CHAPTER 1

The Need for Information Systems Security Compliance

IN THE EARLY TO MID-2000s, many large corporations suffered public failures. Since then, a number of compliance laws have been introduced. Many of these laws and regulations place an increased responsibility on information technology (IT) staff. This increased responsibility ensures there are proper information system controls throughout the environment to provide the necessary security of customer data. In addition, these controls ensure the integrity of the systems upon which business processes run.

Compliance goes beyond just conforming to internal policies and standards. Compliance extends outside of the organization, mapping to external regulations and industry standards. Regular assessments and audits of the IT environment are important for ensuring compliance. Failure to comply with external regulations and industry standards can carry severe penalties. As a result, it is increasingly important to understand the methods by which an organization can be evaluated and the relationship between compliance and risk management and governance.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What an IT security assessment is
- What an IT security audit is
- What compliance is
- How audits differ from assessments
- What the importance of governance and compliance is
- What the consequences of not complying with compliance laws are

Chapter 1 Goals

When you complete this chapter, you will be able to:

- Examine the role of an IT assessment
- Examine the role of IT auditing
- Compare the differences between an audit and an assessment
- Summarize compliance and explain why it is important

What Is an IT Security Assessment?

Assessing IT security is typically part of a larger security program within an organization. Specifically, an IT security assessment is a key activity that involves the management of **risk**—an uncertainty that might lead to a loss. Information systems provide numerous benefits and efficiencies within organizations. However, these benefits come with risks. A risk-based approach to managing information security involves the following:

- Identifying and categorizing the information and the information systems
- Selecting and implementing appropriate security **controls**—actions or changes to be applied to systems to reduce weaknesses or potential losses
- Assessing the controls for effectiveness
- Authorizing the systems by accepting the risk based upon the selected security controls
- Monitoring the security controls on a continual basis

This approach is a continual cycle as organizations evolve and as activities such as assessments and monitoring reveal gaps and ineffective controls relevant to requirements and acceptable levels of risk.

The benefits provided to organizations as a result of information technology involve complex systems and processes. These systems not only benefit organizations, but they have also become critical components to the success of the organization. As a result, the continued and secured operation of these systems contributes largely to that success.

To understand their effectiveness, organizations must assess security controls. Security controls include the physical, procedural, and technical mechanisms to safeguard systems. First, are they implemented? Second, are they functioning as expected? If so, are they producing the required results based on the security policy of an organization?

You should not use a security assessment simply as a method for proving the strength of system security or as a reason to immediately provide greater security. Rather, a security assessment should produce information required to do the following:

- Identify weaknesses within the controls implemented on information systems.
- Confirm that previously identified weaknesses have been remediated or mitigated.
- Prioritize further decisions to mitigate risks.
- Provide **assurance**, a level of confidence that effective controls are in place and that associated risks are accepted and authorized.
- Provide support and planning for future budgetary requirements.

The personnel who conduct security assessments can be internal or external to an organization. While the procedures for assessments may vary widely by organization, the **National Institute of Standards and Technology (NIST)**, the technology agency of the U.S. Department of Commerce, provides a framework for effective security assessment plans in NIST Special Publication 800-53A. This publication defines a recommended assessment procedure, which includes a set of assessment **objectives**, or goals. Each objective has a set of assessment methods, including examination, interview, and test; and each objective has a set of assessment objects, including specification, mechanism, activity, and individual.

An assessment objective includes one or more statements that are directly related to a corresponding control to determine the validity and effectiveness of the control. For example, consider a common control that most users of computer systems have experienced: being locked out of an information system or application after too many unsuccessful logon attempts. The following illustrates the relationship between the control and the assessment objectives, methods, and objects.

Unsuccessful Logon Attempts

Control: The system enforces a limit of four consecutive invalid access attempts on the same username within a period of 15 minutes. The system automatically locks the account for 30 minutes. Subsequently, four more consecutive invalid access attempts within a period of 15 minutes lock the account indefinitely, which requires manual intervention by the system administrator.

Assessment objectives:

- Determine if the system enforces the defined threshold of consecutive invalid access attempts.
- Determine if the system enforces the delayed logon after initial account lock.
- Determine if the system enforces the defined threshold for locking the account indefinitely.

> **TIP**
>
> NIST Special Publication 800-53 Appendix F contains a catalog of assessment procedures. You can tailor the assessment procedures for use in performing a security assessment. Appendix H provides a summary template of all assessment procedures contained in Appendix F.

