CHAPTER 14

Information Security

As industrial economies move toward information-based economies, their information on products and customers become more valuable, and security becomes more important. We need only look at the ascendancy of the financial services industry and their increased investments in data warehouses and business intelligence applications to understand the growing importance of digital information. The explosive growth in the usage of online transactions via the Internet as well as wireless networks to link mobile devices to the Web have also increased the need for business managers, as well as security specialists, who understand these management issues. In the United States, the protection of the confidentiality and integrity of an organization's information is also now *required by law*. The penalties for noncompliance or violation of these laws can range from civil charges and severe fines to criminal charges for repeated and flagrant violations.

Early in the field of information security, the standard mantra was that better passwords, **firewall** rules, encryption, and other security technologies would solve most information security breaches. However, technical solutions are much less useful for thwarting attacks by an employee or business partner or those that exploit a mistake made by a computer user or organizational unit. This chapter will therefore discuss in some detail the *managerial* aspects of information security—including risk management, security policies, and **business continuity planning** (BCP) approaches to system controls, auditing, and compliance. This is not meant to negate the importance of security technologies in any way: Chief Security Officers and other managers are responsible for identifying and implementing appropriate technologies for information security, based on the organization's assessment of its risks.

We begin this chapter with a brief discussion of **computer crime**. Then we discuss a new managerial role that frequently, but not always has a reporting relationship with the CIO: the Chief Security Officer (CSO). This sets the stage for a discussion of some basic risk management approaches for determining what actions should be taken for information protection from a cost-benefit perspective. Then we summarize some examples of U.S. laws on information privacy and security for which there are significant penalties for organizational noncompliance. The chapter then ends with sections on developing organizational policies for information security, business continuity planning, and **electronic records management**.

COMPUTER CRIME

Computer crime is defined today as a crime that involves a computer or a network. Some crimes directly target computers or networks; other crimes use computers and/or networks to commit a crime. Some attacks involve single computers, and some are intended to involve thousands. Descriptions of some of the most common techniques used to attack computers from the outside are described in Figure 14.1. So-called cyberattacks have of course greatly increased over the past decade as organizations have increased their Internet connectivity.

Computer Virus: a small unit of code that invades a computer program or file. When the invaded program is executed or the file is opened, the virus makes copies of itself that are released to invade other programs or files in that computer. It may also do nasty things like erase files or corrupt programs. Viruses are transmitted from one computer ot another when an invaded computer program or files is transmitted to another computer.

Example: ILOVEYOU – May 2000. Written in Visual Basic script; transmitted as an attachment to an e-mail with the subject line ILOVEYOU. Estimated damage: $10-15 billion

Worm: a virus that has the ability to copy itself from machine to machine, normally over a network

Example: Sobig.F – August 2003. Spread via e-mail attachments; sent massive amounts of e-mail with forged sender information; deactivated itself Sept. 10, 2003. Estimated damage: $5-10 billion

Trojan Horse: a security-breaking program that is introduced into a computer and serves as a way for an intruder to re-enter the computer in the future. Like the huge wooden horse used by the Greeks to trick the Trojans into opening their city gates to let in the horse, it may be disguised as something innocent such as an electronic greeting card, screen saver, or game.

Logic Bomb: a program introduced into a computer that is designed to take action at a certain time or when a specific event occurs.

Denial of Service Attack: a large number of computers on the Internet simultaneously send repeated messages to a target computer, resulting in the computer being overloaded or the communications lines are jammed so that legitimate users cannot obtain access.

FIGURE 14.1 **Common Techniques Used by External Attackers**

The types of losses from computer crimes (sometimes called **e-crimes**) can take many forms. Many involve data breaches, such as the loss of medical data or financial data of individuals, especially credit or debit card data. The largest customer data breach to date involving retailers or financial institutions took place over a multimonth period, and industry experts have estimated that the total business losses could be close to $1 billion (see the box "Customer Data Theft at TJX"). In August 2008, the U.S. Department of Justice indicted 11 individuals for this e-crime: three from the United States (including the alleged ringleader), two from China, and the rest from Eastern Europe.

The perpetrator of a computer crime can be a **hacker** or a **cracker.** Hackers usually intend no harm to humans and justify their actions as helpful in pointing out vulnerabilities in computer security practices or particular software products—for example, geeks upset with the dominance of Microsoft operating systems. In contrast, crackers use hacking techniques to intentionally steal information, wipe out hard drives, or to do other harm, including attacks on governments (see box "Cyberwarfare ").

Although *outsiders* therefore pose the greatest security threat to organizations, *insiders* (current employees and former employees) still continue to be the source of a computer crime in about 20 percent of incidents. Typical insider crimes are gaining unauthorized access to information, systems, or networks, or thefts of intellectual property rights, trade secrets, and research and development knowledge by employees who are authorized to have access to the information that they are stealing. Many companies attempt to minimize this type of risk by immediately canceling the computer passwords of an employee who quits or is fired; the employee may even be watched as they clean out their belongings and are escorted off the premises (see box "How Ex-Employees Can Be Dangerous").

Another growing source of e-crime is an organization's business partners who have access to their information resources—including IT vendors, other suppliers, consultants, and contractors. Recent surveys about data breaches experienced by customers at Verizon who used the services of their risk management team found that up to one-third of data breaches implicated one or more business partner.

The globalization of business also brings increased information security risks from business partners. For example, many organizations enter into joint ventures or other strategic alliances for research and development, new product manufacturing, or product testing. Offshore outsourcing has also become increasingly common, with third-party firms processing an organization's payroll or claims data. Some firms also use application service providers (ASPs) that host applications and store customer data for multiple client organizations. All of these business partner arrangements increase information security risks.

Customer Data Theft at TJX

TJX Companies is a $17 billion retailer with more than 2,500 retail stores in North America, the British Isles, and other countries. For a period of more than six months, credit card information of between 45 million and 200 million customers was stolen.

How did the information thieves do this? The evidence suggests that it was not that difficult: It is believed that they tapped into wireless networks, gained administrative control of large databases, and freely downloaded immense amounts of unencrypted information from the company's data warehouse. By any reasonable auditing standards, TJX was guilty of gross negligence. It had complied with only 3 of the 12 required control objectives specified in a data security standard (PCI-DSS) created by major credit card companies.

What was the cost of this theft? TJX will also be spending well over $100 million for badly needed security upgrades, but this dollar amount does not come close to the dollar amount associated with the loss of reputation, goodwill, and opportunity costs for TJX. Financial institutions were also projected to spend over $300 million to replace the credit cards of these TJX customers. By 2009, TJX reported they had already spent $202 million to deal with the data theft, including legal settlements. Forrester Research estimated that the cost to TJX could surpass $1 billion due to consultant costs, security upgrades, attorney fees, and additional marketing to assure customers that their systems were now secure.

[Based on Pereira, 2007; Laudon and Laudon, 2010; and Panko, 2010]

Cyberwarfare

Cyberwar refers to attacks on the IT infrastructure of the enemy with the intent to disable or disrupt the function of the military or the economy of the enemy. Military targets might include command-and-control systems, air defense networks, and computers embedded in weapon systems. Civilian targets might be power grids, financial networks, air traffic control systems, and contractors with military defense departments. There have been a number of incidents that may or may not have been examples of cyberwarfare. In 2007, there were almost 13,000 attacks on U.S. government agencies, and in April of that year, during a dispute between Russia and Estonia over the removal of a Soviet-era statue, sophisticated **denial-of-service attacks** via the Internet shut down Web operations of Estonia's largest bank, several newspapers, and the Web sites of its parliament, the president, and the prime minister. Although most Cyberwarfare developments are cloaked in secrecy, in 2009 a Cyber Command was established in the U.S. Pentagon to defend national security and carry out offensive operations inside computer networks.

How Ex-Employees Can Be Dangerous

Committing a crime against a current or former employer can also sometimes be a way that individuals "get back" at a company for real or perceived transgressions. For example, an insurance company employee who was fired from his IT job planted a **logic bomb** that went off after he left the firm and destroyed more than 160,000 records used to pay monthly payroll commissions.

