realtimepublishers.com™

The Definitive Guide™ To

Information Theft Prevention

permeo™

Dan Sullivan

Copyright Statement

Chapter 2: Understanding Information Protection and Privacy Regulations

Information technology (IT) providers, both those within companies and those providing IT services, are expected to provide for information protection and privacy well beyond what was expected less than a decade ago. Although regulation is new to many in IT, businesses at large have worked within well-established regulatory frameworks and shareholder oversight for decades to the benefit of all. Some regulations—such as Securities Exchange Commission (SEC) rules for publicly traded companies and Occupational Health and Safety Administration (OSHA) requirements for worker safety—apply to a broad range of companies. Others are more targeted—for example, the Environmental Protection Agency (EPA) regulations on water quality are more relevant to manufacturers than to financial service providers. Changes in the regulatory environment have expanded the scope of coverage from traditional business areas, such as financial reporting and manufacturing processes, to include IT. In particular, preserving the integrity of data and protecting the confidentiality of personal information have driven several regulations that either directly or indirectly impact IT operations.

This chapter will examine the some of the broader information protection regulations that exist today as well as best practices for effectively and efficiently meeting those requirements. The first section of the chapter will examine financial integrity regulations and the recent business history that provided the motivation for passage of these types of regulations. The second section of the chapter shifts attention from businesses to individuals and looks into privacy regulations that are emerging from state, federal, and trans-national governments. The chapter closes with a discussion of best practices and frameworks that provide a broad structure for addressing requirements defined in a range of regulations (rather than attempting an ad hoc approach to individual regulations).

Regulating Business Information Integrity

Reducing bureaucracy and eliminating regulations are favorite topics in some political circles, but regulations exist for a reason—especially with regard to keeping free markets functioning efficiently. It may not be obvious, but government oversight of markets has been one of the factors that have ensured their success. Speaking on corporate governance, United States Federal Reserve Chairman Alan Greenspan noted "[G]enerally speaking, the resulting structure of business incentives, reporting, and accountability has served us well. We could not have achieved our current level of national productivity if corporate governance had been deeply flawed" (Source: Alan Greenspan, "Remarks by Chairman Alan Greenspan," 2003 Conference on Bank Structure and Competition, May 8, 2003).

📖 For the full text of Chairman Alan Greenspan's speech, see http://www.federalreserve.gov/boarddocs/speeches/2003/20030508/default.htm.

Although it is not deeply flawed, corporate governance has failed. Enron, Arthur Anderson, WorldCom, Tyco, and HealthSouth are some of the best-known examples of this failure. The corporate scandals of the past several years helped raise awareness for the need for more effective regulatory frameworks. High-profile corporate scandals helped lead to the passage of corporate governance legislation such as the Sarbanes-Oxley Act of 2002 (SOX). In addition to government regulations, some frameworks for protecting information originate from outside government agencies. These tend to be promoted by self-regulating industry bodies or non-governmental standards bodies. The following sections will examine four regulations/frameworks:

- SOX
- 21 Code of Federal Regulations (CFR) Part 11
- Basel II
- International Organization for Standardization (ISO) 17799: 2005

SOX and 21 CFR Part 11 are United States federal regulations. SOX is the well-known legislation addressing broad issues in corporate governance. 21 CFR Part 11 is a more specialized regulation targeting pharmaceutical manufacturing and quality.

Basel II and ISO 17799 are frameworks created by non-governmental bodies that contribute to generally accepted principals for particular types of business operations. Basel II, for instance, addresses how banks measure and report credit risks. ISO 17799 addresses best practices in information security management. Regulations can be grouped along two dimensions—the creator of the regulation and the scope of the regulation.

Although these regulations are from different types of regulating bodies and cover diverse topics, three fundamental aspects of information security meet the regulations' objectives: confidentiality, integrity, and availability (see Figure 2.1).

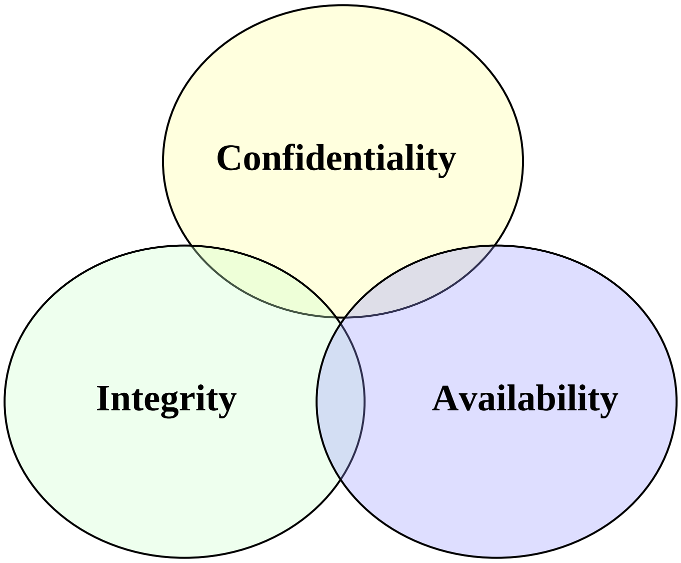

Figure 2.1: Regulations are addressed by three fundamental aspects of information security.

