy and security regulations. A key risk management priority for financial institutions today is ensuring that the service providers, located domestically or offshore and upon which they rely more and more to run key business processes, have adequate security controls to detect and prevent breaches in the confidentiality and integrity of customer information.

Internal Fraud Trumps External Fraud

Internal security threats are more problematic than external threats. IDC estimates that over 60% of all serious threats come from internal sources, including employees, contractors, consultants, system integrators, and partners. Employees pose a significant risk (as evidenced in the Barings Bank example previously cited), and financial services organizations have always maintained extensive safeguards against internal theft and fraud. However today the potential threat has increased exponentially as portable USB mass storage devices, iPods, and other MP3 players able to hold up to 60GB of information are common in the workplace. These devices can be used to download a large customer database in a matter of seconds and then can be transported rapidly and independently of an organization's security system.

Security executives today struggle with managing unauthorized access from internal sources. Great strides have been made in securing the organization with firewalls and other network and physical security measures, but financial institutions must also be concerned with employees accessing information on the inside and somehow transmitting it to the outside with malicious intent.

Wireless Woes

Wireless devices and connectivity are still relatively new to the financial services industry, and present additional security complications. Today's financial services firms use wireless devices to improve productivity, increase business agility, and reduce costs. But with a mobile workforce comes mobile non-public information that must be secure. Mobile devices are particularly vulnerable because they are easy to lose or steal, and, like storage devices previously discussed, are capable of holding a large amount of non-public customer and corporate data. As of the publication of this white paper, there have been no security breaches or business disruptions reported in which a wireless device was the culprit. On the other hand, wireless networks have proved easy for hackers to access, supporting the case for encryption on wireless networks.

Consumers React to Security Breaches with Their Feet

Consumers across the globe are exposed to media coverage of security breaches on a daily basis. Although many of these are outside the financial services industry, this industry bears the brunt because the institutions are the ultimate gatekeepers for financial

transactions resulting from security breaches. A 2005 Financial Insights survey of 1,000 consumers over the age of 18 revealed that close to 60% are worried about identity theft to varying degrees. What is more poignant, however, is that close to 6% of survey respondents admitted to switching banks in order to reduce their risk of becoming a victim of identity theft (Figure 2).

Demonstrated is the toll a security breach or other loss event, either actual or perceived, takes on a financial institution. The financial and reputational impact of a security breach on an institution can resonate for months after the incident as consumers flood contact centers, monitor their

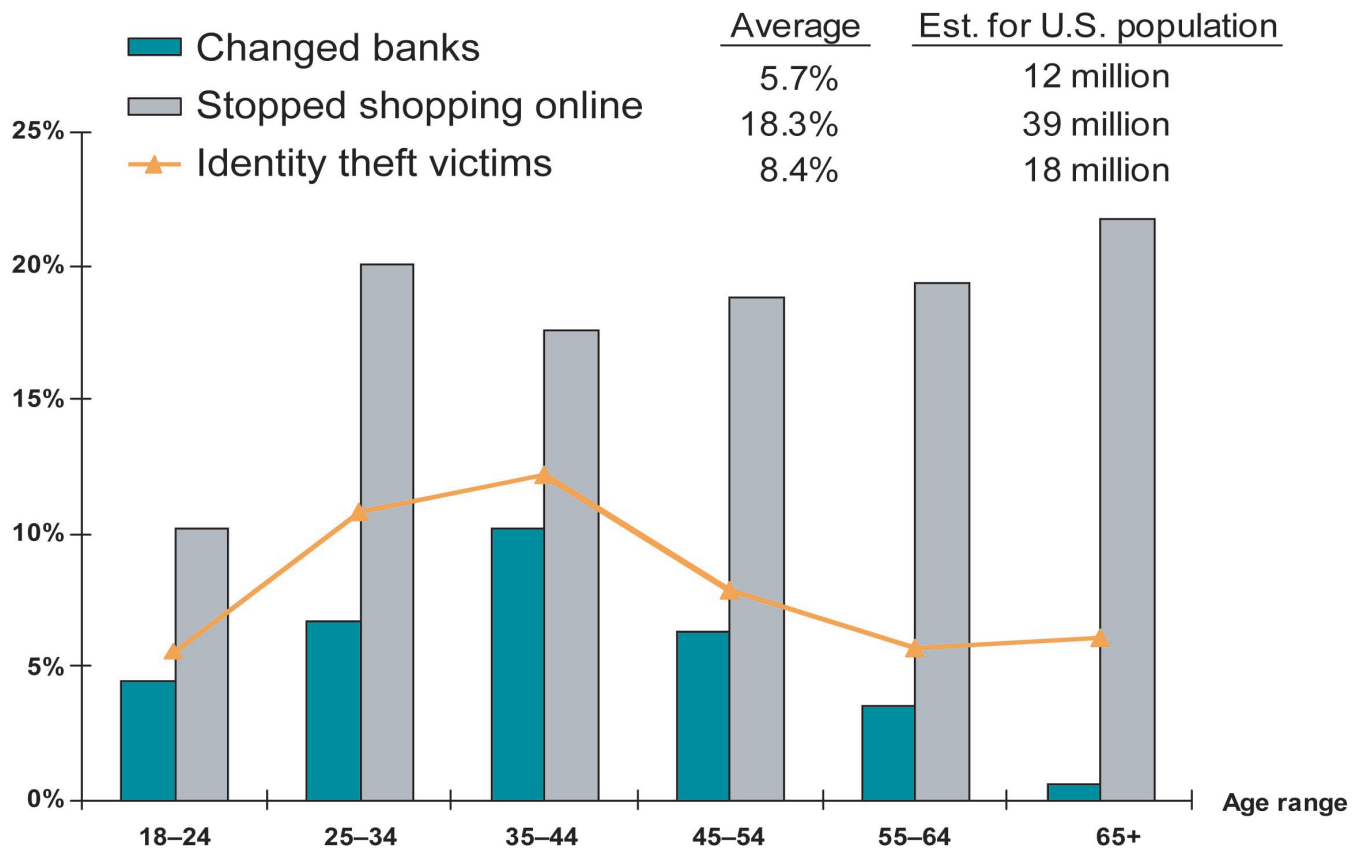
accounts, and leave in search of a safer financial relationship.