Layer #1: Perimeter Layer (web servers, mail servers, etc.)	Firewalls VPN encryption Network-based anti-virus	*Pros:* lots of vendor solutions, easy to implement *Cons:* hackers can easily penetrate it
Layer #2: Network (LAN/WAN)	Intrusion detection systems (IDS) Vulnerability management systems Network access control User control/authentication	*Pros:* solutions provide deep security not easy to breach and regular monitoring *Cons:* IDS tend to report false alarms; some solutions better for specific network devices rather than network as a whole
Layer #3: Host Security (individual computer, server, router, etc.)	Host IDS Host anti-virus	*Pros:* solutions provide good operational protection at device level *Cons:* time-consuming to deploy as are fine-tuned for individual devices
Layer #4: Application	Public key interface (PKI) RSA Access control/authentication	*Pros:* encryption provides robust security *Cons:* overhead results in slower system response
Level #5: Data	Encryption	*Pros:* solutions provide good security *Cons:* Dependent on good organizational policies and good execution by data steward

FIGURE 14.2 **Security Technologies by OSI Layer**

Some computer crimes take advantage of unwary users by **spoofing**—a technique in which a Web site that mimics a legitimate site is set up for the purpose of misleading or defrauding an Internet user. A message board or e-mail might be used to direct the victim to the spurious site, or the spoofer might simply use a close variant of another site's URL to con people who make an innocent typing mistake. This type of practice is called **social engineering.**

Most of today's organizations typically have invested in a variety of technologies for each layer of the OSI model—beginning with firewalls at the perimeter, automated **virus** scanning technologies, physical security systems, **spyware/adware** detection software, automated or manual "patch" management, and other sophisticated network traffic monitoring and tracking tools—or have contracted with service providers to provide such security (see Figure 14.2). Identifying and justifying these types of technologies is an IT manager's responsibility, but all managers responsible for information security compliance should be kept apprised of the technology basics so that they can participate in decisions about capital investments as part of an organization's approach to security management.

In the next section we discuss the relatively new organizational role responsible for information security: the Chief Security Officer role. However, good security management also depends on alert and dedicated IT employees. For examples of thwarted (or minimized) computer crimes due to actions taken by skilled IT employees, see the box "E-Crimes Solved by IT Professionals."

E-Crimes Solved by IT Professionals

Defacement of Web site: tracked down the defacer: he was convicted and served three years in a federal prison.

Attempt to plant logic bombs and password sniffers: non-American hackers (Asian and Eastern European) were detected and threat was avoided

Infected PC of a contractor was spreading a virus: it was caught in the first hour of being online

THE CHIEF SECURITY OFFICER ROLE

Because of new laws and increased security risks, many organizations have implemented a position for security department heads at an officer level: chief security officer (CSO). Also sometimes referred to as a chief information security officer (CISO), the CSO is responsible for continually assessing an organization's information security risks and for developing and implementing effective countermeasures. Managers in this role do not need to have a computer engineer's level of understanding of security technologies. Rather, a CSO needs to be able to talk knowledgeably with technical staff about mature and emerging technologies for information security.

A key governance issue associated with this role is where in the organization the CSO should report. Many CSOs report to CIOs. However, security is much broader than IT security and requires productive relationship with many other departments in the firm, including human resources, legal, auditing, facilities management, and any other units or directors with responsibilities for ethics, compliance, and privacy (Panko, 2010).

The goal of the CSO is not to eliminate all information risk. Rather, the goal is to identify and prioritize all relevant risks, totally eliminate those risks that can be eliminated with a reasonable investment, and mitigate other risks until the point of diminished returns for security investments. Of course, determining that point of diminished returns can be quite difficult.

For understanding the potential value of having a highly competent CSO, one need look no further than the most recent front-page headline about a security flaw. In the United States it is even legal for a vulnerability to be disclosed to the public before an IT industry vendor has a chance to fix it—which recently happened when a Google researcher who discovered a flaw in Microsoft software made his finding public (Worthen, 2010).

RISK MANAGEMENT FOR INFORMATION SECURITY

In Chapter 11 we discussed some risk management techniques for assessing and managing IT project risks—including identifying risks and choosing appropriate actions based on managerial assessments. Information security activities are also based on risk management practices.

A key responsibility of a CSO is to continually assess how to achieve the best balance between the costs versus benefits of risk management practices. You personally wouldn't want to pay $10,000 to protect yourself from an estimated potential loss of $5,000, and organizations don't either. Determining how much the organization is paying for security is relatively easy, The challenge here is in estimating potential losses.

Although after a major system intrusion, information security managers may be asked to do 'whatever it takes' to secure a system, these of course are temporary orders. Those responsible for security management need to be able to answer the following:

> *What human resources and financial assets are to be deployed, in what proportions, to protect what assets?*

This is the essence of information security management, and both quantitative and qualitative means are used to provide the answers to these questions.

First, management must determine what their real information assets are and assign values and priorities for them. It is easy to overlook valuable information assets, and organizations often do not know what they are dependent upon until they lose access to it. So it is imperative that managers take a systematic approach to identifying all of their critical information assets and what business processes are dependent upon what specific information systems.

Second, management must determine how long the organization can function without a specific information asset—which is typically one hour, half a day, one day, two days, one week, or about one month.

Third, departmental managers and the owners of the information assets then need to develop and implement the security procedures to protect these assets. The security budget should include both the dollar outlays and the personnel dedicated to the task.

As shown in Figure 14.3, for each information asset and the business goals they enable, the known vulnerabilities are explicitly stated, and an estimate is provided for what a single loss expectancy (SLE) would cost. An SLE can be difficult to determine because the variance can be large. For example, one intrusion can be somewhat harmless, but another can cost many thousands of dollars.

The best sources to use here are based on the (1) historical experiences of the organization and (2) industry averages. For example, the organization in Figure 14.3 had experienced laptop theft in the past two years, which it concluded had led to the loss of several contracts. If an organization has experienced this type of loss before, the impacts will be easier to estimate. If not, industry statistics may be available to help determine potential losses from specific vulnerabilities.

Information Asset	Goal	Vulnerability	Single Loss Expectancy (SLE)	Annual Occurrence Rate (AOR)	Annualized Expected Losses (AEL)
Private corporate information on laptops	Complete privacy of all important corporate information on laptops	Laptop theft and copying of information from them	$50,000	1.5 times*	$75,000
Company e-mail	Complete e-mail privacy of all important communications	Intercepting e-mail	$10,000	6 times	$60,000

*Based on the theft of three laptops in the past two years.

FIGURE 14.3 **Risk Management Assessment by Information Asset**

The annual occurrence rate (AOR) is simply your estimation of how often this loss happens each year. You multiply this times SLE to get the annualized expected losses (AEL).

$$\mathbf{SLE} \times \mathbf{AOR} = \mathbf{AEL}$$

Similar to Figure 14.3, precise numbers can be calculated to justify security budgets and resource deployments. However, many information crime statistics are actually somewhat "grey areas" due to the difficulties of knowing that an information theft has occurred and a reluctance on the part of companies that were victims in the past to make an information theft public.

When someone steals your camera, you know it is stolen, and the thieves do not leave a copy of it. But information theft is different: It can be stolen, but you still can have your copy of it. In fact, if the thieves are skillful, you actually may never know that it happened: The true information criminal will never tell you that he or she has stolen your information because they will want to come back and do it again, and again. Another reason for poor statistics on information theft is the reality that the victims historically have been unwilling to admit that it has happened. Companies have been silent about information theft in the past because of the bad publicity and legal liabilities that accompany it.

But new laws for the reporting of information theft have led to new behaviors in the last few years. For example, California's State Law 1386 went into effect on July 1, 2003. This law requires all organizations that store information on California residents to report to their citizens any information theft within 96 hours. Failure to do so can have both civil and criminal remedies. (see the box "Silence Is No Longer an Option.")

For calculating the importance of data to an organization, business managers need to be involved to help justify and prioritize investments in information security technologies. Using a scale of 1 through 5, the relative importance of each information asset can be calculated to help determine what assets are the most important for the organization and to determine what percentage of a security budget should be allocated to the different information risks identified. In addition, managers today need to take into account the risks of financial penalties due to an organization's noncompliance with federal or state laws, as described in the next section.

