

Information Risk Management in Financial Services



TOWERGROUP

The Power of Knowledge

Rodney Nelsestuen

Financial Services Strategies and IT Investments

August 2007

Executive Summary

Security is the heart of the sound yet flexible information risk management discipline required in the global financial services industry today. Given the speed and interconnectedness of business, managing risk to ensure security has become a necessary core competency for any financial services institution (FSI). Integrated risk management, which involves a holistic fabric of people, processes, and technology, is needed to manage the many risks to customer and business information.

This whitepaper is intended for senior managers and leaders in the financial service industry. It addresses the critical need for institutions to take a holistic view of information risk management. Doing so requires developing a comprehensive understanding of the enterprise's information needs and risks and then structuring a holistic approach for managing this information. Besides their defensive role in protecting information and meeting regulatory compliance requirements, security practices can add value to the institution's products and services. Executive leadership must understand and address the following points.

Integrated Risk Management. Taking an integrated approach to information risk management for the enterprise means moving beyond the inconsistent and reactive manner in which many FSIs address risk. Reputation and brand image are put at risk when security fails and information is lost, stolen, or misused. Moreover, if needed information is not available when and where it should be, an FSI risks losing its customers' confidence, degrades its competency, and puts the brand and overall institutional reputation at risk.

Value Add. Practicing a holistic approach to security and information risk assures that business information contributes to achieving marketplace and business goals, maintaining a customer and business focus, and building confidence in the institution in the marketplace. In short, information security policy, practices, and technologies that provide a defense for information also can support the business's offensive strategy.

A Flexible Defense. An FSI must constantly refresh and update its security practices and underlying technologies to defend against constantly evolving fraud mechanisms and regulatory requirements and to facilitate secure delivery of services through new and increasingly diverse channels. Together with a well-managed governance approach, these actions provide sound yet flexible security.

TowerGroup Research is available on the Internet at www.towergroup.com

© 2007 The Tower Group, Inc.

May not be reproduced by any means without express permission. All rights reserved.

TowerGroup is a wholly owned subsidiary of MasterCard Worldwide and operates as a separate business entity with complete editorial independence. MasterCard Worldwide is not responsible for and does not necessarily endorse any opinions, statements, or other content presented by TowerGroup.

Security and Information Risk Management

Like a living organism, a financial services institution is made up of a host of discrete parts and myriad unseen elements. Information is the lifeblood of a financial services institution, and security is its immune system. Good security prevents alteration and loss of the FSI's DNA: data and information. Security is itself the foundation of risk management across all lines of business and departments, assuring that the information is available when and where it is needed.

Consequences of failed information security are staggering. Private information of 159 million consumers has been lost, stolen, or misused in the United States since 2005, according to the Privacy Rights Clearinghouse. Documented breaches include general computer hacking, employee fraud, organized crime, social engineering, and even simple human error. The mode of loss is unimportant to the public, however, which expects that companies will properly safeguard customer information.

The Business Must Lead

Not long ago, discussions about information security typically occurred at the technical level and largely excluded business leadership. Network breaches and malicious attacks, denial of service, and worms and viruses were considered the purview of IT staff. FSI leaders simply wanted to know that the enterprise had a "rock solid" security foundation and that their technology was "impenetrable." This image has proven to be shortsighted because it implies that good security is a hardened, immovable shell around data and information assets. Rather, security must be flexible as well as strong. It must be able to meet evolving business and environmental needs and must be adapted as new customer segments, delivery channels, and new threats emerge, grow, and change.

Eventually business leaders began to understand that they needed to be involved in establishing security practices because it was *their* business data and information that was at risk on a number of different fronts. Early efforts to cover all potential holes had resulted in a patchwork of technology and policy additions. The changes were ad hoc and inconsistent, often driven by a need to meet minimum compliance standards, and they were not well orchestrated across the institution. This piecemeal approach to security continued until senior management saw IT costs escalate and began questioning the return on their investment in security technology.