FUTURE OUTLOOK

Security and Risk Management Are Global Priorities

Overall, financial institutions have done a good job of taking information security and operations risk management seriously. However, in a world increasingly without borders, financial institutions are refocusing their efforts on managing and protecting their information assets. Regional variations mean that institutions have varying security challenges based on their geographic location:

Figure 2: Consumer Actions to Reduce Risk of Becoming a Victim of Identity Theft, by Age Group



n = 1,000

Source: Financial Insights, 2007

- **North America, particularly the United States, has suffered at the hands of highly publicized security breaches, and regulatory change is mandating that banks place an increased emphasis on data security.** Security and fraud management was one of the top 10 strategic IT priorities identified by Financial Insights for 2006 as large banks focus their efforts on integrating their security efforts in order to gain enterprisewide visibility. While large organizations have continued to invest in specific security controls, some have also focused on business process auditing and reengineering to ensure that security technologies, policies, and procedures are functioning appropriately at the enterprise level. Bank of Montreal (BMO) pursued BS7799 certification of its Information Security Management System in order to mitigate risk to its brand and reputation and develop SOX's auditable documentation.
- **Data management and security are top priorities for European banks.** Recent regulatory changes in the United States have prompted European institutions to step up consumer information protection under the assumption that European legislation will soon be more involved with this widespread concern. Recent research from Financial Insights European practice indicated that security technologies, data warehousing, and content/document management technologies were the top 3 investment priorities for European banks.
- **Asia struggles to balance dramatic growth with managed risk.** Recent compromises to data in India's burgeoning call center

and business process outsourcing industry have focused new attention on offshore security and privacy standards. Security breaches are not uncommon, including the illegal and unauthorized sale of more than 1,000 U.K. bank accounts to a British newspaper. While these incidents have not created any significant backlash, the Delhi based National Association of Software and Service Companies (Nasscom) is proactively working with the Indian government to toughen data protection laws. Additionally, Nasscom is taking further precautions to mitigate the risk of employee-driven fraud or theft by creating a centralized information repository for conducting background checks on job applicants.

Basel II compliance is an overarching global theme that will eventually require all financial institutions globally to tighten operational risk management and mitigation policies and procedures.

CHALLENGES AND OPPORTUNITIES

The financial services industry will always be subject to increasingly sophisticated criminals seeking financial gains from the valuable customer and corporate data safeguarded by these firms. Criminal schemes will continue evolving to stay ahead of security solutions. Regulators and legislatures will continue to put pressure on financial institutions as a reaction to security breach activity. Financial services firms must take a proactive, rather than reactive, approach to security. In order to maintain a proactive posture, financial institutions must constantly evolve. They must evaluate strengths and weaknesses in

corporate policies and procedures and consumer-facing security measures and make appropriate adjustments to encompass the latest technology, criminal, and security trends.

End-to-end system management is also growing in importance as applications increasingly become componentized, integrated, and partner- or customer-centric. IT must now be able to monitor, manage, and optimize, if possible, services that are not on its premises or under its direct control. Furthermore as threats from viruses, Trojans, hackers come closer to the applications, system management must be able to look beyond the management of networks, hardware, and basic systems processes into the applications themselves. These are difficult tasks with the typical patchwork of IT management tools.

An example of end-to-end system management is health savings accounts (HSAs), where a bank, core processor, and plan administrator seamlessly provide a single service to the consumer composed of components from each. In Europe, large institutions such as Royal Bank of Scotland have partnered with major retailers like TESCO to originate mortgage loans. An example of entry into the corporate customer supply chain is outsourcing services such as HSBC Accounts Payable Integration, which delivers accounts payable processing outsourcing to its customers in partnership with Bottomline Technologies.