Figure 14.5 includes some recent information security breaches involving large numbers of personal records. These examples include breaches that are criminal attacks

Silence Is No Longer an Option

After performing a quantitative risk analysis for all information assets, the annual expected losses (AEL) figures are used in a security cost-benefit analysis (see Figure 14.4). For example, using strong third-party encryption technology to ensure the confidentiality of laptop information was estimated to cost $100 per laptop, and the organization had about 200 laptops that were exposed to such loss. Security prevention solutions are listed in an Actions column, and both one-time and continuing costs are determined for each action. The total costs of the actions are then subtracted from the annualized expected losses (AEL) to determine the benefits to the organization from taking these actions.

Information Asset	Goal	Annualized Expected Losses (AEL)	Actions	Annualized Cost of Actions	Return Benefit
Private corporate information on laptops	Complete privacy of all important corporate information on laptops	$75,000	implement strong third-party encryption on all laptops	$20,000*	$55,000
Company e-mail	Complete e-mail privacy of all important communications	$60,000	implement a client-to-client e-mail encryption system	$20,000	$40,000

*Based on $100 per laptop for 200 laptops.

FIGURE 14.4 Security Cost-Benefit Analysis by Information Asset

Organization & Date	Information Security Breach
Blue Cross Blue Shield – 2009	Personal laptop stolen with unencrypted copy of database with national provider ID number and personal information of more than 850,000 physicians and other U.S. healthcare providers
Kaiser Hospital – 2009	Hospital fined $182,500 and $250,000 by State of California for privacy violations involving at least 27 employees improperly accessing records of octuplets mother and her children
TJX – 2005	More than 45 million customers' credit card information was stolen over a period of more than 6 months
U.S. Military – 2009	Computer hard drive with data for 76 million U.S. veterans was erroneously sent out for repair

FIGURE 14.5 Examples of Information Security Breaches with Major Impacts

as well as careless employee actions. Data breaches due to stolen, lost, or misplaced computer equipment have been on the rise. The loss of a single server, laptop, or portable storage device also has the potential to negatively impact the company's reputation and the level of trust in the company by its customers.

COMPLIANCE WITH LAWS AND REGULATIONS

In this section we summarize the relevant characteristics of several recent U.S. laws on financial and personal health information transactions, which have important impacts on information security practices in organizations. Following brief descriptions of some laws that have had the greatest corporate impacts are provided in Figure 14.6. Then we discuss them in more detail. Similar laws and regulations can also be found in the European Union (e.g., Basel II) and other developed countries (e.g., J-SOX legislation in Japan).

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act of 2002 (SOX) was passed in response to the corporate financial frauds at companies such as Enron, in which many employees lost not only their jobs but also their savings for retirement. SOX has had a major impact on the accounting, record-keeping, and controls landscape for all publicly traded corporations doing business and/or being traded in the United States. (Similar laws and regulations also exist in the European Union and other developed counties.)

To avoid serious legal liabilities, managers need to know the following:

Records Retention: SOX specifically states that corporations must retain all relevant e-mail and instant message records for a minimum of five years, to guarantee that the auditors can easily obtain the necessary documents. This rule has spurred the growth of **electronic records management** (ERM) software, which

Law	Date Enacted	Purpose	Penalties
Health Insurance Portability and Accountability Act (HIPAA)	08/21/1996	Standardization and confidentiality of health data.	Both civil and criminal, with maximums of $250,000 in fines and 10 years in prison.
Gramm-Leach-Bliley Act (GLBA)	11/11/1999	Privacy of personal financial and credit information.	
The PATRIOT Act	10/26/2001	(relating to information security) Keep records of all financial transactions over $10,000. To allow the government to see all telephone, e-mail, and financial information without a search warrant.	Varies, depending upon intent. Deliberate violation and/or noncooperation with governmental inquiry is a felony.
Sarbanes-Oxley Act (SOX)	7/30/2002	Integrity in financial statements and disclosures, internal controls, and auditor independence.	Organizations can be fined up to $100,000. Individuals up to $10,000 and 5 years in prison.
California Information Practice Act (Senate Bill 1386)	07/01/2003	Mandates full and quick disclosure to anyone who has had their information lost or stolen from any company doing business in California.	Allows civil lawsuits for loss of information. The most serious penalty is negative publicity from public exposure.

FIGURE 14.6 **Recent U.S. Laws with Information Security Impacts**

can categorize the type and retention time for specific electronic documents, and ensure their retention. (See the ERM discussion later in this chapter).

IT Audit Controls: Section 404 of SOX states that the officers of publicly traded companies in the United States must now certify that they are responsible for establishing and maintaining internal controls. These officers are required to have evaluated the effectiveness of the internal controls within 90 days prior to the report. Section 404 also requires management to produce an internal controls report as part of each annual Exchange Act report.

The Committee of Sponsoring Organizations (COSO) has created a framework for auditors to assess controls. The COSO guidelines now require the chief information officer (CIO) to be directly responsible for the security, accuracy, and reliability of the information systems that manage and report the financial data. Because the CEO and CFO of companies are typically dependent upon the CIO's controls, the CIO is now critically involved in the sign-offs of a company's financial statements.

The COSO framework specifically impacts information technology in the following five areas:

Risk Assessment: Management must first conduct a risk assessment of the information systems affecting the validity of the financial statements.

Control Environment: Employees should have an environment where employees are involved in the decisions affecting the quality assurance, security, and confidentiality of their information systems.

Control Activities: The design, implementation, and quality assurance teams should be independent. The organization must document usage rules and demonstrate the reliability of audit trails. Management must be able to demonstrate segregation of duties (SOD) within their critical processes where there can be conflicts of interest and increased opportunities for fraud.

Monitoring: Management must create systems that allow for quick and accurate internal audits, and should perform these audits on a schedule appropriate to their level of risk. Management must clearly understand that they are responsible for the results of these audits.

Information and Communication: IT management must be able to demonstrate to management that they are in compliance with SOX. They must be able to demonstrate that they can quickly respond to any

changes in information that would affect financial reporting and SOX requirements.

Gramm-Leach-Bliley Act of 1999 (GBLA)

The GLBA mandates all organizations to maintain a high level of confidentiality of all financial information of their clients or customers. The GLB Act gives authority to eight federal agencies and states to enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to all banks and lending companies, securities firms, insurance companies, and credit-reporting consumer loan agencies. It applies to anyone involved in transferring or safeguarding money, preparing of individual tax returns, providing financial advice, credit counseling, residential real estate settlement services, or collecting consumer debts. With such a broad scope, it seems fair to say that some aspect of most businesses comes under the jurisdiction of the GLB Act. (For a discussion of the law from a customer perspective, see the Laws on Privacy section within Chapter 15.)

THE FINANCIAL PRIVACY RULE The Financial Privacy Rule requires financial institutions to give their customers privacy notices that explain the financial institution's information collection and sharing practices. GLBA requires that the organization must clearly state their privacy policy at the time of establishing the relationship. In turn, customers have the right to limit some sharing of their information.

Financial institutions and other companies that receive personal financial information from a financial institution are now limited in their ability to use that information. Financial institutions may not disclose to a third party any nonpublic personal information. This includes account and credit card numbers, social security numbers, or any otherwise private information that could allow someone to obtain more information from it. Failure to do so can lead to serious civil penalties.

Health Insurance Portability and Accountability Act (HIPAA)

Organizations that deal with electronic transactions of medical records, medical payments or remittance advice, insurance claims, eligibility requirements, or medical referral information must be in compliance with **HIPAA** privacy and security rules. Organizations that have insurance policies for their employees must also comply. Noncompliance with HIPAA's confidentiality standards can lead to serious civil penalties and fines.

If HIPAA applies to an organization, its management must do the following:

1. Assign a person/persons to be responsible for HIPAA compliance
2. Familiarize staff with the key HIPAA compliance issues
3. Know how the law specifically affects the organization
4. Insure in writing and with audits that all of the relevant business organizations it worked with also are HIPAA compliant.