Assessment methods and objects:

- Examine access control policy statement and procedures addressing failed logon attempts.
- Examine associated information system documentation and configuration settings.
- Examine associated information system log records.
- Test the automated mechanism implementing the access control policy for failed logon attempts.

Methods for Conducting a Security Control Assessment

You can use several methods to conduct an assessment of security controls:

- **Examination**—Verify, inspect, or review associated assessment objects to understand or obtain evidence to support the existence and effectiveness of the security control. Examples include reviewing security policies and procedures and observing physical security mechanisms.
- **Interview**—Discuss associated assessment objects with groups or individuals to understand or obtain evidence to support the existence and effectiveness of the security control. Interviews can include senior officials, information system owners, security officers, information system operators, and network administrators.
- **Test**—Put associated assessment objects under specific conditions to compare actual behavior with what is expected to obtain evidence to support the existence and effectiveness of the security control. Objects can include hardware or software mechanisms or system operations or administration activities. Examples include testing actual security configuration settings and conducting penetration tests.

Assessment objectives should be part of your organization's IT security assessment plan. After executing the plan, you can create a report. The IT security assessment report documents the findings of the assessment and provides the information necessary to determine the effectiveness of the controls. Senior management uses the report to provide assurance that risks are appropriate to the goals of the organization and to help create, if necessary, another document for an action plan based on the results of the assessment.

> **TIP**
>
> It's helpful to create an executive summary document that quickly highlights the key findings and recommendations in a security assessment report.

Not all IT security assessments need to be comprehensive to cover all security controls or even all information systems. In fact, security assessments are often performed partially across controls and information systems. Although this chapter has laid out a best-practice framework for a comprehensive IT security assessment, security assessments vary in scope, depth, and breadth. The following is a list of some sample assessments you might encounter:

- Network security architecture review
- Review of security policies, procedures, and practices
- Vulnerability scanning and testing
- Physical security assessment
- Security risk assessment
- Social engineering assessment
- Application assessment

> **NOTE**
>
> Penetration tests are commonly referred to as *pen tests*. The terms *black box, white box*, and *gray box* are also related. A black-box test makes no assumptions about the environment to be tested, whereas a white-box test provides complete knowledge and information, such as network diagrams, about the environment to be tested. Gray-box tests are variations between black-box and white-box tests.

Another common type of assessment, and one that seems to be more popularized in the media, is a penetration test. A **penetration test** is an assessment method that attempts to bypass controls and gain access to a specific system by simulating the actions of a would-be attacker. However, penetration tests operate under specific constraints and rules of engagement. So they don't truly simulate the process a real adversary might take.

As a result, a penetration test is not necessarily the best means by which to judge the security of an information system. The test helps an organization understand its systems and gain insight into the level of effort an attacker might need to go through to penetrate the system. Penetration tests often reveal weaknesses or easily exploited vulnerabilities within a system. It is not uncommon for penetration tests to be a catalyst for selling management on the need to invest more money and/or effort in information security.

What Is an IT Security Audit?

An IT security **audit** is an independent assessment of an organization's internal policies, controls, and activities. You use an audit to assess the presence and effectiveness of IT controls and to ensure that those controls are compliant with stated policies. In addition, audits provide reasonable assurance that organizations are compliant with applicable regulations and other industry requirements.

Many people view an audit as a function of accounting. This makes sense because audits are often a part of the examination of financial systems and records. Consider, however, how financial accounting has moved away from traditional paper ledgers and books to information computer systems. The integrity of information systems is vital to accurate financial reporting. The integrity of information systems plays an important role in preventing financial disasters, such as those that occurred with a couple large companies in the early 2000s. These companies were **Enron** and **WorldCom**, which are discussed in the case studies later in this chapter. Even beyond financial reporting, computer information systems have now become a valuable asset within organizations, and as a result need control and auditing.

There are many types of audits, such as the following:

- **Financial audits**—These determine whether an organization's financial statements accurately and fairly represent the financial position of the organization.
- **Compliance audits**—These determine if an organization is adhering to applicable laws, regulations, and industry requirements.
- **Operational audits**—These provide a review of policies, procedures, and operational controls across different departments to ensure processes are adequate.
- **Investigative audits**—These investigate company records and processes based on suspicious activity or alleged violations.
- **Information technology audits**—These address the risk exposures within IT systems and assess the controls and integrity of information systems.

