

The **Information-** **Security** *Challenge*

BY R.J. SCHLECHT

Whatever happened to the vision of the easy exchange of information in the 21st century? The Internet was presented as the stage for a new business model where customers, employees and partners would drive business to new heights by communicating via a broad range of media, applications and connectivity. ■ Customers would be able to obtain services and manage accounts through multiple user-friendly tools. Employees could work anywhere at anytime. Trading partners would be connected through a multitude of interfaces, using a variety of savvy methods of

The Mortgage Bankers Association recently issued a comprehensive study of mortgage industry information-security requirements. The study also outlines a five-step model for information assurance that's tailored to residential and commercial lenders' compliance needs.

communication. And all of this activity would be fueled by seamless connections to databases throughout cyberspace. ■ When the Internet protocol was created, it was designed through a U.S. Defense Department research project, with the main design goal of providing a network that would survive cataclysmic events causing massive disruption (read: nuclear explosions) and be able to

route around the affected area, resulting in the rest of the network maintaining connectivity and communication.

The protocol has been put to the test as recently as 2005—when Hurricanes Katrina and Wilma disrupted all electronic connectivity in Louisiana and Florida—and the Internet routed around the areas.

What was not contemplated in its design was network-layer security. Therefore, it was reasoned, security would be added on an as-needed basis at the application or system level.

The door to the utopian open exchange of all information is closing, and fast. The reality of viruses, hackers, phishing, pharming, lost tapes and laptops—not to mention the persistence of plain old fraud—has changed that idealistic vision. Now, the latest news stories are not just “Gee whiz!,” but also “Danger, danger, Will Robinson!” The compromise of nonpublic personal information, corporate misrepresentation of finances and even increased threats to our children are headlining the stories we read today.

Regulators and legislators have been listening and reacting to these developments. Regardless of whether the source of risk is terrorism, criminal activity, or vulnerable databases and poor security practices, firms now must meet new standards established to safeguard our physical, corporate and consumer safety. A whole slew of new legal and regulatory requirements have been imposed on business as a result of a range of new risks that are now apparent.

The Enron Corporation and WorldCom scandals drove the U.S. Congress to legislate improved controls over public companies’ financial records. The Sarbanes-Oxley Act of 2002 and the Public Company Accounting Reform and Investor Protection Act established specific accountability for boards of directors, management and auditors as to the correctness and accuracy of financial reports.

The USA PATRIOT Act was signed into law in response to the Sept. 11, 2001, terrorist attacks against the United States. A portion of that statute defines requirements for businesses to better understand who their customers are before engaging in financial transactions.

In February 2005, Alpharetta, Georgia-based ChoicePoint Inc. suffered a major information-security breach that led to the unauthorized disclosure of nearly 163,000 personal and nonpublic information records, according to the Federal Trade Commission (FTC). What triggered the public announcement of this breach was the California Security Breach Information Act (California S.B. 1386). That law requires organizations holding the personal information records of California state residents to notify those residents should a security breach occur that results in the unauthorized and unencrypted disclosure of those records.

Since the California security-breach legislation, more than 30 states have enacted similar versions of breach and

The door to the
utopian open
exchange of all
information is
closing, and fast.

notifications laws, and similar legislation has been proposed at the federal level.

The breath, depth and multitude of federal- and state-enacted legislation has had a significant impact on mortgage lending. Additionally, regulatory agencies continue to issue and revise requirements for financial controls, the safeguarding of personal information and the flagging of high-risk transactions and identity-fraud red flags at a pace that makes it difficult for firms to stay current.

These regulatory requirements are driving information audit standards and security practices. There are any number of industry best practices for both audits and security frameworks that organizations can use. Some are very comprehensive, potentially expensive and complex to execute. Other audits and security frameworks are less comprehensive, but may not offer assurance of appropriate risk mitigation to regulators and trading partners.

The Mortgage Bankers Association (MBA) has responded to the needs of member companies to adopt well-thought-out, smart, responsive programs that address these regulations and the underlying sources of risk. MBA’s Board of Directors Technology Steering Committee (BoDTech) has identified security as a strategic priority for the industry. The BoDTech Committee reports to MBA’s board, and spans the diverse needs of both commercial and residential members.