The PATRIOT Act

The PATRIOT Act greatly reduces the requirements for the government to access information. U.S. law enforcement agencies are now permitted to request business and financial records and use electronic surveillance from organizations without court search warrants. These provisions apply especially to banks for searching money trails and in the use of roving wiretaps for communication companies.

The PATRIOT Act allows victims of computer hacking to request law enforcement assistance in monitoring the "trespassers" on their computers. This change made the law technology-neutral. It placed electronic trespassers on the same footing as physical trespassers. Now, hacking victims can seek law enforcement assistance to combat hackers, just as burglary victims have been able to invite officers into their homes to catch burglars.

The PATRIOT Act extends the money-laundering act of 1986 so that it is mandatory for financial institutions to file a Currency Transaction Report (CTR) for all cash transactions greater than $10,000. It also amends the Bank Secrecy Act of 1970 to lower the legal standards for disclosure.

ORGANIZATIONAL POLICES FOR INFORMATION SECURITY

Every organization today needs to have a clear information security policy that takes into account the information risks to be managed and the compliance needs with laws such as those discussed previously. There are no "implied" security policies:

> *If your security policy is not written down, your organization has no security policy.*

Publicly traded organizations with no written security policy are automatically out of compliance with Sarbanes-Oxley. In addition, insurance companies today will not insure an organization that does not have a clearly written security policy. This is the current business environment, and it is likely to continue to be this way well into the twenty-first century.

Security policies should be written at a high level, and should state what is, and what ***is not***, permissible. There should be no ambiguity in the policy. One should also not substitute existing civil or criminal laws for an organization's security policy. Instead, the policy should explicitly state that such acts are prohibited.

Policies should also clearly state what the punishments are for violation of the policy. This gives management the justification they need to quickly remove any employees who behave improperly: The organization may not yet know whether they have violated the law or not, but if you can prove that they have clearly violated the security policy, then you have clear grounds for employee dismissal.

Although another company's security policy will never be a perfect fit, "boilerplate" information security policies can often be found on the Internet or in other sources. The actual implementation details of the policy, however, should be in a procedures manual, not in the security policy itself.

WHO SHOULD DEVELOP THE SECURITY POLICY? Unless an organization is quite small, it should establish a security policy committee with representatives for as many affected user groups and other stakeholders as possible. This helps ensure not only good policy content but also employee support for the written policy. If a security policy does not have the support of the managers who must administer and abide by it, it will fail.

Then, all relevant employees should be asked to read any new policy developed by the committee (on company time) and be given an easy way to ask any questions about it; if the policy isn't clear, it should be rewritten to be more understandable for the internal worker. Whenever significant changes are made to a policy, this process should be repeated with all affected employees.

Because the technological and legal environments constantly change, the security policy committee should have regular, scheduled meetings to develop and vote on any changes or additions to the policy. Developing a security policy is an ongoing task, rather than an end goal.

WHAT SHOULD BE IN THE SECURITY POLICY? A security policy needs to be written for everything that affects the information integrity and confidentiality of the organization. It should state what the organization does to be in compliance with current laws, and what exactly an employee can, and cannot, do with organizational information.

An organization may actually have many security policies (Barman, 2002), or it may have a single, comprehensive security policy that is a compendium. Common policy areas are:

- Access Control Policies: password log-in and access controls, encryption, and public key infrastructures
- External Access Policies: Internet security, VPN access, Web and Internet, and e-mail
- User and Physical Policies: Acceptable use, network architecture and address, and physical security

Password management policies and formal policies on **acceptable use** of an organization's computer resources are most commonly used to prevent or reduce e-crime. For example, an acceptable use policy typically includes statements about the following:

- The organization's computing resources (hardware, software, network services) are company property.
- An employee does not have privacy rights to their usage of these computing resources (e-mail, usage of Internet sites, etc.).
- Specific types of computing behavior are prohibited by federal or state laws (e.g., electronic libel or defamation, impersonation of others, unauthorized copying of protected intellectual property).
- Other types of actions are also not permitted by the organization (e.g., use of resources for personal profit, transmission of an image that is sexual in nature, initiation or forwarding of chain letters).

Today's organizations are also updating their acceptable-use policies to include the usage of social media.

HOW STRICT SHOULD A SECURITY POLICY BE? The rigidity of the policy should be appropriate for the estimated risks to the organization. A mantra used by some is: Tighten it up until it hurts, and then loosen it up until it works.

WHEN AND HOW SHOULD AN ORGANIZATION DEVELOP A SECURITY POLICY TO ADDRESS A NEW SITUATION? A new policy should be developed as soon as possible: The longer an organization operates without a complete policy, the greater are the information and legal risks. For example, social media is now in widespread use, but not all organizations have updated their policies on the usage of sites such as Facebook, Twitter, and LinkedIn.

HOW SHOULD POLICIES BE DISSEMINATED? The organization should make it easy for all employees (including contractors) to know where they can find the most current version of a security policy. Manuals are typically made available to all employees, and policies are typically included in training materials. Less common today are hard copies of manuals: Organizations have increasingly been distributing policies on the organization's

intranet, with e-mails sent to employees about policy changes or totally new security policies.

New employees should be asked to thoroughly read existing security policies and then sign them as a condition of employment. Some organizations require all of their employees to review and accept their appropriate usage policy on an annual basis. In some situations, the employee may be asked to acknowledge acceptance of the policy each time data is accessed.

PLANNING FOR BUSINESS CONTINUITY

In the past, IS leaders have focused on activities to keep IT resources operating as part of "disaster recovery" contingency planning. For example, many organizations have contracts with external service providers to provide backup data center processing and telecommunications support. However, business continuity planning (BCP) involves much more than IT recovery from a natural disaster—such as a flood, tornado, earthquake, hurricane, or fire. BCP involves putting plans in place to ensure that employees and core business operations can be maintained or restored when faced with any major unanticipated disruption. Research has shown that an organization's inability to resume in a reasonable time span to normal business activities after a major disruption is a key predictor of business survival. As many U.S. organizations learned after the 9/11 terrorist attacks, and Hurricane Katrina and the New Orleans floods that followed in 2005, business continuity also requires having:

- Alternate workspaces for people with working computers and phone lines
- Backup IT sites that are not too close but not too far away (to be within driving distance but not affected by a regional telecommunication disaster)
- Up-to-date evacuation plans that everyone knows and has practiced
- Backed-up laptops and departmental servers, because a lot of corporate information is housed on these machines rather than in the data center
- Helping people cope with a disaster by having easily accessible phone lists, e-mail lists, and even instant-messenger lists so that people can communicate with loved ones and colleagues

The process for creating a BCP begins with a business impact analysis, which can include the following:

1. Define the critical business processes and departments
2. Identify interdependencies between them
3. Examine all possible disruptions to these systems
4. Gather quantitative and qualitative information on these threats
5. Provide remedies for restoring systems

For item 3, some dependencies that affect access to organizational information are obvious—such as electricity, communications, and Internet connections. Others may be less obvious, such as the maximum tolerable downtime for each application system. Traditionally, these have been measured in categories like Lower-priority = 30 days, Normal = 7 days, Important = 72 hours, Urgent = 24 hours, and Critical = less than 12 hours.

This process should result in quantitative rankings, along with qualitative judgments, about the severity of the disruption, which are then used to determine an appropriate remedy for system restoration. The BCP should also state who is responsible for doing what, under which conditions. Templates for logs and other documentation should be available to implement the plan.

BCP plans should also be tested. In fact, testing a BCP may be the most costly part of the process, as it demands pulling staff away from their normal work to simulate a parallel situation to which a disruption occurs. It is also difficult to test a plan because of the potential scope of the disaster. Depending on the organization's industry, auditors may require periodic testing within a certain time frame.

Nevertheless, sometimes an organization discovers that a disaster far exceeds the assumptions it used to develop its BCP. This happened, for example, to Northrop Grumman Corporation, a $30 billion defense and technology company that had about 20,000 employees working in its Ship Systems sector in two states bordering on the Gulf of Mexico, where Hurricane Katrina made landfall in August 2005 (see "Post-Katrina BCP Lessons").