To meet demands for fiscal and risk management accountability, today's leading FSIs are aggressively pursuing an integrated approach to risk across lines of business and operations. However, even then, coordination remains a challenge. For example:

- One North American bank had decided on a single enterprise solution for intrusion detection but had four different implementations, each managed by a different technology unit. Although it is true that technical configuration may vary for credit cards as opposed to, say investment products or deposits, ineffective governance in this case resulted in duplication of licensing fees and even more costly duplication of personnel functions. The organization only partially reduced the inefficiency that had

characterized the previous helter-skelter proliferation of its security technology and policy.

- Another global institution has 17 senior executives whose main function is to manage different areas of risk. Although their accountabilities are clear, this approach has resulted in significant and costly duplication of people, process, and technology.

These examples highlight the challenge of integrating information risk management across a financial institution. Risk can be categorized into four basic areas: strategic, operational, financial, and regulatory, as shown at left in Exhibit 1, a conceptual view of the extended universe of risk in need of comprehensive risk management at an FSI.

Exhibit 1



Integrating the Risk Management Universe, Leveraging the Overlaps



Note: BPO = business process outsourcing; HR = human resources; BCP/DR = business continuity planning/disaster recovery; KYC = know your customer.

Exhibit 1
Source: TowerGroup

The exhibit demonstrates the many areas of information risk to be managed. The institution must know where all information resides, understand the importance of that information based on an enterprise-wide information classification system, and engage domain experts in the development of appropriate risk management policies and processes. Because so many risk categories overlap, uncoordinated point solutions can result in costly redundancy in some areas and critical gaps in others. Information gathered on fraud attempts may be managed by several different technologies in the FSI and by different departments and personnel. Lack of

coordination among them is likely to result in gaps in risk management. For example, intrusion detection information from a network system must coordinate with the fraud detection and management system to provide a clear picture of an event and to manage it effectively. Use of disparate technologies can also result in unnecessary overhead as data is moved from one system to another for regulatory and management reporting needs.

The four basic types of internal risk (strategic, financial, operational, and regulatory) shown in the left half of the exhibit can be further divided into the eight areas shown in the right half. A holistic approach to risk management enables the domain experts in each of these areas to be accountable without duplication of effort. It requires an integrated policy for information classification and management that should provide the transparency needed for sound business management.

KEYS TO IMPROVED RISK MANAGEMENT

A few key changes set the stage for improved risk management.

Know where information and data exist

Not all FSIs have a good approach to data discovery, especially if they have undergone mergers and acquisitions that resulted in an increased number of systems and applications in the enterprise. In addition, vital data often resides in employee spreadsheets or documents, where it is unknown as a corporate asset and lacks the protection of established security systems and practices. Vendors of security solutions may have to partner with providers of data and information discovery technologies if their solutions lack discovery capabilities. Sometimes critical information exists only in people's heads. Capturing and managing such intellectual property requires proper documentation, which must be specified by policy. Policy adherence standards must then be built into job descriptions and the performance management system.

Monitor data, information, and system access throughout the FSI

Monitoring should be automated, real time, and continuous, and the system should generate strong alerts if data in transit is at risk. Case management tools need to be accessible at several levels. Besides having tools capable of managing the details of suspected or real security breaches, management must have a higher-level view into these cases as they are discovered and managed. Risk monitoring capabilities should allow for both an aggregate view of active cases and case prioritization based on level of risk.

Protect information

To protect customer information, the FSI needs to use good business practices and enforce policies that encourage sound and systematic data access. In addition to security technologies, policies must be readily available and accessible via multiple devices so that the hard work put into policy development bears fruit. Ensuring compliance requires that users know and respect the information, security, and risk management policies. One tactic is to have the system generate policy pop-ups when users innocently attempt to do something beyond their security clearance. Pop-ups can be designed to communicate a wide range of information (for example, outlining the process to gain authorized access) or simply to reinforce security policies.

Assure information availability

Protecting data from misuse is not enough. It is equally important to assure that data is available to the right people at the right time in order to serve the business goals and objectives of the institution effectively. For this reason, information security policies should also contain standards and goals for information *availability*.