The Mortgage Bankers Association (MBA) has responded to the needs of member companies to adopt well-thought-out, smart, responsive programs that address these regulations and the underlying sources of risk. MBA’s Board of Directors Technology Steering Committee (BoDTech) has identified security as a strategic priority for the industry. The BoDTech Committee reports to MBA’s board, and spans the diverse needs of both commercial and residential members.

In October 2005, MBA released a white paper, *Protecting Personal Information (PI): The Good, the Bad, the Ugly*, in order to raise awareness of security issues at the highest levels in the industry. In March 2006, MBA’s nonprofit data standards subsidiary, MISMO®, released a white paper titled *Identifying and Safeguarding Personal Information: Recommended Guidelines and Practices*. And at its 2006 Annual Convention & Expo in Chicago, MBA announced the development of a major study, *A Five-Step Information Assurance (IA) Model for Mortgage Industry Institutions*, as part of a multi-phased approach to provide information, research and educational offerings on this topic.

MBA’s new study researched and analyzed major legislation, regulations, audit standards and security practices for common themes or patterns. The concept of harmonizing these various critical information assurance requirements was to derive a generalized model for the mortgage industry (see Figure 1).

The resulting model is not designed to replace existing practices such as those set forth by the International Standards Organization (ISO), Geneva, Switzerland; the Committee of Sponsoring Organizations for the Treadway Commission (COSO), Altamonte Springs, Florida; or the Control Objectives for Information and Related Technologies (COBIT)—an open standard published by the IT Governance Institute and the Information Systems Audit and Control Association

(ISACA), both based in Rolling Meadows, Illinois.

Rather, its purpose is to aid organizations having difficulty getting their hands around such a large and dynamic target. Most important, the new study sets forth a model for firms to address information assurance from a comprehensive perspective rather than a reactive one that responds to numerous individual regulatory standards. This model is broad-reaching and applicable across all industry sectors and for firms of all sizes. Its chief benefit will be enhanced compliance among trading partners, which in turn will deliver bottom-line return on investment (ROI) to firms as they seek efficiencies and profits through mortgage eCommerce.

The new BoDTech research consisted of identifying major requirements within three basic areas: legislation and regulations, audit standards and security practices. The study identified an “A list” of the most common requirements found in each of the three areas.

Examples of “A-list” legislation and regulations include the Sarbanes-Oxley, Gramm-Leach-Bliley and USA PATRIOT Acts; Securities and Exchange Commission (SEC) Regulation AB; the European Union (EU) Privacy Directive; and regulations from the Federal Financial Institutions Examinations Council (FFIEC), FTC and Government Accountability Office (GAO).

“A-list” audit examples include FFIEC and Federal Deposit Insurance Corporation (FDIC) information technology audit requirements and National Institute of Standards and Technology (NIST) and American Institute of Certified Public Accountants (AICPA) recommendations.

“A-list” information-security standards were developed based on materials from ISO, COSO and COBIT. Within each area, the identified items were analyzed and their rel-

The new BoDTech research consisted of identifying major requirements within three basic areas: legislation and regulations, audit standards and security practices.

evant information assurance requirements highlighted. Common requirements and patterns were then identified and summarized. The final step involved analyzing the three areas together, using the same process to generate a single, harmonized summary.

The results of the harmonization evaluation were interesting. While individual statutes, regulations, audits or security frameworks all have a specific focus, patterns emerged when these were all mapped together. Grouping these patterns logically resulted in the identification of five steps firms can take to build an enterprisewide model for information assurance.

Basic building blocks for information security

This five-step information assurance model represents the basic building blocks for any information security program. These are as follows:

- *Business and risk description*: The foundational step to any information-security program is the definition of business and lines of businesses, identification of assets and risk assessment.