ELECTRONIC RECORDS MANAGEMENT (ERM)

The importance of electronic records management has grown as recent U.S. laws have required that an organization must retain certain records for a minimum period of time. For example, Section 802 of Sarbanes-Oxley requires that public companies and their public accounting firms maintain all audit and review work papers for five years. The Internal Revenue Service can require a period of seven years, and willful destruction of corporate audit records can result in sentences of imprisonment for up to 10 years. The Department of Education requires that guarantors of federal student loans maintain records for a minimum of five years after the loan is repaid. HIPAA gives individuals the right to receive an accounting of any disclosures of their public health information for up to three years prior to

Post-Katrina BCP Lessons

Northrop Grumman Corporation learned a lot about Business Continuity Planning from Hurricane Katrina—the hard way. Here are four of its lessons:

— Keep Data and Data Centers More Than 100 Miles Apart

The BCP assumption was that a backup data center facility only needed to be a minimum of 100 miles away from the facility it was backing up. But Katrina's width exceeded this distance, and two data centers that served as backups for each other got wiped out

— Plan for the Public Infrastructure to Not Be Available

Katrina wiped out all public communications in the company's Gulf Coast location. In addition, roads were washed away or closed and airports were shut down; water was also shut off or, if not, it was polluted.

— Plan for Civil Unrest

Personnel had to be brought into the area to secure a physical facility

— If Your A team Is Not Available, Assemble a B Team

The company's qualified technical support personnel weren't available, so other employees were trained to work with IT industry suppliers to assemble and test new equipment

[Based on Junglas and Ives, 2007]

the date a request is made. Tiered penalties (e.g., unintentional disclosures versus willful neglect) include both large civil fines and even criminal imprisonment. There are currently over a dozen major laws within the United States alone that require information retention and protection.

In general, most businesses have greatly underestimated their **digital liability** for actions their employees have taken. For example, Microsoft executives clearly did not think out the consequences when sending e-mails about Netscape (see the box entitled "Is E-Mail Forever?").

Digital liability management requires ensuring that managers are knowledgeable about the risks involved in information mismanagement, the need for precise policies, and the legal and regulatory environment that its

Is E-Mail Forever?

The basis of a U.S. government antitrust case against Microsoft was that Microsoft conspired to use its monopoly on the desktop computer market to drive Netscape (which introduced the first commercial browser) out of business. Microsoft denied it—but were there copies of incriminating e-mails somewhere to prove otherwise? Yes—there were hundreds of e-mails, all on servers outside of Microsoft.

How can this happen? If an organization is using Open Shortest Path First (OSPF) routing, then it is allowing the network to choose the quickest route to send its information, including its e-mail. This means that an e-mail could pass through a number of public servers anyplace on the continent. The sending organization has no control over these servers, and these machines are constantly backing up the information passing through them. Thus, it is very reasonable to assume that there will be discoverable electronic copies archived somewhere.

Recent history has also shown that companies cannot even control their e-mail on their own private subnets. Individuals can make copies, save them, forward them, and most definitely do not "wash" them forever off their storage devices.

So: **Is e-mail forever?** As users and managers, you should assume that yes—it is. In other words, it is much more probable that a computer forensics specialist will be able to recreate the e-mail than the creating person will be able to erase it forever from everyplace.

organization faces. All digital liability management must be based upon risk analysis. This may seem obvious, but business history is littered with cases of companies that did not assess the risks of their actions.

The sheer complexity of large organizations, in combination with changing national and international laws and the increased use of electronic documents, requires a centralized approach to electronic records management (ERM). In many organizations, an investment in not only ERM specialists but also commercial, off-the-shelf ERM software may be justified.

In general, an ERM manager (or an ERM committee) should be responsible for the following:

1. *Defining* what constitutes an electronic record. Electronic records include not just e-mail, but financial records, research and development, IM messages, customer and transaction databases, and many others.
2. *Analyzing* the current business environment and developing appropriate ERM policies. For example, what should be kept, and for how long? When and how should records be destroyed? Who can make copies, and on what types of media? Where are these media copies kept, and who has access to them?
3. *Classifying* specific records based upon their importance, regulatory requirements, and duration.
4. *Authenticating records* by maintaining accurate logs and procedures to prove that these are the actual records and that they have not been altered.
5. *Formulating and managing policy compliance* The ERM policies must have precise controls, explaining what is to be done, when it is to be done, who is to do it, with logs and controls to prove that the policy has been complied with. Employees need to be trained and policies need to be regularly audited for completeness and currency.

Amendments to the U.S. Federal Rules of Civil Procedure (FRCP) that took effect in December 2006 place a new burden on records managers for the purposes of records retention and timely information gathering in response to potential litigation. Failure to comply with these **eDiscovery amendments** can lead to severe financial penalties, so good ERM practices have become an important part of information risk management (Volonino et al., 2007). Additional FRCP amendments in 2009 clarified that businesses are required to preserve and produce electronically stored information that may be relevant to a lawsuit *even before the lawsuit is filed* (Ward et al., 2009).

Summary

Today's organizations are increasing their investments in information security practices and budgets for information security technologies. This does not mean that organizations strive to be completely secure. Rather, it means that, to the best of current technical and information management knowledge, an organization seeks to minimize an organization's risks at an acceptable cost level. Based on a thorough risk analysis, the organization's resources, and its current legal and regulatory environment, the organizational goal is to find the appropriate balance between accessibility, integrity, and confidentiality.

An organization must be in compliance with current laws. Noncompliance is not an option, and a company's employees need to be educated on all of the relevant laws for their position and their organization.

Information security management needs to be viewed as a process and never as an achievable end state. A CSO, high-level business manager, or organizational committee needs to be responsible for assessing the impacts of changing regulations or other work environment changes. IT managers are responsible for assessing and implementing security technologies, as well as assessing new risks associated with new technologies. Together they need to develop and implement new information security policies to address them.

Information security requires continuous adjustments, based on imperfect information, about a potentially hostile and ever-changing external environment.

Review Questions

1. What are some examples of computer crime?
2. What is the difference between a hacker and a cracker?
3. What is the role of a chief security officer, and why is this organizational role a relatively new one?
4. What are the overall goals of information risk management?
5. What resources can organizations use to calculate an expected annual financial loss for a given information asset?
6. Why does the Sarbanes-Oxley Act impact the work of IT personnel?
7. Why is it important for an organization to have an information security policy?
8. What is the specific purpose of an acceptable use policy?
9. What information security issues does electronic records management address?

Discussion Questions

1. Do you think the acts of hackers should be punished the same as those by crackers? Why or why not?
2. Use the Internet to identify a recent report of a computer crime, and summarize what it involved and what the punishment (if any) was.
3. The importance of having vigilant IT professionals who are capable of detecting and minimizing the damage from a security breach has become increasingly important. Is this a type of job position that you would like to hold, and why—or why not?
4. If you were offered the position of a CSO for a large organization, what reporting relationship would you want? Under what circumstances do you think a reporting relationship to the CIO is the best choice?
5. To achieve SOX compliance has required many organizations to significantly change their business processes and invest in new software products. Use the Internet to research some examples of these types of impacts that SOX has had on U.S.-based companies in particular—or J-SOX has had on Japanese companies?
6. HIPAA concerns will be growing over the next years as more physician practices in the United States adopt electronic health records (to take advantage of a federal government incentive plan under the HITECH Act). Find a recent article that discusses concerns about the security of health information of patients.
7. Reflect on when you last received authority to have a computer account with an organization (e.g., your university), and comment on your own experience when you were asked to sign (or otherwise signify acceptance of) an organizational policy similar to the acceptable use policy described in this chapter. Would you recommend any changes to the organization for what to include in the policy and how to present this policy to a new account holder?
8. How easy is it to find out about an information security policy (e.g., an acceptable use policy) at your university? At an organization where you are an employee?
9. What were some of the lessons learned about business continuity planning that can be derived from organizational experiences following the 9/11 attack on the World Trade Center in New York or Hurricane Katrina in 2005?
10. Use the Internet to research some of the IT-related issues that had to be addressed by organizations (or individuals) in a recent natural disaster in your own country.
11. What have been some of the impacts of the eDiscovery amendments on U.S. organizations?