Have an effective "Plan B"

Real-time transactions and any-time access are becoming a core requirement for financial services. Therefore, business continuity planning (BCP) has resurfaced as a critical necessity. Disaster recovery methods and processes for hardware and software are readily available and in most cases are standardized and effective. But system and application availability means little if the firm has not established and tested operational processes and trained personnel on those processes to assure continuity of the business itself when an operation is either degraded or cut off entirely by some natural or manmade disaster or technological failure. Moving from a centralized service unit to a work-at-home or even mobile environment requires planning for access and security through a number of access points, channels, and providers. These links need to be tested on a periodic basis.

- In the disastrous events of 9/11, Cantor Fitzgerald, the bond trading company to much of the bond industry, lost its data center and connectivity along with hundreds of its employees when the World Trade Center collapsed. Because the company had a concurrent data center in New Jersey that ran in a real-time mode and alternated processing with the New York site, the disaster recovery was complete as far as the data center was concerned. Nonetheless, business was interrupted. Both of the proprietary networks went through the World Trade Center office. The company had to establish secure connectivity both for employees working from several locations and for customers. In most companies, doing so could have taken weeks. Because Cantor Fitzgerald had a network connection between New Jersey and its London office and could leverage Internet connections, the firm was able to return to business within 48 hours with the help of numerous companies, including Compaq, Verizon, Cisco, Microsoft, and UBS PaineWebber.

INTEGRATED RISK MANAGEMENT

To integrate its people, policy, process, and IT, an enterprise must coordinate all these elements in a holistic framework. Exhibit 2 shows that the IT infrastructure is but one important part of the enterprise approach to risk management called integrated risk management (IRM).

Exhibit 2



Integrating Information Risk Management with the Business and Technology Framework

Risk and reward decisions include the business and marketplace strategies of the enterprise

Operations are improved by closing the gaps between areas of accountability and by broad attention to compliance

Efficiency results from reducing duplication and increasing departmental and individual accountability across functions

Controls assure that structures remain in place

Integrated risk management (IRM) requires integration of all elements of an enterprise, from strategy to infrastructure, and from reporting to data

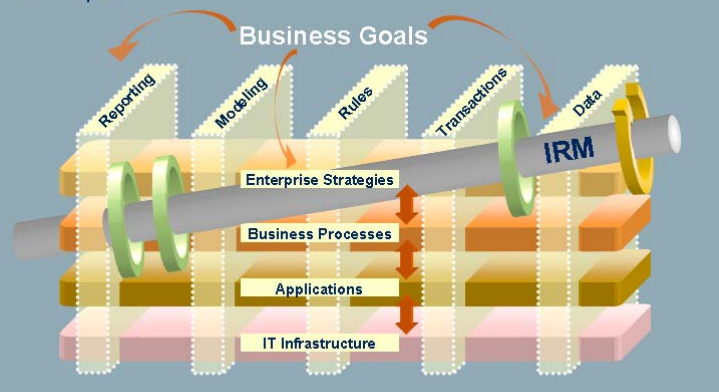


Exhibit 2
Source: TowerGroup

Applications cannot be secured without attention to business processes as well as the enterprise's business strategy. Some FSIs approach the marketplace with a "high-touch" philosophy that involves much interaction with customers. Others seek to be a low-cost, or transactional, provider. High-touch providers expose a richer set of customer data to internal or external users as they seek to demonstrate to customers a high level of knowledge of their individual financial needs and meet individual preferences. Transaction-based FSIs need closer attention to moving data because speed and efficiency are a part of the business value proposition, which poses its own form of risk.

Integrated risk management involves both the business requirements and the technology architecture at all levels of the institution. Integration creates a balanced approach to risk and establishes clear accountabilities. The removal of organizational walls results in better coverage of internal and external risks, including fraud and reputation risk. As Exhibit 2 demonstrates, IRM incorporates the many organizational elements of strategy, process, applications, and IT infrastructure for better execution of the daily business of transactions. IRM also uses analytics strategically to anticipate and improve business results, and it improves control by improving data quality and compliance with internal and external requirements. Finally, IRM improves transparency and visibility into all facets of the business through enhanced and more accurate and timely reporting.