Example of Corporate Governance of Information Integrity: SOX

A string of corporate corruption cases that developed in the fall of 2001 brought to light the need for effective corporate governance. These scandals devalued shareholders equity, cost employees jobs and pensions, and contributed to a widespread distrust in corporate governance. As one legal analyst put it “Enron was, quite simply, the opening chapter in a series of sordid tales about corporate governance run amok” (Source: Kathleen F. Brickley, “From Enron to WorldCom and Beyond: Life and Crime After Sarbanes-Oxley,” available at http://law.wustl.edu/WULQ/81-2/Brickey.pdf). Although the high-profile scandals have faded into history, their consequences have not.

The ripple effects of these scandals are still evident several years later. A *Wall Street Journal*/Harris Interactive poll published in October 2005 found that 55 percent of United States investors surveyed feel that corporate governance standards are too lenient and 30 percent of investor respondents have divested or reduced holdings in firms as a result of poor corporate governance.

> 🕮 For detailed results of the Wall Street Journal/Harris Interactive poll, see http://www.harrisinteractive.com/news/newsletters/WSJfinance/HI_WSJ_PersFinPoll_2005_vol1_iss05.pdf.

One of the most widely recognized attempts to improve corporate governance is the passage of the Public Company Accounting Reform and Investor Protection Act of 2002, more commonly known as SOX. This legislation, which applies to publicly traded companies, addresses several governance topics:

- Board of Director responsibilities and restrictions
- Auditor independence
- Corporate responsibility for accurate reporting
- Financial disclosures
- Conflicts of interests
- Corporate fraud accountability

Some of the legislation is particularly relevant to information management and protection, as this chapter will explore.

> 🕮 For an executive summary of SOX, see http://www.csbs.org/government/legislative/misc/2002_sarbanes-oxley_summary.htm. The full text of the law is available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf.

SOX Sections Relevant to IT

Three SOX sections are especially relevant to IT operations: sections 302, 404, and 409. None of these sections of the law dictate how firms should implement IT; they simply state the regulatory requirements that IT must address.

Section 302: Corporate Responsibility for Corporate Reports

Section 302: Corporate Responsibility for Corporate Reports describes the actions required of corporate officers to ensure the integrity of financial reports. The act specifically states that officers signing financial reports are responsible for establishing and maintaining internal controls to protect the integrity of that information.

Section 404: Internal Controls and Financial Reporting

A relatively short and unthreatening passage addresses the heart of IT responsibilities under SOX—section 404. This part of the act states that the SEC will enact rules that "state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting." This passage reinforces the need for internal controls that was also made clear in section 302.

Section 409: Timely Reporting

In addition to calling for accurate reports on the financial state of a public company, section 409 requires that material changes in the financial condition of the company must be reported in a timely manner.

IT Responsibilities Under SOX

The sections of SOX relevant to IT focus on maintaining adequate information systems so that information about the financial state of the company is readily available and is not—and has not been—in a compromised position. This translates into several requirements:

- Meet business requirements for information systems
- Maintain secure systems for information integrity
- Manage change to maintain information integrity and meet reporting requirements

Like the legislation, these requirements are broad and can be implemented in many ways. Regardless of how they are implemented, the implementations will share some common characteristics.

Meet Business Requirements

IT managers and designers must ensure that business requirements are accurately accommodated in information systems. Some of the more mundane aspects of this directive include maintaining reliable backups and ensuring business continuity plans are in place in the event of a service disruption. The more challenging issues arise when trying to accommodate, for example, complex business rules about how to categorize revenues, forecast production levels, or quantify some element of the competitive landscape. The crucial aspect of this requirement is to make sure business procedures and policies are accurately reflected in operational systems.

Maintain Secure Systems

Another requirement centers on information integrity. Systems and network administrators must ensure that data is not changed in any unauthorized way, assuming all operational systems collect, process, and analyze data correctly. For example, access controls to applications must be in place so that only those responsible for adding and updating financial data can make those changes. File permissions contribute to file security and prevent accidental or intentional deletion of database files. Antivirus and other malware detection solutions are necessary to prevent malware from changing, stealing, or destroying data on both servers and desktop devices. Maintaining secure systems requires a comprehensive security program that addresses vulnerabilities across the entire path that data flows—database to server to client.

Manage Change

It is difficult to imagine an IT system that does not change. Information management procedures and tools need to respond to changing business requirements and adapt to new situations. At the same time, dependencies between systems prevent developers from freely modifying code without possibly affecting other applications. With appropriate change management procedures, however, IT managers can update their systems as needed while coordinating those changes with others impacted by the changes.