In addition, organizations are finding that integrated audits are more appropriate. Again consider the reliance on IT systems for transactions, storage of data, and communications across all operational aspects of an organization. Next, consider that many organizations—especially those that process payment cards and those that are publicly traded—are required to comply with numerous laws and regulations. As a result, it makes sense to be able to cover multiple regulations from a single audit event and prevent audit inefficiencies by treating compliance, financial, operational, and IT audits as silos. Aside from duplicating efforts, audit requirements can overlap between the various types of audits. As a result, it begins to make sense that an IT audit includes elements of a regulatory compliance audit or an operational audit includes elements of a financial and IT audit.

The scope of an IT audit often varies, but can involve any combination of the following:

- **Organizational**—This examines the management control over IT and related programs, policies, and processes.
- **Compliance**—This pertains to ensuring that specific guidelines, laws, or requirements have been met.
- **Application**—This involves the applications that are strategic—for example, those typically used by finance and operations.
- **Technical**—This examines the IT infrastructure and data communications.

External or internal auditors typically perform IT security audits. In most large companies, the auditor is actually a team of auditors. An external auditor is independent of the organization and is often engaged from one of the big accounting and consulting firms. Publicly traded companies are required to engage external auditors. Internal auditors are employed by the organization that they audit. Unlike external auditors, internal auditors are not independent of the organization they audit. They directly report to the board of directors

or a subcommittee of the board of directors. This is important so as not to be influenced by management and to ensure the integrity and honesty of their findings. Organizations often outsource their internal audit functions to an external consulting firm.

FYI

Who are the "big" auditors? That list is shrinking, but by 2002, what was called the Big Five had become the Big Four. These are the largest accounting and professional service firms. The Big Four includes PricewaterhouseCoopers (known as PwC), Deloitte, Ernst & Young (known as EY), and KPMG. Arthur Andersen was dropped from the Big Five list as a result of the Enron collapse, for which they were the auditors. Arthur Andersen was indicted for obstruction of justice and subsequently ceased operations.

An effective IT security audit program should ultimately accomplish three goals:

- Provide an objective and independent review of an organization's policies, information systems, and controls.
- Provide reasonable assurance that appropriate and effective IT controls are in place.
- Provide audit recommendations for both corrective actions and improvement to controls.

In many cases, external auditors do not advise the client as internal auditors would. External auditors are typically limited to providing information about gaps discovered and leading the client to accepted principles. Internal auditors can provide recommendations for improvements; however, they should never be involved in the design or implementation of any system or control.

What Is Compliance?

Despite being a relatively simple term, the term **compliance** has become something of an enigma within many organizations. Different people view and define compliance in different ways. This is evident across different industries, within the same industries, and even within organizations.

The Merriam-Webster Online dictionary defines compliance as "the act or process of complying to a desire, demand, proposal, or regimen or to coercion." To comply is "to conform, submit, or adapt as required or requested." In regard to IT compliance, compliance pertains to two broad areas: internal and external. *Internal compliance* refers to an organization's ability to follow its own rules, which are typically based on defined policies. *External compliance* refers to the need or desire for an organization to follow rules and guidelines set forth by external organizations and initiatives. Although many external-compliance mandates are regulatory in nature, other compliance initiatives also include standards and guidelines that must be followed as set forth by industry regulations.

The credit card industry is a prime example, which developed a set of security standards in an attempt to provide self-regulation. The majority of compliance mandates are, however, laws and regulations. There are numerous compliance mandates to which organizations may be required to adhere. In most cases, regulations do not provide specifics and are open for interpretation. Compliance frameworks, such as **Control Objectives for Information and Related Technology (COBIT)**, and standards, such as NIST, help interpret how to comply with the regulations.

Unlike a simple traffic law, such as the requirement to stop at a red light, compliance laws and regulations are not always so clear. This is often another source of frustration for those with the responsibility of helping an organization comply. The general steps to meeting compliance include the following:

1. Interpret the regulation and how it applies to the organization.
2. Identify the gap or determine where the organization stands with the compliance mandate.
3. Devise a plan to close the gap.
4. Execute the plan.

> **NOTE**
>
> Meeting compliance often includes implementing mechanisms to prove that an organization has properly executed its plan.