As regulations and business risks change, businesses often respond with new categories of risk management. The problem with this approach is that it creates a new management function and often results in wasteful and costly duplication of effort and resources. IRM requires the coordination of every type of risk throughout the FSI, along all lines of business and operations.

Security breaches are more likely if an institution has uncoordinated risk areas than if it has an integrated approach to risk management. IRM imposes controls and processes to reduce the potential for breaches from external sources. This includes risks of loss of FSI information by trusted business partners. Two examples follow.

- In 2005 ChoicePoint, a vendor of consumer information, was duped into providing fraudulent companies with information on 163,000 customers. These companies posed as legitimate organizations buying legitimate information about these consumers. This example of modern and sophisticated social engineering resulted in 800 cases of identity theft. The Federal Trade Commission (FTC) fined ChoicePoint \$10 million in civil penalties and \$5 million for consumer redress. The consequences of fraud for this vendor went beyond fines and penalties. The FTC also imposed requirements for costly due diligence processes and specific and periodic external audits going forward, all of which will increase the cost of security for ChoicePoint.
- In 2007, Fidelity National Information Services revealed that its subsidiary, Certegy Check Services, Inc., had been the victim of internal fraud by a former employee. The perpetrator sold bank and credit card information on potentially 2.3 million consumers to external companies for marketing purposes. The misuse of the information is not believed to include fraud or identity theft, but the long-term effect of this breach is as yet unknown and it cannot be guaranteed that misuse will not occur.

These examples highlight the need for financial services institutions to know whom they are doing business with. The FSI must ensure that all business partners have policies and technology in place to safeguard any information they may be handling for the institution. In short, an FSI must require vendors and trusted business partners to commit to processes that align with the FSI's own risk management approach.

The Legal and Regulatory Environment

The alphabet soup of global regulators compounds the compliance challenge facing financial services institutions, which must meet the requirements of varied and rapidly changing regulations. In Europe, the EU Data Protection Directive requires all FSIs to assure that security measures are in place to guard against the accidental loss of personal data and prevent fraudulent activity. The directive also addresses inadvertent loss of data and corruption or other damage to data. In the United States, the Federal Financial Institutions Examination Council (FFIEC) views security as an evolving area and issues new requirements and directives as threats to business change, such as recommending two-factor authentication.

USER AUTHENTICATION

Globally, more FSIs are subject to stronger authentication requirements for business conducted online, via telephone or in a mobile environment. For example, in 2005, Hong Kong mandated stronger authentication for third-party and other "high-value" financial transactions, to reduce threats from phishing attacks. Singapore mandated two-factor authentication for high-value transactions in 2005 and extended that requirement to all online transactions by the end of 2006. These requirements go beyond the simple and more traditional two factors of something you have (a card) and something you know (a personal identification number, or PIN) to involve authentication via a separate channel. An example of such "out-of-band" authentication would be a text message or even a phone call generated at the time of login. Another alternative is a one-time password generated on an electronic fob or "token" that a user carries on his or her person. In many countries, the United States included, users' perception of these more complex two-factor authentication processes as a "hassle" may limit their effectiveness and their adoption. Consumers may perceive FSIs that do not adopt two-factor authentication as easier to do business with than those requiring another step of consumer participation in security. This is arguably a false advantage, but consumers drive the industry, absent strong legal and regulatory requirements to the contrary.

A more convenient user authentication solution, whose popularity will grow over time, is the use of biometrics, including fingerprints and retina scans or facial scans. Login will probably still be required as backup in case the biometric fails (e.g., because of a smudged fingerprint scanner), so biometric solutions will be one factor of a two-factor authentication solution. Consumers may initially be uncomfortable with biometrics, perceiving it as a physical intrusion.