The reach of SOX goes far beyond the boardroom and the finance department. Information integrity is a central element of corporate governance; therefore, information management is also crucial. The law does not dictate how companies are to maintain information integrity and meet reporting requirements; however, commonly used system development, security, and operational procedures are recognized as applicable to meeting regulatory requirements:

- Application access controls
- File system access controls
- Policy definition and implementation, including information usage controls
- Authentication
- Encryption
- Firewalls
- Content filtering
- Antivirus and other malware detection and prevention systems
- Change management procedures

Fortunately, these methods apply to regulations other than SOX as well.

Example of Industry-Specific Regulation: 21 CFR Part 11

Regulations targeting information integrity are not limited to financial information. Understandably, pharmaceutical manufactures are strictly regulated in both manufacturing processes and record keeping. Just as audits of financial records are needed to trace the movement of funds through a company, well-defined documentation is needed to ensure that manufacturing processes continue to meet stringent standards and that appropriate monitoring controls are in place. 21 CFR Part 11 is maintained by the United States Food and Drug Administration (FDA) and governs electronic records and electronic signatures in the pharmaceuticals industry.

> ✎ CFR is the set of rules and regulations published by the executive department and federal agencies in the United States. Title 21 is the set of regulations published by the FDA and Drug Enforcement Administration (DEA).

A More Detailed Information Protection Approach

Unlike SOX—legislation passed by the United States Congress that does not dictate specific procedures—21 CFR Part 11 was developed by an agency with expertise in the field of pharmaceuticals. This regulation and supporting publications from the FDA provide much more detailed guidance about what must be done to meet the objectives of the regulation. For example, in an industry-guidance document, the FDA identifies several necessary information protection practices:

- Access controls
- Operational system checks
- Authority checks
- Device checks
- Policies governing electronic signatures
- Documentation controls
- Operating system (OS) controls

> 📖 For details about the guidance published by the FDA, see “Guidance for Industry Part 11, Electronic Records; Electronic Signatures—Scope and Application” at http://www.fda.gov/cder/guidance/5667fnl.htm.

Anticipating Vulnerabilities Associated with Remote Access

An organization can implement the previously listed information protection practices for managed devices, such as database servers, application servers, and desktop systems. Access controls, for example, are based on the identity of the user and can be used to limit access to an information resource from any device. However, potential problems can arise from the sometimes difficult-to-anticipate vulnerabilities that emerge when security mechanisms are used in a variety of ways.

For example, consider a pharmaceutical representative who employs a Web portal that provides a single point of access to email, collaboration tools, research libraries, and other tools. While at an industry conference, the representative uses a public PC in the hotel's business center to check email and download sales collateral from the company portal. Running late for a presentation, the representative logs off the portal and clicks the home icon in the browser, unknowingly creating an information theft vulnerability. When working in the office, logging off the portal may be enough to maintain adequate levels of security; on public devices, this action is not enough. Unless the buffer cache and cookies are cleared after that session, identifying information may be accessible to the next user.

Regulations in 21 CFR Part 11 require that the integrity of electronic documents be protected; however, common practices, such as remote access, can expose vulnerabilities in access control procedures as well as other security measures. When assessing the steps necessary to meet information protection regulations, it is essential to consider the combination of ways that information is accessed and how to minimize the threat exposure to information integrity created by those practices.

Both SOX and 21 CFR Part 11 are government regulations that emphasize information integrity. Industry organizations also have an interest in defining and enforcing minimal acceptable practices in this area—if for no other reason than to establish and control standards rather than wait for governments to step in and do the job.

Example of Industry Regulations for Risk: Basel II

The Bank of International Settlements (BIS) is an international organization established in 1930 to promote cooperation between banks. Although it was created under the auspices of international law, it competes with private banks and has had private investors in the past. BIS is currently owned by member central banks. Its primary objectives are:

- Promoting monetary and fiscal stability
- Supporting cooperation between central banks
- Acting as a bank to central banks

In addition, it seeks to promote improved accounting standards. To that end, BIS has established a set of standards known as Basel II (the formal title of this standards set is "International Convergence of Capital Measurement and Capital Standards: A Revised Framework"). These standards address:

- Credit risks or risks related to loan defaults
- Operational risks, such as disruption of internal procedures
- Market risks, including changes in a bank's position relative to equity markets

Like SOX, the goal of the Basel II framework is to establish reporting standards to ensure investors and other stakeholders have an accurate description of a bank's financial position. The framework does so by establishing three regulated areas: minimum capital requirements, managerial oversight, and disclosure. To effectively manage and report on the state of a bank, the organization must have mechanisms in place to ensure integrity and availability of information. Access controls, network and server defenses, threat assessments, security policies and procedures, and business continuity plans are fundamental to meeting Basel II requirements.

> 📖 For more explanation of the role of BIS and it history, see "What is the Bank if International Settlements" at http://www.investopedia.com/articles/03/120903.asp.