Bibliography

Baase, Sara. 1997. *A gift of fire—social, legal, and ethical issues in computing*. Upper Saddle River, NJ: Pearson Prentice Hall.

Barman, Scott. 2002. *Writing information security policies*. Indianapolis, IN: New Riders Publishing.

Cerullo, Virginia, and M. J. Cerullo. 2004. "Business continuity planning: A comprehensive approach." *Information Systems Management* 21, 3 (Summer): 65–69.

[Health Data Management] *HDM Breaking News*, June 11, 2010. *www.healthdatamanagement.com/issues*. [Last accessed June 14, 2000]

Identity Theft Resource Center. 2010. "ITRC Breach List." *www.idtheftcenter.org* [Last accessed June 28, 2010]

Junglas, Iris, and Blake Ives. 2007. "Recovering IT in a disaster: Lessons from Hurricane Katrina." *MIS Quarterly Executive* 6, 1 (March): 39–51.

Knapp, K. J., and W. R. Boulton. 2006. "Cyber-warfare threatens corporations: Expansion into commercial environments." *Information Systems Management*, 23, 2 (Spring): 76–87.

Laudon, Kenneth C., and Jane P. Laudon. 2010. *Management information systems*, 11th ed. Upper Saddle River, NJ: Pearson Prentice Hall.

Merrill, Molly. 2009. "Breach leaves docs at risk." *HealthcareITNews*, December 3. *www.healthcareitnews.com/news/breach-leaves-docs-risk*. [Last accessed September 25, 2010]

Panko, Raymond R. 2010. *Corporate computer and network security*, 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall.

Pereira, Joseph. 2007. "How credit-card data went out wireless door." *Wall Street Journal* (May 4): A1, A12.

Volonino, Linda, Janice C. Sipior, and Burke T. Ward. 2007. "Managing the lifecycle of electronically stored information." *Information Systems Management*, 24, 3 (Summer): 231–238.

Ward, Burke T., Carolyn Purwin, Janice C. Sipior, and Linda Volonino. 2009. "Recognizing the impact of e-Discovery amendments on electronic records management." *Information Systems Management*, 26, 4 (Fall): 350–356.

Worthen, Ben, and Spencer E. Ante. 2010. "Computer experts face backlash." *The Wall Street Journal*, June 14: B6.

CASE STUDY IV-7

Meridian Hospital Systems, Inc.: Deciding Which IT Company to Join

It was late October of 2009, and Willis "Willie" Stahe was running late. As president of Midwest University's Computing and Information Systems student club, he had helped organize a student-alumni networking event and was relieved to find the room packed for lunch and the afternoon seminar. He threw his backpack into a corner and headed for the podium. After a short introduction and thank you to everyone for coming, he stopped at the buffet table and filled a plate.

As he reached for a crescent roll, he crossed arms with a tall, older man, surprisingly dressed casually. Willie thought his long-sleeved shirt looked like it was flannel. "Sorry. I guess I'm still rushing," Willie said.

"Quite all right. After you," flannel shirt said quietly.

"I feel like I've just been hit by a truck," Willie continued. "I just attended a presentation by this speaker in our Management of Information Systems class. He co-founded a local start-up software firm."

"Sounds interesting," flannel shirt said. Willie raced on, "See, I graduate this semester and I am one of the lucky ones to actually have an offer from Hewlett-Packard to start as a software developer in January. I told them I would get back to them at the end of this week. I just told them that because I was playing it cool. But now, I'd really like to interview with this start-up company. They're here today and Friday only."

"Seems to me like you should go through the interview first. That may help make the decision for you," flannel shirt said.

"The start-up sounds so cool. But Hewlett-Packard—how could I turn that offer down?" Willie thought out loud.

"A lot of software start-ups crash and burn. But in the last few years, some of the large IT companies have had their problems as well. Before you turn HP down, perhaps you should really study this other company," flannel shirt said.

"The speaker did give us some handouts. Plus, I guess I could do some additional library and Internet research myself," Willie said. "Thanks for talking me through this. When did you graduate from Midwest?"

"Alum? Is that why there are so many people here? Is this an alumni event?" flannel shirt asked.

"Yes. Why? You're not an alum?" Willie asked.

"No. I'm here interviewing. We haven't done a lot of campus interviewing, so I don't know the layout here. One of the interviewers said there was a break room down the hall," flannel shirt said.

"Oh. That's down the hall the other way," Willie said.

"Whoops," flannel shirt said. "I was surprised at the crowd given the economy, but I thought Midwest was going all out to retain recruiters!" Willie and flannel shirt laughed. Then flannel shirt said, "It's time I get back. Good luck with your decision."

"Thanks," Willie said and shook flannel shirt's hand. As Willie started to ask his name, the caterer interrupted to ask what Willie wanted to do with the extra food. "Just leave it out. Someone will eat it," Willie said. "No. Wait. Put it in the Placement Office break room. For the recruiters."

As Willie picked up his backpack, he thought about what flannel shirt had said. He would sign up to interview with the start-up Friday. But before that, he would need to do a lot of research. He was going to stop by the gym after the seminar, but decided he had better stop by the library instead.

The Job Opportunity at Meridian Hospital Systems, Inc.

In his class, Willie had been impressed by guest speaker Jim Stone, cofounder and Executive Vice President of Meridian Hospital Systems (MHS), not so much by his colorful charts and demonstration of the company's software as by what he said. He had not expected the co founder of a Midwest company to be so insightful about the current developments in the software industry from both a technology and competitive standpoint. He had always assumed that anybody who was somebody in software was on the West Coast.

This case was developed by Daniel W. DeHayes and Stephen R. Nelson. The case was written to provide a basis for class discussion rather than to illustrate effective or ineffective business practices. Some figures, names, and dates have been disguised.

And the job sounded interesting. Willie would be assigned to a team that was developing MHS's next product offering. As a software developer, Willie would have access to all the tools he had heard about and used in his classes. He would join a small group of eight developers, most of who graduated only one or two years ago. The group would be headed by a 30-year-old with a Ph.D. in computer science.

He found himself excited by the prospects of this company, about how he could have an important role so early in his career. He was excited about Hewlett-Packard, too, but not about what he would be doing so much as that he would be working for Hewlett-Packard. He had already made sure all his friends knew he had been given an offer. And his mom had made sure everyone in the family, the church, her bridge group, the whole neighborhood knew it, too. Even Aunt Nellie in Dallas wrote to congratulate him on the offer. The HP opportunity was even better than when he interned at a large public accounting firm in their IT group last summer.

However, Willie also felt that the offer from HP had its uncertainties. Willie knew from his research that the company had had some troubles a few years ago. While the company had bounced back under the leadership of their CEO (Mark Hurd) and had overtaken IBM as the largest company in the technology sector in 2008, the competition in the hardware, services, and software industries was fierce. HP, Dell, and IBM were each in the process of acquiring and integrating major services firms: HP and EDS, Dell and Perot Systems, and IBM and PricewaterhouseCoopers. And he had heard that Hurd was known for significant cost reductions, and those almost always involved letting people go (the company let over 15,000 people go when Hurd first took over his position). These matters made Willie a little uncertain of this employment option.

But he also knew that job offers at HP were tough to come by, especially during these difficult times in the economy, and he was happy to have received one. At the same time, Willie began to wonder how long he might be employed by the company—particularly if the current economic recession resulted in layoffs. He knew that he would be low on the seniority list. If the company needed to reduce cost to be more competitive, he might be among the first let go. And, as had happened to some of his friends at other firms, the offer might even be revoked after he had accepted.

In his class notes, he read that MHS was founded in 2007 by three software veterans who had worked together for a company that was eventually acquired by IBM. All three had at one time in their careers worked for large corporations. Willie also learned that the founders named Meridian Hospital Systems to reflect their Indianapolis roots (Meridian is the main north/south street in Indianapolis) as well as their target market (hospitals). The focus of the company was to make the process of assembling and processing product orders from diverse units in the hospital easier.

From the MHS Web site, Willie found some additional information about the founders of MHS (see Exhibit 1). Willie knew MHS had not been in business very long, but to its credit it had received several rounds of venture capital investment so someone felt the company was a long-term survivor. Although the risk associated with working for a company that was not well established was great, so was the reward if the company grew as expected. Regardless of the current economic and corporate climate, even Hewlett-Packard started with just two founders and a garage.