An alternative security solution depends on analysis of consumer habits to make sure that a user requesting access is who he or she claims to be. Known as risk-based authentication, this process uses analytic software to evaluate requested and observed customer information and other data captured during an online transaction and compare it against the presumed customer's characteristic behavior patterns. A customer's Internet Protocol (IP) address, device characteristics, and stored certificates can be used to establish and authenticate the user's identity to a higher level of certainty. In this approach, policy establishes risk parameters for deployment of increased security practices. Solutions from leading security technology vendors already have the ability to set policy parameters at different levels and automatically detect when to enforce them.

GOVERNANCE AND COMPLIANCE

Security has several interrelated layers. At the most important level, security addresses the actual risks to the business and its customers. Ideally, these risks are managed according to the FSI's own well-developed policies and governance structures. They are also managed for purposes of regulatory compliance, which is a fact of life in the industry. Although regulations may overlap between regulatory bodies, there are often differences in interpretation by the agencies when enforcing regulatory compliance. Exhibit 3 suggests the challenges any financial services institution faces in responding to the regulations, regulators, internal standards, and, ultimately, the risks themselves.

Exhibit 3



Regulation, Regulators, Policy, and Risk

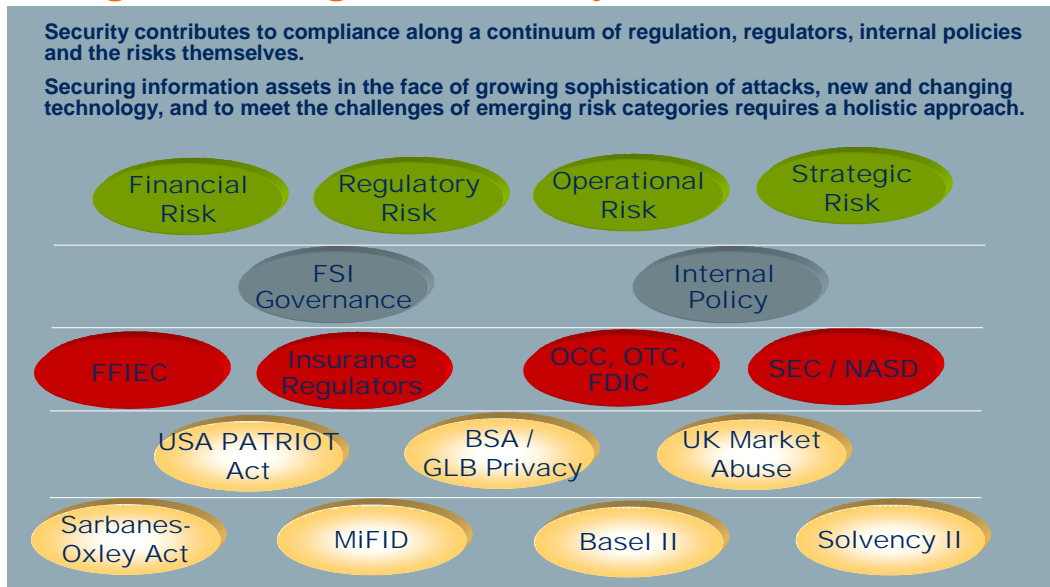


Exhibit 3
Source: TowerGroup

Exhibit 3 demonstrates the many audiences interested in information security. The lower half shows a sample of regulatory agencies and regulations that impact information, security, and risk management. In addition to the FFIEC, US regulators include the Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTC), Federal Deposit Insurance Corporation (FDIC), Securities and Exchange Commission (SEC), and National Association of Securities Dealers (NASD). Besides the USA PATRIOT Act, US regulations include the Bank Secrecy Act (BSA) and Gramm-Leach-Bliley Act privacy requirements, and Sarbanes-Oxley Act. Regulations from outside the United States include the UK Market Abuse protections, the European Commission's Markets in Financial Instruments (MiFID) directive, the Bank for International Settlements' Basel II guidance, and the European Union's Solvency II initiative.