Basel II and 21 CFR Part 11 are examples of industry-specific regulations. Although they apply to unrelated industries, they have the same core objective—information integrity—and their implementations depend on similar sets of security measures. The same pattern is seen in regulations ranging from those that apply to federal government agencies, such as the Federal Information Processing Standards (FIPS), to cyber security programs promoted in the electric power generation industry by the North American Electric Reliability Council (NERC). Regardless of an organization's business or role in society, the need to gather, store, protect, and analyze information is pervasive.

Given this widespread need for information protection frameworks, it is not surprising that a broad standard has been developed in addition to those legislated by governments or created by industry-specific bodies.

Example of a Generalized Information Security Standard: ISO 17799: 2005

ISO 17799 is an information security standard published in 2000 and revised in 2005 by the ISO. The 2005 version of the standard defines best practices in 11 key areas of information security:

- Security policy—The security policy section addresses the need for security policies and their review.
- Organizing information security—The information security organization area discusses the need for management commitment to security, coordination, allocation of responsibilities, confidentiality agreements, independent reviews, and procedures for dealing with external parties.
- Asset management—The asset management topic covers ownership of assets, acceptable uses, and information classification.
- Human resources security—Not all information security topics are technical, as demonstrated by the need for coverage of human resources security, which includes employee roles and responsibilities, and employee screening, termination, and removal.
- Physical and environmental security—The physical and environmental security section addresses physical access controls such as perimeters, entry controls, and security mechanisms for facilities. It also covers physical security equipment.
- Communications and operations management—Operational procedures, delivery management, backup and recovery, media handling, information exchange, monitoring, and auditing are covered in the broad communications and operation management area.
- Access control—The access control section covers topics such as user access management policy, user responsibilities, network access controls, OS access controls, application access controls, and mobile computing.
- Information system acquisition, development, and maintenance—The information system acquisition, development, and maintenance area includes topics such as security requirements of information systems, correct processing in applications, cryptography, security of system files, and security controls related to application development.
- Information security incident management—The often-overlooked information security incident management topic addresses the reporting of security events and weaknesses and management of security incidents.
- Business continuity—Business continuity addresses business operations, risk management, and testing related to maintaining business operations.
- Compliance—Acknowledging the importance of this topic, the compliance area addresses compliance with legal requirements, security policies, and audit considerations.

> 🕮 ISO 17799 was revised in 2005. The ISO Community Portal (http://www.17799.com) has a mapping of security categories between the 2000 and 2005 versions of the standard available at http://www.17799.com/papers/2000v2005.xls.

ISO 17799 is a set of best practices that applies to virtually any organization. Unlike regulations such as SOX, the ISO 17799 framework does not require adherence by any companies, non-profit, or government agency—adoption is voluntary. This framework does, however, provide a comprehensive structure for establishing security policies and procedures.

As discussed earlier, information integrity is one of the two drivers behind the adoption of information-related regulations. Privacy is the other.

Ensuring Individual Privacy

As economic institutions face growing concerns about corporate governance, individuals are becoming increasingly concerned about personal privacy. Consider the opinions of Internet users from 8 or 9 years ago:

- A 1997 poll of Internet users found privacy was the number one concern (Source: GVU 8th WWW User Survey, available at http://www.gvu.gatech.edu/user_surveys/survey-1997-10/).
- A 1998 *Business Week*/Harris poll found that privacy was the main reason respondents were staying off the Internet (Source: "A Little NET Privacy, Please," available at http://www.businessweek.com/1998/11/b3569104.htm). The same poll found that 50 percent of Internet users wanted the government to pass laws "now" on the collection of personal data.
- A 1998 AT&T study found that the most important factor considered by users when submitting personal information on the Web was whether the information would be shared with other businesses or organizations (Source: "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," available at http://www.research.att.com/projects/privacystudy/).

Today, those and broader privacy concerns are reflected in privacy legislation that has been enacted by state, national, and trans-national governments. This section includes a discussion of some of the best-known privacy regulations, such as the Gramm-Leach-Bliley Act (GBLA), the Heath Insurance Portability and Accountability Act (HIPAA), and California Senate Bill (SB) 1386.

The confluence of corporate governance interests demanding more integrity in business operations and reporting and individuals' concern about the potential for information abuse emerging with advancing IT has created a new regulatory environment that brings IT within the regulatory scope. As Figure 2.2 illustrates, privacy regulations require the data be protected, regardless of where or how it is transmitted and stored. Fortunately, a common set of measures and best practices can provide the foundation for meeting the existing and evolving requirements to maintain information integrity and confidentiality.