Financial institutions must take a more holistic enterprisewide view of security and operational risk mitigation to avoid exposure to legal, brand, and reputational risks. Within this holistic approach, the financial industry must grapple with two pain points.

Endpoint Security

The proliferation of remote access using both traditional and wireless connections is straining security protocol at financial institutions. Remote access has exacerbated the need for effective endpoint security because even more precautions must be in place to protect the organization from unauthorized access. Endpoint security seeks to protect corporate networks from threats associated with remote access, mobile devices, and poor client security practices. Endpoint security also seeks to protect the financial institution's network by carefully controlling which individuals are allowed access and what network resources they may utilize, which is critical to combat internal fraud.

Financial institutions face the same issues as those in other industries — enterprises don't know if remote users are running their endpoint security solutions as intended. Access to corporate networks by remote users is pervasive and on the rise. Employee use of laptops, remote desktops, and wireless devices is predominant to access corporate networks. With this increase in wireless connectivity to financial institution systems, endpoint security has become a top technology concern, particularly at large organizations.

Industrialization of the Financial Value Chain

Industrialization of the financial value chain is occurring as banks integrate with the processes of their customers to generate new revenues and use partners in the delivery of services to customers, either directly or as business process outsourcing. With the increased sharing of information across processes within

and outside the organization's walls, the concept of federated identity becomes critical. A federated identity is a single user identity that can be used to access a group of Web sites bound by the ties of federation. Without federated identity, users are forced to manage different credentials for every site they use. This collection of IDs and passwords becomes difficult to manage and control over time, offering inroads for identity theft.

Federated identity becomes more important as the IT resources, applications, and personnel of customers and partners become part of banks' products and services. IT must now manage not only the identity and permissions of individuals but Web services components as well. Federated identity provides the means to share a single application across multiple trusted partners.

ESSENTIAL GUIDANCE

Actions for Institutions

The need for a holistic security solution is mandatory for financial services firms across the globe. Financial institutions must satisfy operations risk regulatory requirements as well as security mandates to avoid hefty penalties and unfavorable headlines. Financial services executives today must plan to mitigate the many risks associated with securing the enterprise, including customer and revenue loss, financial penalties, tarnished reputation and brand, and legal ramifications.

Leading banks and financial services firms recognize the importance of an enterprise approach to security, fraud, and operations risk management. Financial institutions can benefit from best practices to design or upgrade their own protective environment. A trusted

security partner can help navigate the complexities to arrive at a comprehensive, enterprisewide, cost-effective security solution. To this end, financial services organizations should consider the integrated capabilities of a security partner in the following areas:

- **Data and application security.** Protects non-public consumer and corporate information and the applications that move them as maintained within the organization on mobile devices, transmitted across wireless networks, accessed by consumers, and housed or used by service providers.
- **Network security and redundancy.** Wireless network access is a relatively new concern in the industry, and security providers should understand the unique challenges as well as preventative measures available.
- **Virus detection.** New viruses are constantly coming down the pike and are increasingly more damaging in nature. Security providers with extensive experience in virus detection and network security will be better skilled to provide protection to the financial institution.
- **Identity management and authentication.** Managing the identities and authenticating internal and external users are critical to protecting access to non-public information. Federated identity is becoming more prevalent.
- **Business continuity.** Proven effectiveness in backup, recovery, and restoration is the foundation of a comprehensive security solution.
- **Physical security.** This is an essential criterion in a service provider's datacenter locations.

Copyright Notice

Copyright 2007 Financial Insights, an IDC company. Reproduction without written permission is completely forbidden. External Publication of Financial Insights Information and Data: Any Financial Insights information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate Financial Insights Vice President. A draft of the proposed document should accompany any such request. Financial Insights reserves the right to deny approval of external usage for any reason.

CORPORATE HEADQUARTERS

5 Speen Street, Framingham, MA 01701 USA • Direct +1.508.620.5533 Fax +1.508.988.6761



Financial Insights provides independent research, custom consulting, and detailed multiclient studies on the technology issues and challenges facing the financial services industry. Our global research covers topics of strategic importance to corporate and retail banks, insurance carriers, asset management firms, and securities and brokerage firms. Our local practices in Asia/Pacific, Europe, Latin America and Canada add an in-depth regional viewpoint. Financial Insights, an IDC company, is headquartered in Framingham, Massachusetts, USA.

IDC is a subsidiary of IDG, the world's leading IT media, research, and events company.

Visit www.financial-insights.com for more information.

Regional Locations

United States: Framingham, MA | New York, NY

Europe: London, UK | **Asia/Pacific:** Singapore

Canada: Toronto, Ontario | **Latin America:** Miami, FL