MHS's Strategy

Once he had a reasonable idea of the job he would be interviewing for, Willie reviewed what he knew about MHS's market and product strategy from Stone's presentation and some materials he distributed in class.

When creating their business plan in mid-2006, MHS's founders decided to focus first on applying the company's software development skills to a single industry. They were aware from business publications of the difficulty many organizations had in obtaining the best price and terms for products and services, especially if they had diverse operations. They had also read an article about some retailers that had difficulty determining exactly how much product to order in a fast-moving competitive environment with a set of stores spread around a large geographic area.

Accordingly, the founders of MHS decided to focus on a specific market segment that met the following requirements:

- was of significant size with a high volume and velocity of dollars and transactions
- had a readily identifiable block of buying organizations and influencers
- had a need for consolidation of orders from diverse organizations
- did not currently have ways to consolidate orders from departments
- wanted to maintain the role of demand determination in decentralized organizations, yet have centralized accountability and control
- had a unique procurement processing and documentation requirement
- was not especially sensitive to privacy issues or excessive regulatory burdens pertaining to its procured goods and services
- was not overcrowded with first or early movers with software designed to solve the problems

Management

Joseph A. Dobbins, Co-Founder, President and CEO. Dobbins has over 20 years of experience in technology and software. He serves as director of the Midwest Information Technology Association, which focuses on the development of technology companies in the Midwest. He has held executive-level responsibility for all aspects of a technology company, including sales, marketing, product development, and operations. Previously, he was vice president and COO for an IBM company focused on enterprise software for customer relationship management (CRM). Dobbins has delivered dramatic revenue growth, routinely overachieving all financial and operational targets. Dobbins has also been senior vice president for a software vendor for the consolidated service desk market (help desk, asset management, change management, decision support). Once this company was acquired, he became senior vice president for worldwide operations, establishing a global direct and indirect sales organization. Dobbins directly managed creation of North American, European, and Asia-Pacific operations. Dobbins began his career at Xerox and Honeywell in sales/sales management. He holds a B.S. degree from the University of Detroit.

James S. Stone, Co-Founder and Executive Vice President, Product Group. Stone was previously vice president and CTO for IBM's Corepoint, where he had responsibility for all product and business strategy aspects and where he managed a 550-person global product effort across five geographic sites and four product families. Earlier Stone managed a shift in product direction toward integrated technologies and applications. Prior to Corepoint, Stone was general manager and vice president for a software vendor for the consolidated service desk market (help desk, asset management, change management, decision support) where he was responsible for product development. He led the effort to launch a new business unit into the fast-growing customer relationship management (CRM) enterprise software market. Stone started his technology career at BorgWarner Automotive Research Center, developing advanced vision-guided robotics. He then spent several years at Eli Lilly, a leading pharmaceutical firm, developing enterprise-level applications and very large databases for Lilly Research Laboratories. Stone holds an M.B.A. degree from Indiana University and a B.S. degree in computer science from Ball State University.

Matthew B. Mahoney, Co-Founder and Executive Vice President, Marketing. Mahoney has spent 19 years in marketing management and entrepreneurial business development, ranging from start-ups to Hewlett-Packard. Previously, he was vice president of worldwide marketing for Corepoint where he was responsible for a $26 million marketing budget and 45 people across five global regions. He successfully planned and executed a comprehensive marketing launch of the company in a remarkable 12 weeks, attaining significant awareness levels within the Global 1000. Mahoney spent the first nine years of his career at Hewlett-Packard where he marketed UNIX, manufacturing automation systems, and software to major accounts, and consulted with the company's value-added reseller channel partners. One client, a leading industrial engineering simulation and production scheduling software firm, recruited him to manage its newly formed alliance with IBM. There, he headed marketing and developed the company's first channel marketing program. For the past 15 years, Mahoney has participated as investor and director in local entrepreneurial ventures. He holds a B.S. degree in electrical engineering technology from Purdue University.

EXHIBIT 1 **Meridian Hospital Systems Management**

Source: Company Records.

After an analysis of several industries, MHS's founders chose hospitals as their initial targeted industry. They found that hospitals met all the criteria. They next conducted 12 interviews with hospital administrators to verify that the reported problems in procurement did indeed exist. They also found that it was typical for hospitals to spend between 20–40 percent of their annual revenue on goods and services. The diverse nature of hospitals made it very difficult to effectively control the procurement process to insure the most favorable pricing and terms. The hospital market was well-known for not being very efficient in taking advantage of quantity discounts in its purchasing procedures. Stories about hospitals placing an order today for some product and tomorrow ordering the same product were quoted during MHS's market research. During these interviews, hospital administrators expressed considerable interest in software that would help solve their problems in procurement.

Hospitals were traditionally highly decentralized in their operations due in part to the wide variety of special knowledge needed in order to procure the correct products. In turn, departments guarded their decision-making authority closely. It was also true that these departments often developed close relationships with certain suppliers that negated the effects of competition when it came to buying. It was only after the continuing increase in cost pressures that more centralized processes could be instituted. In addition, the hospital industry traditionally was slow compared to many other industries to adopt new information technology. Hospitals spent a smaller percentage of their overall operations budget on information technology as compared with many other industries.

Based on the founders' market research, MHS's first strategy was to create online purchasing processes for hospitals, using reverse auctions and other techniques to help

lower costs. MHS developers spent eight months in late 2007 and early 2008 developing such Web-based systems for hospitals. However, the slow acceptance rate of their product during 2008 made MHS's founders go back to the market for additional interviews. After these interviews, MHS's management changed strategy in September 2008 and decided to focus on helping hospitals understand and aggregate their demand better.

In their second round of interviews with buyers, MHS's founders discovered that buying *per se* was not the immediate problem. In order to achieve real savings, hospital buyers must first be able to forecast and aggregate demand from a number of diverse departments and laboratories. If this information could be aggregated somehow, then a comprehensive and longer-term view of demand could be created.

This rapid change in strategy made Willie worry about the stability of MHS. The change also reminded Willie of some material covered in an entrepreneurship class he took with Professor Morphen at Midwest University. The professor pointed out that the short-term cash difficulties small businesses faced (e.g., from lack of demand for their products) sometimes caused managers to make dramatic changes in direction of the firm with little or no notice to employees. Morphen underlined the dangerous implications of this behavior on the ability of the small company to move forward toward its vision consistently. However, Morphen also tried to make sure the students understood the need for small businesses to change and innovate quickly when circumstances required it.

MHS's second software product was delivered to hospitals in very late 2008 and helped the procurement department understand current demand across several departments. This Web-based software tool allowed diverse departments to enter demand for a variety of products and services for the next month. In turn, the centralized purchasing department could use these aggregated figures to obtain the best prices and terms from suppliers. Several upgrades to this product were released over the next several months. Demand for the product started to grow rapidly in mid-2009.

The company had plans to introduce additional improvements in the current software product and to roll out new software tools to facilitate the longer-term forecasting of demand based on historical data and using department input. Details of the software were not yet released by MHS.

Willie's First Interview with MHS

Willie signed up to interview with MHS on campus Friday. He was pleased that Jim Stone was there to do the interviewing. Willie found Stone's description of MHS's software developer job, positioning Willie "closer to the road" and accountable for making a major contribution to an application and a customer, exciting.

After asking Willie about his grades (a 3.52 on a 4.0 scale), his internship experience, and the extra computer science courses he had taken, Stone extended him an invitation for a second interview on Tuesday morning. Willie called Hewlett-Packard to ask if he could postpone his decision to the end of next week. His sponsor was reluctant to agree but eventually replied that they needed to know his decision no later than Wednesday so they could extend the offer to another candidate should Willie decide not to accept. Willie would have little time to make the most important decision of his career. But he had no choice.

The Second Interview with MHS

It took Willie longer than normal to get dressed for Tuesday's interview. He was not sure whether he wanted to wear a full suit or slacks, a button-down and tie. A full suit seemed to be the safest bet. He would make a horrible impression if he did not wear one but was expected to. On the other hand, the button-down and tie seemed to say "confident."