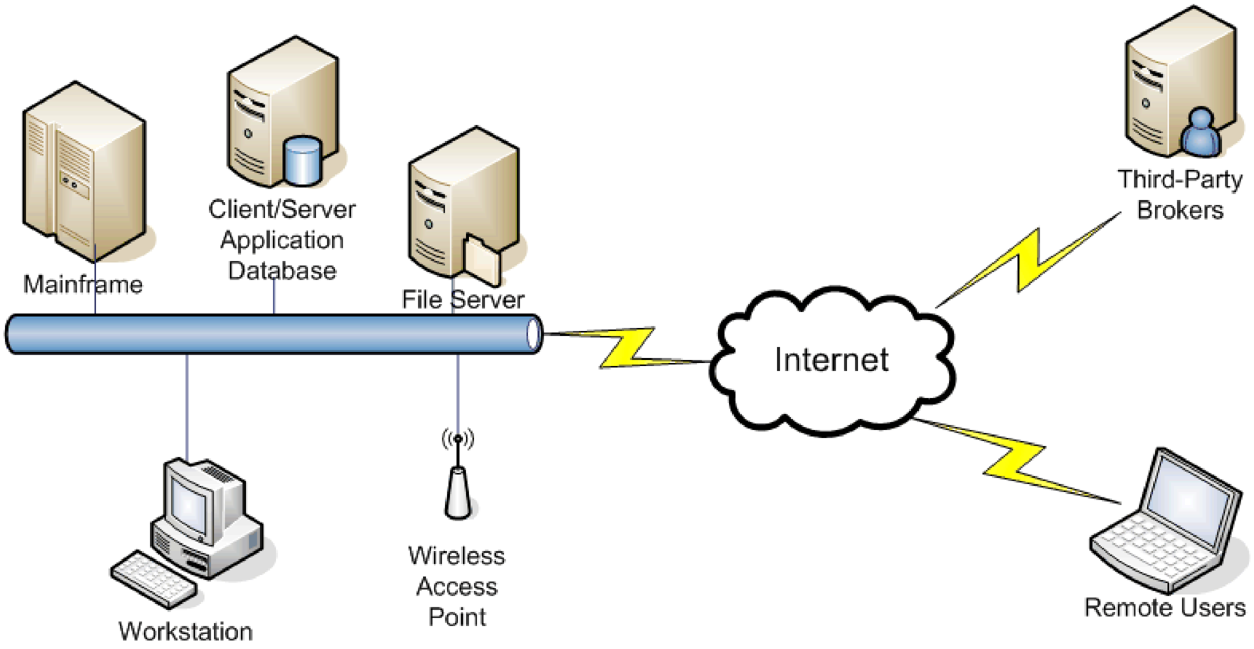

Figure 2.2: Organizations must protect privacy information regardless of where or how it is stored.

Financial Information and GLBA

GLBA, formally known as the Financial Modernization Act of 1999, revised rules that governed the banking industry since the Great Depression. In addition to changing restrictions on combining investment and banking activities, the act imposes restrictions on how financial services companies collect, use, and share consumers' private financial information. (Financial information includes name, address, phone number, bank account numbers, Social Security numbers, and credit and income histories.) The legislation defines financial services firms in a broad manner to include banks, insurance companies, investment firms, consumer lenders, funds transfer services, tax preparation services, and financial counselors.

The bill defines three main requirements related to non-public financial information:

- Financial Privacy Rule
- Safeguards Rule
- Pretexting

Together, these three parts of the legislation constitute the privacy protection mechanism of the law.

Financial Privacy Rule

The Financial Privacy Rule of GLBA establishes several requirements for financial institutions:

- Institutions must provide privacy notices to consumers
- Privacy notices must explain what private information is collected, what parts of the information is shared, and how the information is used.
- Privacy notices must also explain how non-public information is protected from disclosure and unauthorized change.
- When information is shared with third parties, those institutions assume the same responsibility to protect the consumers' private information.
- Consumers must have the ability to opt-out of information sharing arrangements with third parties.
- Financial institutions may not share customer account numbers with non-affiliated companies for the purpose of marketing even if the consumer has not opted out of the information-sharing agreement.

📖 The Financial Privacy Rule is discussed in detail at http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html.

Safeguards Rule

The Safeguards Rule of GLBA requires financial services companies and companies that receive financial information from financial services companies to adequately protect consumer information. The safeguards put in place must include a written security policy that describes how non-public information is protected. In addition, institutions must

- Identify the employee or employees responsible for coordinating the security policy
- Identify risks to consumers' non-public information in each department that handles that information and assess the potential impact of those risks
- Test and monitor the procedures to protect information
- Contract with service providers, as needed, to implement safeguards
- Adapt safeguards as needed as information management practices and need requires

The Safeguards Rule also requires firms to address three areas central to information security: employee management and training, information systems security, and system failure management.

Employee Management and Training

With regard to employee management and training, the guidance from the United States Federal Trade Commission (FTC), the agency responsible for enforcing GLBA, suggests several actions on the part of financial service companies:

- Checking references
- Having employees formally agree to abide by confidentiality policies and procedures
- Training employees on basic security principles
- Instructing employees on the details of the company’s information security policy
- Implementing access controls to limit non-public information to only those who have the business need for it

In addition to employee training, it is vital to implement appropriate security measures in information systems.