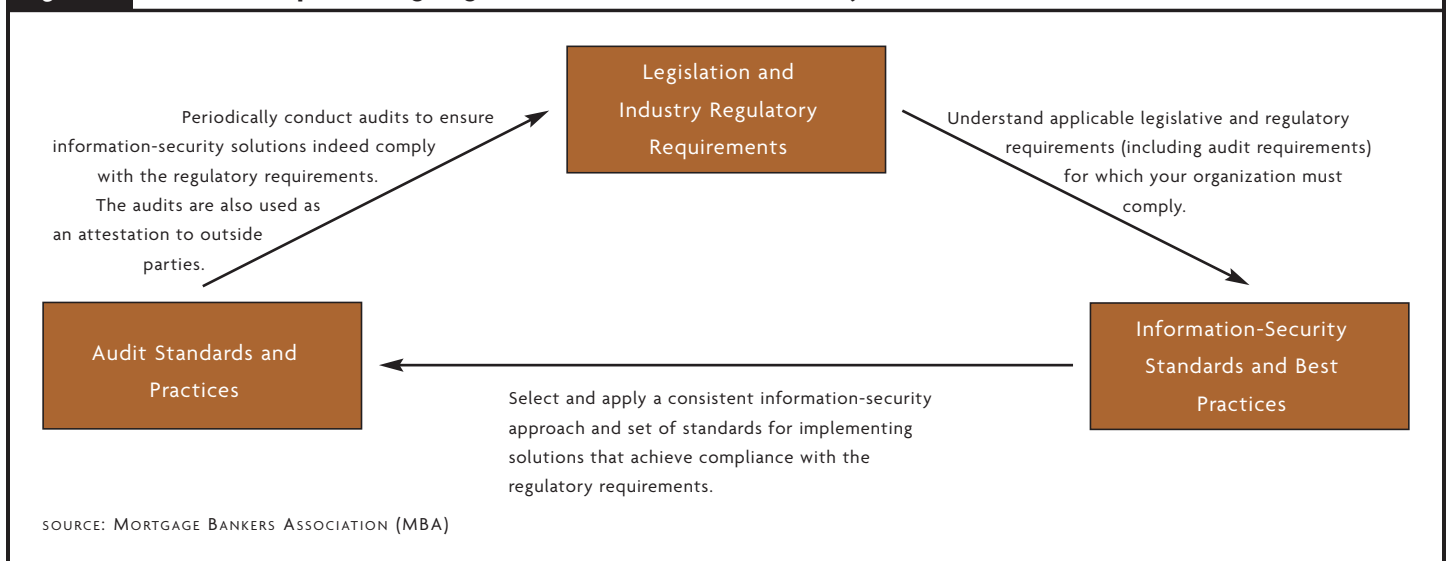
- *Policy and architecture*: The framework defining what an institution must do to satisfy legal and regulatory requirements and conduct successful audits.

- *Solution specification and implementation*: The detailed technology, procedures and personnel specifications, as well as the implementation and execution plan defining how an institution is going to satisfy legislative and regulatory requirements and conduct successful audits.

- *Solution support and re-evaluation*: The testing, monitoring and business continuity assurance to successfully sustain an information-security solution.

- *Education*: The last line of defense that recognizes that

Figure 1 Relationships Among Legislation, Information-Security Standards and Audit Standards



technology and procedures cannot address and mitigate all information risks.

The focus of the IA model centers on identifying and mitigating information security risks within an organization. Legal and regulatory requirements are a critical component of identification and classification of assets. Depending on business models, other assets such as intellectual property (IP) may also be identified as subject to risk. Threats, vulnerabilities and likelihood of adverse events are analyzed in order to assess risk. Together, these tasks make up the first step of the model—business and risk description—by providing a complete understanding of the business environment.

The second step—policy and architecture—entails a deeper dive into a firm's operating environment. This is where mitigation strategies are proposed and high-level policies formulated. These policies are used to evaluate whether proposed safeguards are actually achieving their objectives.

Once a strong foundation is in place, specifications for technologies, processes and people are developed and implemented. Together, these comprise the third step—solution specification and implementation. Throughout the IA model, assessing and re-assessing risk is the overriding principle.

The fourth step—solution support and re-evaluation—provides assurance that practices, procedures and mechanisms used to mitigate risk are achieving the desired objectives. This is done through testing, monitoring, auditing, business continuity and incident-response programs.

The final step—education—is not generally presented as a core component on many lists of information-security best practices. However, the mortgage industry can gain great value from an ongoing program of information-security awareness. The mortgage lending process, either residential or commercial, normally involves multiple businesses and employees. Awareness of corporate policies concerning risks—regardless of regulations, liabilities and corporation reputation—can be viewed as low-hanging fruit, where rewards can exceed expense.

Each step of the five-step IA model has its own specific set of actions. These actions focus on specific activities, such as risk assessment, policy, technology specifications, maintenance, continuity and so on. The ability to break down the core five steps into manageable components aids in the implementation of the IA model.