However, regulatory requirements simply formalize activities and policies that an FSI should have in place for its own well-being. Thus, above the regulations and the regulators, the schematic shows FSIs' internal policies and processes. Of course, no regulation, regulator, or FSI policy is conceived for its own merit. Instead, it is intended to serve and protect customers and the institutions themselves. With this business focus, we can turn to the value of information security as a differentiator contributing to marketplace success.

Marketplace Advantage of Improved Information Security

Exhibit 4 presents "SECURE" as a mnemonic associated with the benefits and marketplace advantage of securing information. Security and risk management support the marketplace goals of an FSI, especially the objectives of achieving organic growth and entering new markets.

Exhibit 4



SECURE: The Marketplace Value of Integrated Security and Information Risk Management

Secure – for customer trust

Execute – for customer confidence

Control – for customer service

Ubiquitous – for multiple channels

Return – for increasing share of wallet

Excellence – for marketplace differentiation

Exhibit 4
Source: TowerGroup

TRUST AND CONFIDENCE

The concepts outlined in Exhibit 4 provide a framework for management to think about the value of security and a holistic approach to both security and risk management. Two elements of this larger framework directly affect how the *marketplace* views the organization, and both are core to fostering organic growth.

- **Trust** is the customers' belief in the financial institution and view of its employees, products, and services as reliable.
- **Confidence** is the customers' belief in the *competence* of the financial institution.

In short, trust means that customers believe the FSI will do the right things with the information it has. Confidence means the customers believe the FSI has the ability to protect their information from those with ill intent. Both trust and confidence are important. In one survey of European customers, 65% indicated they would seriously consider leaving their financial institution if they lost trust or confidence that their information was safe. With a strong reputation of trust and confidence in place, the FSI is better positioned to achieve its marketplace goals.

CUSTOMER SATISFACTION

Information security technologies and practices can be structured to support the business and directly contribute to growth. Patterns of customer access and usage collected by authentication systems can add value beyond playing a defensive role in detecting and stopping unauthorized access. Customers' attempts to access restricted areas may signal one of the following needs:

- The need for training and information. Training can improve the experience and satisfaction of those customers. Without it, they may become dissatisfied if, because of their lack of knowledge, they continue trying to access the wrong systems and applications.
- New opportunities for cross-selling or up-selling products and services if a customer is trying to access areas for which they currently have no products or services.

Understanding usage patterns can help an FSI to enhance customer service by indicating where to redirect resources as customer habits, life cycles, and change over time.

CHALLENGES OF AN EVOLVING ENVIRONMENT

Not only does customer behavior change over a long-term relationship, but new customer segments, markets, and delivery channels emerge and evolve. Information security policy, processes, and technologies need to evolve in response. For example, the expectation that private information will remain secure is challenged by the popularity of virtual social networks, which encourage interactive sharing of information by users. New and emerging usage habits and online practices compound the need for information security to play both an offensive and defensive role in financial services. A single-user interface can expose multiple applications and sources of information and data simultaneously, a trend that will increase as the Web becomes the platform for business in Web 2.0.

From the perspective of more traditional new markets and migration of current market segments, one trend of growing importance for information security practices is the aging of the population. The rapidly expanding population over age 65 controls approximately 70% of financial assets in the United States. Customers in this cohort are especially vulnerable to fraud and theft for two reasons. First, many have less experience with electronic channels than do younger generations and therefore might be susceptible to techniques such as phishing. Second, the sheer size of their portfolios makes them high-value targets. With so much at stake, fraud prevention is as important as detection. Fraud prevention requires a holistic approach to security, one that covers both technological and nontechnological security

practices, including consumer education. User education at all levels is a crucial aspect of any information security approach in financial services.

Security's value for both defense and offense

Exhibit 5 lists some of the key roles for security as both defense and offense.