Compliance is closely related to **risk management** and **governance** on all levels, be it technical, procedural, or strategic. Risk management seeks to mitigate risk through controls. For example, an organization identifies, evaluates, and takes action to lessen its risk. Compliance helps risk management by verifying that the desired controls are in place. Governance seeks to better run an organization using complete and accurate information and management processes or controls. For example, a sound security policy and comprehensive procedures are in place to implement the policy.

Compliance helps governance by ensuring such information and controls also satisfy applicable standards or regulations. On a strategic level, compliance ensures an organization can effectively meet organizational goals and objectives as planned. This means IT must ensure it is capable of delivering services to satisfy business needs and to stay compliant with external laws and regulations.

How Does an Audit Differ from an Assessment?

Although there seem to be many similarities between an audit and assessment, there are some stark differences. One is the mindset people tend to have about the word *audit*. This word brings to mind thoughts of distrust and punishment. Regardless of whether these feelings are justified, these thoughts are based on several outcomes that can result from an audit:

- **Failure**—Audits are typically more clear-cut in the sense of pass or fail. It is possible to fail an audit, but most people don't think of an assessment in terms of pass or fail. Rather, you might see an assessment as an opportunity to assess the current state and make improvements as necessary.
- **Blame**—Audit findings might place blame on specific individuals or groups within an organization. Assessments, on the other hand, are nonattributive. That is, they don't view an individual as being directly responsible for a poor finding. Many organizations use assessments to prepare for audits. Assessments provide a chance for improvement in a more comfortable and productive environment that helps facilitate the goals of the organization.
- **Consequences**—Audits can have consequences, many of which are negative. Consider

that an organization can fail an audit and, subsequently, have blame attributed to an individual or group. In addition, noncompliance with regulatory and industry standards can carry stiff penalties. The consequences of failing an audit can create a sense of fear, whereas an assessment simply identifies gaps to improve security operations and achieve goals.

Security auditing, in general, must follow a more rigid approach and process over a security assessment. This is a key point, especially when you consider that an audit is an assessment. Moreover, an audit contains the following unique characteristics:

- Auditors should never be involved in the auditing of processes, systems, or applications that they themselves designed or implemented.
- Audits are an independent evaluation. A security assessment may also be conducted independently, but it is not necessary. Many organizations use a combination of both.
- Audits follow a rigorous approach and are conducted according to accepted principles. This also requires that auditors be qualified. The approach taken for an assessment can fall across a wide spectrum, but in many cases, they have taken a cue from audits with well-defined approaches and frameworks.
- In the event an organization passes an audit, the organization typically receives some type of certification or confirmation. This is not the case for assessments.
- An audit is concerned about past results and performance, whereas an assessment considers previous and current results as well as expected performance.

You might find it helpful to evaluate a security audit and security assessment in more personal terms. Consider, for example, your own financial situation. When was the last time you personally assessed your financial state? Are you comfortable with your current situation? Are you on track to meet long-term goals? You can use many different tools and materials to do this yourself. Or you can hire a financial consultant or tax advisor to look at your situation, set goals, and identify gaps that exist in meeting those goals. Now imagine the U.S. Internal Revenue Service (IRS) knocking on your door to audit you. Granted, an individual IRS audit seems more adversarial. Keep in mind that is why companies go through audits in the first place. A successful audit enables a business or organization to be more profitable and/or successful without risk of penalties or being deemed incompliant.

Why Are Governance and Compliance Important?

Without proper governance in place, an organization can have neither effective risk management nor compliance. A common theme thus far has been the reliance on IT throughout the organization. As a result, IT can have a tremendous impact on either the success or failure of an organization. The interest in formally governing the use and application of IT should come as no surprise. IT is now woven into the fabric of business and has made organizations dependent on information and the systems that help generate and store information. In addition, IT will continue to provide opportunities for competitive advantage and reduction of costs throughout the organization. On the other hand, IT systems are subject to numerous threats that continue to evolve and seek to exploit vulnerabilities.

At a fundamental level, internal compliance to corporate policies is critical to the success of any business. Risk management means deeming some risks acceptable so a company may accomplish its business goals. Compliance, therefore, embraces the organizational mission,

and noncompliance can harm or even impede business.

Regulatory compliance benefits organizations, consumers, and shareholders. Regulatory compliance protects the reputation and integrity of the organizations that are required to comply. It considers the interests of the consumer and shareholders. Regulatory compliance also has a farther-reaching economic impact on ensuring public confidence in organizations and capital markets.