Information Systems Security

The guidance on information systems security outlines procedures that should be in place but leaves implementation details to firms managing the systems. The FTC includes the following suggestions:

- Store records securely by implementing both physical and logical access controls
- Implement physical protections from fire, water, and other physical dangers
- Implement backup and recovery procedures
- Provide for the secure transmission and collection of sensitive information
- Define a records retention policy and dispose of non-public information in a secure manner
- Implement audit procedures to detect violations of the firm’s security policy or cases of information theft

An especially challenging suggestion is to not “store sensitive customer data on a machine with an Internet connection” (Source: FTC, “Financial Institutions and Customer Data: Complying with the Safeguards Rule,” September 2002). Financial services firms may be willing to isolate mainframes and database servers used for backend processing from the Internet, but Web-based applications used in branch offices, programs that transmit consumer information to brokers and third-party affiliates, and employees that remotely access a company’s applications all run the risk of storing sensitive information on devices with Internet connections.

In today's Web-enabled environment, nearly every user has access to the Internet via a Web browser, which is arguably the most powerful application on the client desktop. This Web-enabled environment has shifted control away from IT into the hands of individual users. Users can immediately access a limitless supply of applications and content, which can create unnecessary security threats for an organization. For example, sensitive or confidential information may leave the company without anyone's knowledge, compromising corporate governance and compliance regulations. In addition, harmful malware or spyware could be introduced into the network, increasing the probability of information security breaches and performance problems. Thus, it is important for IT to implement technologies and methodologies such as encrypting information during transmission, implementing proxy appliances, implementing information usage policies and controls, and removing all cached copies of the data.

These suggestions assume sensitive information is tightly coupled to devices that can be reasonably well secured. Such is not always the case. Rather than depend on device-centric security, an on-demand security model—in which security is associated with the data wherever it is transmitted—is more appropriate. This security model is emerging and will likely become a preferred method for addressing some of the more challenging aspects of the Safeguards Rule.

The third key area the FTC addresses is how to manage system failures.

Business Continuity

Natural disasters, fires, and cyber-attacks can all disrupt operations. Under the Safeguards Rule, financial service companies are required to plan for those events and take appropriate precautions:

- Document and maintain contingency plans in case of physical or logical breaches of protective measures
- Manage system vulnerabilities through patch management
- Implement malware countermeasures, such as firewalls, proxy appliances, antivirus software, and content-filtering applications
- Maintain regular backups

The FTC also suggests notifying customers if their non-public information is lost, damaged, or subject to unauthorized access. A similar requirement is found in California SB 1386 (discussed later in this chapter); such requirements have lead to wide publicity of significant security breaches at banks and credit card processing companies—all the more incentive to implement effective security measures to protect consumer information.

> 📖 Additional information about the Safeguards Rule is available at http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html. The rule, as established by the FTC, is available at http://www.ftc.gov/os/2002/05/67fr36585.pdf. Details for implementing the Safeguards Rule are found at http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.pdf.

Another set of requirements in GLBA related to securing consumer information is a form of social engineering known as pretexting.

Pretexting and Phishing

Pretexting is a form of social engineering in which a person uses false pretenses to obtain non-public information. This threat can include the perpetrator calling a bank pretending to be a customer who has lost his checkbook and account number. In another example, someone could call customers pretending to conduct a survey on customer service for the bank and asking for account information. GLBA explicitly prohibits pretexting, including make false statements to financial services personnel or consumers of such firms.

📖 For more information about pretexting, see "Pretexting: Your Personal Information Revealed" at http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm.

Pretexting is similar to the online problem of phishing in which scammers use email to solicit private information used for identity theft. The most common forms of identity theft, according to the FTC, are credit card fraud, bank fraud, communications services fraud, and fraudulent loans. GLBA has been used in prosecutions of phishing scams, including one that tricked victims into revealing credit card numbers by pretending to be messages from America Online and PayPal (see http://www.ftc.gov/os/caselist/0323102/0323102zkhill.htm for details about this case). In another case, perpetrators of a mortgage scam were charged with violating GLBA (see http://www.ftc.gov/os/caselist/0223224/0223224.htm for details).

Financials services companies regularly use countermeasures to pretexting, such as asking pre-determined privacy questions (for example, asking customers to provide their favorite color or the name of their first pet). Consumers, however, are still targets of phishing scams and other pretexting schemes.

Financial services firms have little choice but to take the privacy protection regulations seriously—severe penalties are defined for violations. Under GLBA, institutions may be fined $100,000 per violations, and directors can be fined $10,000 per violation.

GLBA revised decades-old regulations governing the financial services market as well as introduced privacy measures to protect non-public information. As IT improves the ability to share information and business consolidations, such as bank and investment companies mergers, increase the motivation for such sharing, regulations are evolving to ensure the privacy concerns of consumers are met along the business objectives of the market. The healthcare industry also benefits from improved information sharing but must address privacy concerns as well.