Following the model helps organizations gain an understanding of their business and risks; helps them adopt effective policies and safeguarding requirements; and aids in the acquisition and support of products, personnel security, certifications and third-party management to safeguard against risk.

By providing a security framework that mirrors a product or service life cycle—from concept and business justification, implementation of process, deployment and product train-

The focus of the
IA model centers on
identifying and
mitigating information
security risks within
an organization.

ing—the model fits nicely into corporate activities. While the model does not specify which controls to adopt, ISO, COBIT or statements on auditing standards (SAS) control statements can be easily leveraged so that firms can extend what is already in use across their operations.

In fact, the IA model was created specifically so that firms could establish a comprehensive set of processes that would cover the requirements of the many compliance programs with which they must comply. These compliance programs, spanning legal and regulatory requirements, audit practices and security frameworks, contain both very broad and very targeted obligations for firms.

The overlaps and gaps among these different programs have resulted in confusion for those seeking to comply. When there is a choice, the multitude of audit practices and security frameworks have left some questioning which choice is best for their business, and how that selection will impact their relationship with trading partners or service providers.

From an internal perspective, management needs to decide which programs are best-suited for a firm's specific business strategy. From an external-trading-partner perspective, senior executives must determine which programs provide the "correct" level of assurance and the least disruption of service. And then there is the question of how a firm can avoid having to start over with each partner.

A comprehensive approach moves an organization to a proactive position in deterring risks to information security rather than a reactive one. The IA model provides firms with a risk-based approach that identifies assets, architectures, policies and procedures. When, for example, regulators adopt changes to an existing regulation, a firm following the IA model has the foundation in place so that needed changes can be implemented efficiently. Taking a comprehensive approach also reduces the silo effect, where firms have established "islands" of information security for specific applications and processes. The more global approach enables a holistic view of security and vulnerability across the entire enterprise.

Because the five-step IA model is built upon the common elements of various audit standards and security frameworks, their content is evident throughout the model. For example, ISO's (plan-do-check-act) and COBIT's (plan-build-run-monitor) four-step processes have analogs in the MBA five-step IA model, as does NIST's three functional areas (management, operational and technical safeguards).

Where the MBA five-step IA model differs is in its inclusion of a specific educational component. This recognizes that information assurance is truly an enterprisewide activity, and that an organization is only as strong as its weakest link. Setting forth a specific step for education and awareness strengthens all the links.

The MBA five-step IA model also calls for specific participation by and approval from a firm's senior management.

Senior management tie-ins have become a standard feature of the legal and regulatory landscape, as demonstrated by Sarbanes-Oxley and the proposed identity-theft “red flags requirements” of the Fair and Accurate Credit Transactions (FACT) Act. The five-step IA model’s recognition of this reflects the market need for forward-looking guidance.

Reducing the compliance burden

In the end, the five-step IA model provides a way for the mortgage industry to reduce the burdens imposed by numerous different requirements all aimed toward a common goal: the ability to assure that information, data, applications and processes are in place to protect a firm, its operations and its customers.

The Internet has come a long way. More businesses than ever—both within and outside the mortgage industry—are connected and in the process of enabling or expanding their transactions to be Internet- or Web-services-based. The time is now to consider what information is sensitive and how to better protect it in motion and at rest.

The mortgage banking industry has an opportunity to take

steps today that will further protect it before security problems become more widespread. MBA is prepared to help in this critical arena. Its *Five-Step Information Assurance Model for Mortgage Industry Institutions* is one example of this. The document is available for purchase at the Online Store on MBA’s Web site (www.mortgagebankers.org).

Additionally, both the MBA Residential/Single-Family Board of Governors (RESBOG) and Commercial Real Estate/Multifamily Finance Board of Governors (COMBOG) have ongoing activities in the area of information and data security, providing members forums through which they can stay ahead of the curve in this important segment of the business. In the near future, look for upcoming training courses that CampusMBA, MBA’s education division, will be hosting on this model. These courses will allow you to learn more about applying the model to your business processes and systems. **NB**

RJ. Schlecht is director of industry technology for security and compliance with the Mortgage Bankers Association (MBA) in Washington, D.C. He can be reached at rschlecht@mortgagebankers.org.

REPRINTED WITH PERMISSION FROM THE MORTGAGE BANKERS ASSOCIATION (MBA)