Case Study: Enron

Enron Corporation was a U.S.-based energy company that at one point was the seventh-largest company in the United States and the largest trader of natural gas and electricity in the country. Enron came about in the mid-1980s, focusing on the natural gas market. By the 1990s, it had pursued a diversification strategy to achieve growth. Subsequently, Enron got involved with trading and ownership in electric, coal, steel, paper, water, and broadband capacity.

Enron collapsed in 2001 and filed bankruptcy, which at the time was the largest bankruptcy in history. The collapse was a result of a complex and methodical accounting scandal. The fallout was massive, resulting in thousands of employees who were laid off and who lost their life savings plans that were tied to the company's stock. In addition, shareholders saw a loss of $11 billion. Economically, the disaster perpetuated a lack of trust in the stock market and eroded public confidence.

> **NOTE**
>
> WorldCom would go on to surpass Enron as the largest bankruptcy. Ultimately, it was the Enron fiasco that led to the downfall of Arthur Andersen as one of the largest auditing and consulting firms.

Enron's auditing firm, Arthur Andersen, had attested to Enron's financial health for years, despite widespread fraud and hidden losses at Enron. In addition, the auditing and consulting firm assisted Enron in deal structuring and other consultative practices. Enron paid Arthur Andersen a combined $52 million in consulting fees in the year 2000 alone. Arthur Andersen was eventually convicted of obstruction of justice as a result of shredding paper documents and destroying electronic documents related to their client. Arthur Andersen's involvement with Enron also led to the discovery of other audit discrepancies, including those at WorldCom.

Although complex and occurring over a period of many years, investigative findings discovered that Enron used several complicated and questionable accounting methods, including the following:

- Enron had reduced its tax payments and inflated its income and profits.
- Enron had increased its stock price and credit ratings.
- Enron had hidden losses in off–balance sheet subsidiaries.
- Enron employees funneled money to themselves and acquaintances.
- Enron's financial condition was misrepresented in public reports.

The Enron board of directors was faulted on several accounts. One of these was not being involved in the examination of terms related to moving debt off the company's balance sheets. They missed the chance to uncover fundamental flaws in the accounting practices at

the company. A report written by the special committee investigating Enron described what went wrong with management: "We found a systematic and pervasive attempt by Enron's management to misrepresent the Company's financial condition." Enron's culture was one that seemed to cast aside traditional controls. In fact, the investigating committee also stated that Enron had an "across-the-board failure of controls and ethics at almost every level of the company." The report continued, describing "a flawed idea, self-enrichment by employees, inadequately designed controls, poor implementation, inattentive oversight, simple (and not so simple) account mistakes, and overreaching in a culture that appears to have encouraged pushing the limits."

Enron has become in many ways the premier symbol of fraud, corruption, and audit failure. The scandal also resulted in a host of new regulations and legislation being enacted, including the **Sarbanes-Oxley Act**. This act addresses many of the shortcomings and lessons learned from the Enron scandal.

The following are some questions for further thought and discovery:

- How do a company's acquisitions relate to risk management and governance?
- The Enron scandal resulted in steps to improve standards, controls, and accountabilities. How much do morals contribute to such events and what can be done to address this issue?
- What financial incentives may have been in place for Enron's consulting firm to perhaps have lax auditing standards?
- Given the large sums paid on consultancy fees, is it possible that talented auditors are focused on consulting while less-experienced employees audit?
- How might a control framework for IT that is more closely aligned with business processes have prevented this?
- How could adequate controls on IT systems and financial applications have helped?
- Do you think that controls designed to prevent or detect fraud were in place? How important is the monitoring of such controls, and how should access be controlled?

Case Study: WorldCom

Prior to filing bankruptcy in 2002, WorldCom was the second largest telecommunications company in the world. It handled Internet data traffic globally and accounted for more international voice traffic than any other company.

WorldCom grew quickly from its modest beginning in 1983, and achieved its tremendous growth through 65 acquisitions. In the 1990s, the company made some large acquisitions, including MCI Communications. Through this period, WorldCom spent approximately $60 billion and accumulated approximately $41 billion in debt. The MCI acquisition was the largest merger in U.S. history at the time.