Regulating Healthcare Information: HIPAA

HIPAA became law in the United States in 1996, enacting broad privacy protections for health and medical information. The objective of the law is to promote efficiencies in the health care system through the use of electronic records. As with changes in the banking industry, the quest for efficiency was balanced with demands for patient privacy protections. The key privacy provisions are:

- Patients are granted access to their medical records and may correct errors.
- Patients are to receive privacy notices from health care providers describing how their health care information may be used.
- Health care providers may share protected health care information for the purpose of treatment but disclosure is limited for non-health care uses.
- Patients must authorize the disclosure of their personal information before it may be used for marketing purposes.
- Health care providers should ensure their communications with patients are confidential.

> 📖 For more information about HIPAA privacy regulations, see http://www.hhs.gov/news/facts/privacy.html.

In addition to the general provisions of HIPAA, regulations define specific administrative requirements with regard to information security. In general, health care providers must ensure the confidentiality, integrity, and availability of protected health care information. They must implement countermeasures to anticipated threats and protect against anticipated hazards and disclosures. The regulation further defines several required safeguards:

- Implement procedures to prevent and detect security breaches
- Conduct risk assessments and implement procedures to mitigate those risks
- Monitor and audit system logs related to security events
- Identify a person responsible for creating and managing policies and procedures to implement these regulations
- Implement physical and logical access controls
- Implement security awareness training
- Protect against malware
- Establish and enforce password policies
- Implement incident response procedures
- Implement business continuity plans and procedures

The list is, not surprisingly, similar to the requirements under GLBA. There is also significant overlap with security standards addressed in ISO 17999. Clearly, there is a great deal of overlap in the development of information security regulations. Fortunately for businesses, government agencies, and other organizations, this overlap means a common set of best practices can meet many of the requirements of different regulations. Of course, there may be regulation- or industry-specific requirements but there should be no need for silos of security measures for individual regulations. Many of the same security procedures used to comply with SOX can equally well apply to HIPAA and GLBA.

Details about implementation requirements of HIPAA may be found in "Standards for Privacy of Individually Identifiable Health Information" at http://www.hhs.gov/ocr/combinedregtext.pdf.

HIPAA carries stiff penalties for violations. Firms may be fined $100 per violation up to $25,000 per year for each requirement violated. Penalties for individuals range from $50,000 in fines and 1 year in prison to $250,000 in fines and 10 years in prison.

As noted at the beginning of this section, there is significant public concern about the ability of individuals to protect their privacy. In the United States, the federal government has reacted to this concern with targeted, industry-specific regulations such as GLBA and HIPAA. The state of California has also addressed privacy concerns with legislation.

State Privacy Initiatives: California SB 1386

The State of California, in response to growing concern over identity theft, enacted legislation in 2002 requiring firms, government agencies, and persons doing business in California that gather personal financial information to notify victims when there is a security breach that compromises victims' private information. The bill, known as California SB 1386, defines personal information to be the person's first name or first initial and last name in combination with one of the following:

- Social Security number
- Drivers license or state identification card number
- Account number or credit or debit card number in combination with access codes allowing for access to the account

The act defines a security breach as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information." Individuals whose personal data is compromised to hacking or other unauthorized release and has suffered damage from it may seek civil damages against the organization that compromised the data.

The full text of California SB 1386 is available at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

California SB 1386 is a state law that applies to companies outside of the state who are doing business with customers in California. With roughly 12 percent of the population of the United States in California, many national and international businesses find themselves under the reach of this law.

Thus far, the discussion of privacy regulations has focused on those originating in the United States. In fact, some of the most stringent privacy regulations are enacted by other nations and trans-national governments.

Additional National and Trans-National Privacy Regulations

Privacy laws have been enacted in countries around the world. Although the scope of coverage, the methods of enforcement, and the effectiveness of different laws will vary, the fact that there is such widespread adoption of some form of privacy regulation indicates these types of laws will likely be in force for the foreseeable future. Examples of countries enacting privacy legislation include:

- Argentina—Law for the Protection of Personal Data and Regulation of the Data Protection Act
- Australia—Federal Privacy Act
- Canada—Personal Information Protection and Electronic Documents Act (PIPEDA)
- European Union (EU)—Directives on Data Protection and Privacy
- Israel—Protection of Privacy Law 5741
- Japan—Personal Data Protection Bill and Act for the Protection of Computer Processed Personal Data
- New Zealand—Privacy Act
- Uruguay—Law No. 17.838 of 2004 (regulating commercial personal information)

Although examining the details of each of these may have merit for comparative legal studies, for our purposes, it will help to briefly highlight two—Canada's PIPEDA and the EU's directives.

Canada's Privacy Principals

Canadian privacy legislation embodies a series of 10 principals that are common to broadly understood definitions of privacy. To begin, organizations are responsible for personal information they collect and should appoint someone to be directly responsible for complying with privacy legislation and regulations. When organizations collect information, it must be done with a person's consent and the purpose for collecting the information should be identified. Information collected should be limited to what is necessary for the stated purpose. Moreover, the information should not be shared without the person's consent and should be retained only as long as needed. Organizations are custodians of data and should maintain adequate safeguards to ensure the information is not disclosed to unauthorized users or for unauthorized purposes. The information that is maintained should be accurate and up to date. Finally, individuals should have access to their information and have the right to challenge compliance with the principals of privacy legislation.