Exhibit 5



The Business of Security: a Holistic Value

| Defense | Offense |
|---|--|
| ▶ Stopping unauthorized access to systems and information | ▶ Assuring needed access to the right users at the right time |
| ▶ Stopping misuse or theft of information | ▶ Building trust in the marketplace |
| ▶ Serving as the basis for fraud and risk management | ▶ Establishing customer confidence in the institution's competence in handling information |
| ▶ Protecting intellectual property | ▶ Observing customer behavior to identify emerging needs |
| ▶ Meeting compliance requirements | ▶ Evaluating customer segmentation for building relationships with at-risk populations |

Exhibit 5
Source: TowerGroup

A flexible foundation for meeting new threats

Among the emerging threats are new security issues with respect to employee behavior as well. With the Internet now an indispensable tool in business and its resources, younger workers, including "millennials" (people born at or near the end of the 1970s, who came of age in the new millennium), regularly have multiple Web sites open on their desktops, including streaming music or video, as they multitask and combine work and lifestyle activities. Although traditional managers may be shocked at this idea and think that access to outside online sites can be limited, it is clear that the emergence of new work styles is a force to be reckoned with.

Users have also adopted newer "convenience" technologies such as Universal Serial Bus (USB) devices, or thumb drives. These represent a new form of an old threat, especially in

to information security will make the difference in the level of effectiveness achieved with the security measures.

Leveraging the Cost of Security

Good security will limit loss of information as well as limit the risk of financial loss. Integrating information security across the enterprise can also help an FSI to lower costs by reducing redundancies while effectively managing risk. In addition, it can help identify business areas where resources are poorly leveraged. For example, older products and services may have reached the level of maturity at which historical resource allocation and capacity exceed the value of the service as perceived in the marketplace. As products and services evolve across their life cycles, the data that security tools and technologies capture about user activity can serve as business intelligence that can lead to more efficient future deployment of IT resources.

FSIs must be able to leverage every IT investment they make to achieve operational leverage. Technology vendors have an opportunity to move from playing a largely defensive game in security to providing leading-edge customer intelligence through repurposing system-captured data and information about customer behavior. To extend business and customer value, vendors must build flexibility around security needs. They must enable FSIs to meet numerous and changing global regulations as well as customer privacy, protection, and reporting needs. To improve operational leverage from investments in technology, FSIs need solutions that enable and support ongoing simplification in compliance. Reuse of data from one reporting need for another is a fundamental means of leveraging technology costs.

In this regard, enterprise-class vendors have a distinct advantage over point-solution providers. The holistic reach of broader solutions can synthesize information accumulated from all points in the organization and examine disparate data in a manner that creates new levels of business and customer intelligence. Leading solutions not only monitor unauthorized activity but also can monitor authenticated users to provide this added value. Integrated solutions at the enterprise level also have the ability to combine those "double-duty" regulatory compliance and reporting needs while reducing cost or spreading this sunk cost between security for risk management purposes and for marketing purposes.

Tier One financial institutions often have the resource base to leverage separate, best-of-breed technologies in effecting risk management efficiently. Still, a more holistic enterprise approach driven by participative governance will extend the value of IT to yield better business results because stakeholders from all parts of the enterprise will participate in security, information, and other risk management.

Conclusions

Information security requirements change with regulations and with changes to the operating environment. For this reason, while security needs to be sound, it also needs to be flexible. Security is also about much more than basic regulatory requirements for user IDs and passwords or prevention of unauthorized access to or loss of sensitive information. In its defensive role, security is the foundation for effective fraud management. At a higher level, security plays a key role in developing integrated, enterprise-wide risk management competence that protects the institution's business, including its intellectual capital. Finally, information security can be a foundation upon which an FSI builds its marketplace differentiation by leveraging people, process, and technology in a holistic manner.



RSA, The Security Division of EMC, commissioned TowerGroup to conduct independent research and analysis of security and risk management practices and trends in financial services. The content of this report is the product of TowerGroup and is based on independent, unbiased research not tied to any vendor product or solution. Although every effort has been taken to verify the accuracy of this information, neither TowerGroup nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this research or any of the information, opinions, or conclusions set out in the report.