The market value of WorldCom continued to grow substantially through these acquisitions, and high expectations continued to be placed on the company. This generated pressure to keep the stock price at elevated levels, which in turn allowed WorldCom to continue its acquisition spree. A proposed merger in 2000 with Sprint would have eclipsed the merger with MCI; however, the merger was disapproved and WorldCom started to unravel. In an attempt to maintain its earnings, WorldCom liberally interpreted accounting rules to make its financial statements seem profitable. The company soon moved from liberal interpretation into outright fraud by creating false entries.

A team of internal auditors became suspicious over numerous financial oddities and began investigating, but the auditors encountered problems. They tried to discuss financial

irregularities with WorldCom's external auditors, Arthur Andersen, who did not fully cooperate. Responsible to the WorldCom chief financial officer (CFO) at the time, the internal audit group raised issues with the CFO but was pressured to stop. The internal auditors persisted and eventually uncovered what would become the largest account fraud in U.S. history.

How could this have happened, and what were some of the events and situations that led to this mess?

- The board of directors became simply a "rubber stamp."
- The board of directors allowed the chief executive officer (CEO) and CFO of WorldCom to have unfettered power.
- WorldCom acquired many companies without a strategy for linking them properly.
- The board of directors approved deals worth billions of dollars with little discussion.
- Little oversight of debt accumulation existed.
- Little oversight of company loans made to the CEO existed.
- The company lacked internal controls and transparency.
- External consultants failed to apply techniques consistent with their risk rating of the company.
- Internal auditing was underqualified and focused on nonauditing activities.

Consider the questions previously discussed in the Enron case. What parallels can you draw between these two disasters? How can information technology be used as a tool across all lines of business within an organization? How can IT better align with the organizational processes?

Resulting regulations have had far-reaching impacts on information technology—specifically controls and the auditing of those controls. These controls include general controls, which are embedded in IT services, as well as application controls, which are embedded in business applications. Why are these controls important? Why is the auditing of these controls important?

What If an Organization Does Not Comply with Compliance Laws?

Of course you wouldn't break a law, right? But asking what if your organization doesn't comply with compliance laws is a fair question. Let's look at an example of an individual compliance issue to understand why.

It is a law to come to a complete stop at a stop sign, yet many people ignore it. This scenario is actually a form of risk management. Many people consider it an acceptable risk to approach slowly and continue on if there is no traffic, without coming to a complete stop. The threat of another car exists, yet many people feel safe enough with the slow approach and rolling stop. There is always the threat of a police officer pulling you over and issuing a ticket. Yet how often is this enforced? If it were, what is the punishment? Given the likelihood of being pulled over by law enforcement, combined with what is likely a bearable fine, many people decide the risk is low and the benefit of noncompliance outweighs the risk.

> **NOTE**
>
> Don't forget about the other negative effects that noncompliance can have on an

organization, beyond the threat of fines and imprisonment. For example:

- Legal fees resulting from infringements contained within many regulations
- Brand damage and lost revenue as consumers abandon a business
- Negative effect upon stock price, hurting shareholder value
- Increases in the cost of capital

Organizations have spent and continue to spend large sums of money to achieve and maintain regulatory and industry compliance. This is especially true as regulations have placed greater accountability on individuals within an organization. Noncompliance can result in huge fines as well as jail time. Some regulations are subject to strict liability. Strict liability means even if there wasn't intent, government agencies can levy huge fines on organizations and some individuals can spend years in prison. Even greater punishments are in store where intent can be proven!

In addition to the financial and reputational consequences of noncompliance, organizations can also experience operational consequences. This can happen, for example, in the case of compliance standards imposed by the payment card industry. Potential consequences include payment card–imposed operational restrictions and even loss of card-processing privileges.

The **Payment Card Industry Data Security Standard (PCI DSS)** is an industry-created standard that applies to organizations that process credit cards. Companies that meet a specific threshold for large volumes of credit card transactions are required to achieve compliance. This is done via an audit by an independent Qualified Security Assessor (QSA).

Case Study: TJX Credit Card Breach

Imagine being the chief information officer (CIO) of one of the largest department store chains in the United States. Now imagine your CEO publicly announces that the company has just become the victim of the largest known theft of credit card data in history. This is a nightmare situation for any IT security professional, and this is what happened to The TJX Companies.