The EU has enacted privacy legislation with similar principals, which has created issues for United States companies doing business with Europeans.

EU’s Privacy Directives and Safe Harbor Provisions

The EU’s Data Protection Directive enacts privacy protections guaranteed by the European Convention on Human Rights. Many of the principals are similar to those embodied in Canada’s PIPEDA, but one provision of the legislation was troubling for international trade. The legislation included a requirement stating that protected information not be transferred to a country outside of the EU that does not adequately protect private information. The United States’ approach to privacy protection did not meet that standard.

The EU and the United States negotiated a framework known as Safe Harbor, which provides sufficient privacy protections for European companies to share private information about EU citizens. Any United States company that abides by the provisions of the framework is eligible to receive protected information from European businesses. The framework consists of seven basic principles:

- Notify individuals about the collection and use of personal information
- Give individuals the ability to opt-out of providing personal information to third parties
- Information may be transferred to a third party if the person agrees to the transfer or if the receiving party applies the same level of privacy protection as the source company
- Individuals must have access to information and the ability to correct inaccurate data
- Companies must take reasonable measures to protect private information from unauthorized disclosure, loss, or misuse
- Collected information must be relevant for stated purposes and measures must be taken to ensure that data is kept reliable and accurate
- An independent mechanism must be in place to ensure compliance and address complaints

The principals adopted in the Safe Harbor framework are similar to those found in privacy legislation both in the United States and Europe.

📖 For more information about the Safe Harbor framework, see http://www.export.gov/safeharbor/.

The need to protect personal information is well established in many countries. In the United States, legislation is targeted to particular types of privacy, such as financial and health care privacy, while in Europe, a consolidated approach protects personal information in general.

Financial integrity and personal privacy regulation both depend upon adequate procedures and controls in IT. Without a comprehensive view of information security, organizations run the risk of implementing multiple schemes to comply with multiple regulations.

Implications for Information Management

Compliance with the regulations outlined in this chapter depends upon IT. Although information security, in a narrow sense, is not enough to meet regulatory demands, it is an essential part of the broader issue of IT governance that does enable compliance. The three aspects of governance that must be in place to comply with existing regulations are:

- Preserving confidentiality of data
- Maintaining integrity of data
- Ensuring availability of data

As noted earlier, these are the fundamental objectives of information security. Ensuring that the objectives are met requires a broad view of governance.

Governance is the oversight, management, and implementation that ensures security practices are in place and effective. There are many ways to implement governance procedures, and organizations should adapt those practices to their specific needs; however, many organizations will benefit from starting with existing frameworks such as ISO 17999 or the Control Objectives for Information and Related Technology (COBIT). Rather than delve into more of the details of ISO 17999 or discuss the specifics of COBIT, the following section explores how such frameworks are structured and then used to meet the needs of confidentiality, integrity, and availability.

> 📖 COBIT was developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute. Information about the framework is available at http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981. A primer on COBIT is available at http://www.isaca.org/Template.cfm?Section=COBIT6&CONTENTID=22368&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Structure of Governance Frameworks

The purpose of frameworks is to impose structure on what can appear to be an unwieldy collection of the business requirements, hardware devices, applications, processes, and procedures that make up IT operations. Using COBIT terminology, you can understand frameworks for managing these operations in terms of four levels of objects:

- Domains
- Processes
- Control objectives
- Control processes

The domains are high-level areas of IT management and include planning and organization, acquisition and implementation, delivery, and support and monitoring. Within each domain is a set of processes that identifies an IT strategic plan, defining information architecture, acquiring and maintaining application software, ensuring continuous service, and assessing internal control adequacy. Control objectives are policies and procedures designed to ensure that business requirements are met and include items such as developing an information architecture model, developing hardware and software acquisition plans, and managing security measures. Control processes are the procedures taken to realize control objectives.

Summary

IT professionals are subject to levels of regulatory overview that was uncommon even several years ago. Demands for improved corporate governance have lead to legislation such as SOX. At the same time, non-governmental and quasi-governmental agencies have developed frameworks and standards to improve the integrity of business practices. Regulations are not limited to business operations and reporting. Significant public concern about private information has grown with improvements in IT that allow for relatively easy sharing of information. The concern is fostered by increasing fear of identity theft, which has prompted even state governments to legislate protections of personal information.

With the increasing number and growing complexity of regulations, IT professionals could be unduly burdened with compliance efforts if proper practices are not in place. First and foremost, IT practitioners should view compliance as an outcome of best practices in IT governance and information security management. With a focus on well-defined objectives and implementing best practice controls for identity management and access controls, confidential data transmission and storage, blocking and removal of malicious software, and business continuity maintenance, compliance will follow. The next chapter will build on this foundation of security best practices knowledge by exploring the key technologies for on-demand security to prevent information theft.