He opted for gray dress pants, a black long-sleeved turtleneck, and a black jacket—kind of a Steve Jobs look. He felt comfortable and well prepared.

When he entered MHS's office, he was surprised. Unlike the huge marble reception area at Hewlett-Packard, there was only a desk, unstaffed, in MHS's entry. Two chairs and a small table with business magazines were off to the side. He was not sure whether he should just start roaming the halls or if he should sit down and hope someone showed up. He sat down.

"Has someone helped you?" Willie looked up and was surprised to see flannel shirt, the interviewer he had run into at the alumni event! "Hi. I'm Joe Dobbins," flannel shirt said as he extended his hand. "I guess we didn't introduce ourselves properly last time we met."

"Willie Stahe," Willie said as he shook hands.

"Have you solved your dilemma over whether or not to go with Hewlett-Packard?" Joe asked.

"Not yet. I'm here for a second interview," Willie said.

"Oh. So we're the cool start-up you want to work for," Joe said.

"I think so," Willie answered. "It's such a huge change from where I thought I'd be and what I thought I'd be doing."

"It's a big decision, a big challenge," Joe said as he sat in the chair next to Willie. "We're only a few years old and have money in the bank to last only through February of next year, assuming the worst case. I'm out raising more equity capital now. Our product is selling but revenue has to

grow substantially if we are to cover our costs. It's a challenge. Tell me, what kinds of challenges have you faced?"

"Getting to college was a big one. My Dad's business was close to filing for bankruptcy my senior year in high school. Not only did I not get to go to prom and stuff like that, but I wasn't sure I would be able to get to college," Willie said.

"That's a big hit for an 18-year-old. How'd you handle it?" Joe asked.

"I wasn't eligible for most of the government programs because need is based on the previous April's tax return, which for us wasn't great, but it was enough to make us ineligible. So I looked at holding off a year and working and saving or trying to get a bank loan and working while going to school. With my Dad's situation, it was unlikely I'd get the bank loan," Willie said.

"So you held back a year?" Joe asked.

"No. Actually, I went into the bank anyway. My Dad and I worked on why we thought his business still had potential and then we laid all the cards out on the table and convinced the bank I'd be a good credit risk," Willie said.

"Seems like that was a creative and effective solution. Wish we could do the same thing in this environment. We have had real problems even getting banks to listen to us," Joe noted.

"Then we met with a financial aid counselor and ended up getting a low interest loan for most of the money," Willie paused, deep in thought. "I think what's more important is that my confidence in my Dad and his business, and working with him to look at the positives when everything seemed doomed really helped him reenergize and get the business back on track. Of course, that helped me as well," Willie said.

"Kind of like not running from the smoke," Joe said.

"Huh?" said Willie.

"It's a saying we have here. Don't run from the smoke. If you see something's wrong, run to it, not away from it," Joe said.

"I guess it was a lot like that," Willie said.

"I see you've met Joe," Stone said as he walked toward them. "You'll be meeting with him later on."

"I don't think that'll be necessary, Jim," Joe said. "He's answered my questions. Willie," he extended his hand, "it was a pleasure talking with you. I hope we have the opportunity to work together sometime."

Willie wished he had been paying more attention to what he had been saying. "Wow. I didn't even know I was being interviewed," he said.

"That's what everyone says after talking with Joe," Stone said. "He pretty much can tell within the first five minutes whether someone will fit with MHS. Looks like you made a favorable impression. About your next interview—normally the founders don't all interview a candidate. But since you've gotten an offer from Hewlett-Packard, I thought you might like to talk with Matt Mahoney."

"He's the one that started out at Hewlett-Packard, isn't he?" Willie said.

"Right. I thought he might be able to answer a lot of your questions," Stone said. "Hey, Matt, this is the Midwest student I was telling you about, Willie Stahe."

"Good to meet you," Matt said as he extended his hand. "Have a seat."

As he sat down, Willie was struck by how neat Matt's office was and how neatly he was dressed. Matt had a soft voice and disarming smile, and Willie immediately felt comfortable.

"Jim tells me you're interested in working with us, but that you've also gotten an offer from Hewlett-Packard," Matt said.

"I'm really torn. It's like a dream come true to be offered the chance to work for Hewlett-Packard. Move out to the West Coast. I haven't even told my family that I'm interviewing with you. I don't think they would understand," Willie said.

"What don't you think they would understand?" Matt asked.

"That I'd be turning down big bucks for incredibly smaller bucks that may or may not turn into big bucks," Willie said.

"Considering you wouldn't be living on the West Coast, I think you'll find our salary is pretty competitive. And predicting future big bucks is largely dependent on each of us who work here and how much you believe in our vision and business model," Matt said. "Disregarding salary, which job would you take?"

"Hmm—that is a tough question. I think that I would take this job," Willie said.

"Why?" Matt asked.

"Because what I'd be doing would matter, would have a significant impact. I could be part of something new that will be the leader in the industry, first in health care and then in others after that. Maybe I'd be on the ground floor of the next Microsoft, or the next Hewlett-Packard," Willie said. "You worked at Hewlett-Packard. Why did you leave?"

"In a large corporation, if you want experience with other perspectives, you pretty much have to displace someone else. And the higher up you go, the more difficult it is to get different experiences," Matt said. He added, "With a start-up like MHS, everyone will share in the company's good fortune and can take on additional responsibility as we grow. There's always an opportunity to expand your set of experiences."

"How come you chose to start MHS after you left IBM rather than take a position with another established company?" Willie asked.

"All the other opportunities I looked at were all start-ups. I'm interested in making an impact, in creating something. To me, that's where the challenge, and the excitement, lies," Matt said. "Plus, our business is still evolving. It's exciting working in a dynamic environment. Although Hewlett-Packard changes, it's incremental change. They know their products and their markets well. Have you looked at working for other start-ups?"

"No. This is the only one. I fully intended to work for Hewlett-Packard. It's a goal I've had for over a year, and I was pretty focused on attaining it," Willie said.

"Then I guess you have a big decision to make," Matt said.

"I do," Willie said sadly. "Thanks for meeting with me."

"Good luck," Matt said as he shook hands with Willie.

"What did you think?" Stone asked Matt.

"The main question for Willie isn't whether he wants to work with us. I think it's whether he wants to say no to Hewlett-Packard," Matt said.

Willie met with a few other software developers and the chief architect. He really liked the software design tools and the design of MHS's second product offering. But it was all over in two hours. During the exit interview, Stone offered him a software developer job to start in January at an annual salary that was $6,000 less than the one from Hewlett-Packard, but with comparable benefits. He then showed him the space on the floor where his new cubicle would be constructed.

Decision Time

As Willie left the building, he was torn. He secretly had hoped he would not like someone—anyone—at MHS. But he found that not only did he like everyone he met, he felt stimulated by their enthusiasm and energy.

He could work for Hewlett-Packard for a few years and then leave to work for a start-up, or maybe start his own company. But, if that was really what he wanted to do in a few years, then why not do it now while there was an opportunity? But how could he say no to Hewlett-Packard? That was a prestigious opportunity that would open many doors. Just working for them would establish his credibility.

But there was definitely reason to be concerned about this employment option. The changes and uncertainty at HP caused him to worry a little about what might happen if he was to join that firm.

Regardless, if Willie chose Hewlett-Packard for employment, he was very unsure of how long he would stay. He had heard from friends at Midwest University who used to work for large software companies that outsourcing the development function to other countries was always possible.

However, he still questioned whether he should accept the offer at MHS. As he had found in his search for information on the health care software industry over the weekend, many of the smaller companies were showing signs of rapid future change because of a more demanding competitive environment. How would MHS's management team keep the direction of the company focused, but still give employees the sense of ownership they wanted? If the company began to have more serious financial troubles, would Willie be asked to leave quickly?

Again, he headed for the library instead of the gym. He needed to review his notes from the two-day interview at HP and the visit to MHS. He also needed to make a list of pros and cons for working for Hewlett-Packard versus working for MHS. Then he would talk to some friends. Once he had the options clearer, he knew they would help him make the final decision. He had to give Hewlett-Packard his answer tomorrow.