The TJX Companies, Incorporated is a large off-price retailer of apparel and home fashion. The company operates under several brands, including T.J. Maxx and Marshalls. On January 17, 2007, TJX announced it had become a victim of an intrusion into portions of its information systems that process and store customer transaction data.

An unauthorized intruder first accessed systems in July 2005, and unauthorized access continued through mid-January 2007. On December 18, 2006, TJX discovered suspicious software on its systems and immediately initiated an investigation along with leading computer security firms. Within a few days, TJX had notified law enforcement officials and met with the U.S. Department of Justice and the U.S. Secret Service to brief them on the discovery. Shortly thereafter, TJX notified contracting banks and payment card processing companies. Before the public announcement of the incident, the company had notified the U.S. Federal Trade Commission (FTC), the U.S. Securities and Exchange Commission (SEC), and the Canadian authorities.

At the time, this had evolved into the biggest credit card breach in history. Conservative estimates initially put the number at over 45 million credit and debit cards breached, as well as the personal information of hundreds of thousands of customers, including Social Security numbers and driver's license numbers.

NOTE

Initially, the TJX attackers accessed only historical data. To capture live transaction data, the attackers installed software that recorded the traffic. This enabled the attackers to steal credit card data as customer transactions were occurring in the store.

Although the exact details of the breach aren't clear, what is known is that the breach initially occurred as a result of the attackers targeting the wireless network of one of TJX's retail stores. The wireless network used Wired Equivalent Privacy (WEP) as an encryption method, which even at the time had been proven inadequate. The alternative was Wi-Fi Protected Access (WPA), which was introduced to replace WEP. Once the attackers penetrated this weak link, they eavesdropped on usernames and passwords used to log on to TJX's main systems in Framingham, Massachusetts. Eventually, the attackers created their own accounts on the main system and collected sensitive data.

In the aftermath, TJX has become the poster child for credit card breaches. The incident has also generated a lot of conversation and debate around adequate security controls for confidential personal information. Much of the blame for this incident was placed on the poorly secured wireless networks, but what type of defense in depth or compensating controls existed? The FTC charged TJX with failure to maintain proper security controls, specifically citing the lack of firewalls, wireless security, failure to patch vulnerabilities, and failure to update antivirus signatures.

The following are highlights of the fallout resulting from the breach. TJX:

- The company agreed to pay $9.75 million to settle state investigations.
- The company settled with the FTC. As a result, TJX had to create a comprehensive security program to protect the confidentiality of personal information it collects. In addition, TJX must submit to a third-party audit of the program every two years for the next two decades.
- The company settled lawsuits brought by consumers and banker groups. Customers were provided with a special, three-day sale and vouchers as a result of the settlement of class-action lawsuits.
- The company settled with Visa and MasterCard for almost $41 million.
- The company was required to implement a data-security program to ensure that this type of incident could never happen again.
- The company offered three years of credit monitoring to about 450,000 people who needed to provide their driver's licenses for transactions that occurred in the stores.
- The company set aside $250 million for breach-related costs. Many analysts believe this number could ultimately be much higher.

NOTE

The TJX breach has since been eclipsed in size. Heartland Payment Systems announced a breach in 2009, which resulted in 130 million compromised payment card records. The attacker of Heartland Payment Systems was indicted in August of 2009, and was also the leader of the TJX breach.

Unlike the collapse of Enron and WorldCom, TJX did not break any laws. It was simply not compliant with stated payment card processing guidelines. Court documents filed by the banks that sued TJX indicated that TJX did not comply with 9 of the 12 broad provisions within the standard established for the payment card industry. Although the breach has

been costly for TJX, it is a multibillion dollar retailer that has survived and made appropriate adjustments. Smaller organizations, however, might not have survived.

Although it costs money to implement proper controls and procedures for compliance, noncompliance and security breaches have their own costs. You learned that fines can be levied for noncompliance, but what about the costs of a breach? Forrester Research puts the cost *per record* breached at anywhere between $90 and $305, depending on the type of breach and how regulated the industry within which the breach occurs is. Consider the following categories from where costs can occur following a breach:

- **Discovery, notification, and response**—Legal counsel, mailings, call center support, discounted product offers
- **Lost productivity**—Employees' attention diverted or put on other tasks requiring attention
- **Opportunity cost**—Loss of customers and attaining new customers
- **Regulatory fines**—FTC, PCI, Sarbanes-Oxley
- **Restitution**—Money set aside for payment
- **Additional security and audit requirements**—Those levied as a result of a breach
- **Other liabilities**

The following are some questions for further thought and discovery:

- Consider the reasons why TJX might have had the weaker WEP encryption configured. Was this the internal standard? Did retail equipment perhaps not support newer, more secure methods? If so, should compensating controls have been in place? What types?
- Do you feel that TJX properly handled the incident upon discovery of the breach? Consider how incident-response procedures are important to the IT security program.
- Had TJX collected and retained unnecessary personal data? What are the risks of holding onto data?
- Did TJX understand where customer data resided, how it was transmitted, and whether it was encrypted?
- If the data was encrypted, could the breach have been possible? Is it enough to just encrypt sensitive data? What about the cryptographic keys that perform the encryption/decryption of the data? How and where are those stored? Is this defined in a policy? If so, how is it audited?
- What were the results of TJX's payment-card processing audits and third-party vulnerability audits?
- Were weaknesses and vulnerabilities within TJX discovered and documented through internal security assessments?

CHAPTER SUMMARY

Conducting audits and assessments of IT environments has increasingly become more important and visible since the collapse of companies such as Enron and WorldCom in the early to mid-2000s. Although they might share similar qualities, the differences between an audit and an assessment can be great. Likewise, internal auditors and external auditors have many of the same functions, yet some important differences in their roles

and expectations. Regardless, assessments, audits, and auditors are all key components to ensuring a successful risk-management and compliance strategy. Adequate governance and oversight of these activities helps ensure that businesses don't follow the path that Enron and WorldCom did, and also helps in preventing incidents such as what TJX went through.

KEY CONCEPTS AND TERMS

Assurance
Audit
Compliance
Control Objectives for Information and Related Technology (COBIT)
Controls
Enron
Governance
National Institute of Standards and Technology (NIST)
Objectives
Payment Card Industry Data Security Standard (PCI DSS)
Penetration test
Risk
Risk management
Sarbanes-Oxley Act
The TJX Companies, Incorporated
WorldCom

CHAPTER 1 ASSESSMENT

1. A security assessment is a method for proving the strength of security systems.
   A. True
   B. False

2. Categorizing information and information systems and then selecting and implementing appropriate security controls is part of a _____.

3. Whereas only qualified auditors perform security audits, anyone may do security assessments.
   A. True
   B. False

4. NIST 800-53A provides _____.

5. Which one of the following is *not* a method used for conducting an assessment of security controls?
   A. Examine
   B. Interview
   C. Test
   D. Remediate

6. Which of the following is an assessment method that attempts to bypass controls and gain access to a specific system by simulating the actions of a would-be attacker?

A. Policy review
B. Penetration test
C. Standards review
D. Controls audit
E. Vulnerability scan

7. An IT security audit is an _____ assessment of an organization's internal policies, controls, and activities.

8. Which of the following best describes an audit used to determine if a Fortune 500 health care company is adhering to Sarbanes-Oxley and HIPAA regulations?
A. IT audit
B. Operational audit
C. Compliance audit
D. Financial audit
E. Investigative audit

9. The internal audit function may be outsourced to an external consulting firm.
A. True
B. False

10. Compliance initiatives typically are efforts around all except which one of the following?
A. To adhere to internal policies and standards
B. To adhere to regulatory requirements
C. To adhere to industry standards and best practices
D. To adhere to an auditor's recommendation

11. At all levels of an organization, compliance is closely related to which of the following?
A. Governance
B. Risk management
C. Government
D. Risk assessment
E. Both A and B
F. Both C and D

12. Which one of the following is true with regard to audits and assessments?
A. Assessments typically result in a pass or fail grade, whereas audits result in a list of recommendations to improve controls.
B. Assessments are attributive and audits are not.
C. An audit is typically a precursor to an assessment.
D. An audit may be conducted independently of an organization, whereas internal IT staff always conducts an IT security assessment.
E. Audits can result in blame being placed upon an individual.

13. Noncompliance with regulatory standards may result in which of the following?
A. Brand damage
B. Fines
C. Imprisonment
D. All of the above
E. B and C only

14. Which of the following companies engaged in fraudulent activity and subsequently filed for bankruptcy?
A. WorldCom
B. Enron
C. TJX

D. All of the above

E. A and B only

15. Some regulations are subject to _____, which means even if there wasn't intent of noncompliance, an organization can still incur large fines.