# Chapter 9

# Information Systems Controls for Systems Reliability—Part 2: Confidentiality and Privacy

## Learning Objectives

After studying this chapter, you should be able to:

1. Identify and explain controls designed to protect the confidentiality of sensitive corporate information.
2. Identify and explain controls designed to protect the privacy of customers' personal information.
3. Explain how the two basic types of encryption systems work.

**INTEGRATIVE CASE NORTHWEST INDUSTRIES**

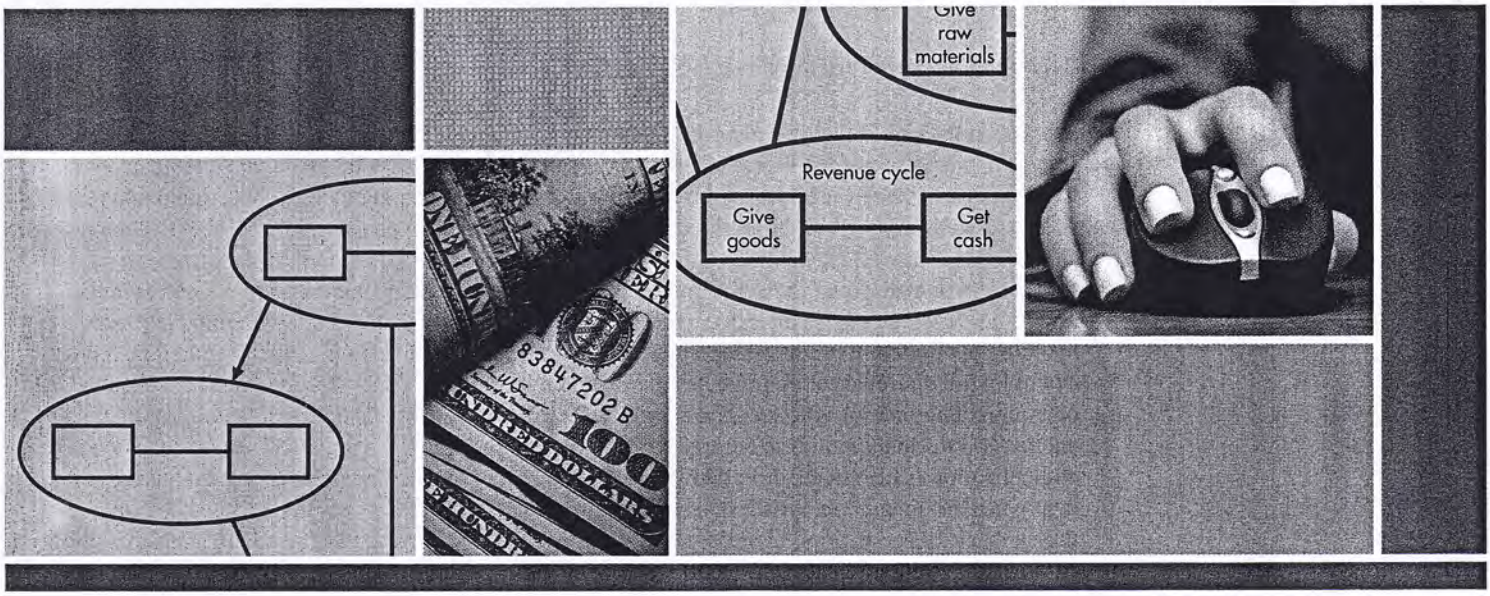
Jason Scott was preparing for his meeting with the company's chief information security officer (CISO). Although Jason was satisfied that Northwest Industries' computer security policies and procedures provided the company with adequate protection against intrusions, he was concerned about other aspects of systems reliability. In particular, he wanted to learn what Northwest Industries was doing to address the following issues:

1. Protecting the confidentiality of sensitive corporate information, such as marketing plans and trade secrets
2. Protecting the privacy of personal information collected from customers

Jason planned to use his interview with the CISO to obtain a general understanding of the company's information systems controls. He then planned to follow up by collecting evidence about the effectiveness of those controls.

## Introduction

Chapter 8 discussed information security, which is the fundamental principle of systems reliability. This chapter covers two other important principles of reliable systems in the Trust Services Framework: preserving the confidentiality of an organization's intellectual property and protecting




the privacy of personal information it collects from customers. We also discuss the topic of encryption in detail, because it is a critical tool to protecting both confidentiality and privacy.

## Preserving Confidentiality

Organizations possess a myriad of sensitive information, including strategic plans, trade secrets, cost information, legal documents, and process improvements. This intellectual property often is crucial to the organization's long-run competitive advantage and success. Consequently, preserving the confidentiality of the organization's intellectual property, and similar information shared by its business partners, has long been recognized as a basic objective of information security. This section discusses the actions that must be taken to preserve confidentiality: (1) identification and classification of the information to be protected, (2) encryption of sensitive information, (3) controlling access to sensitive information, and (4) training.

### Identification and Classification of Information to be Protected

The first step to protect the confidentiality of intellectual property and other sensitive business information is to identify where such information resides and who has access to it. This sounds easy, but undertaking a thorough inventory of every digital and paper store of information is both time-consuming and costly because it involves examining more than just the contents of the organization's financial systems. For example, manufacturing firms typically employ large-scale factory automation. Those systems contain instructions that may provide significant cost advantages or product quality enhancements over those of competitors and, therefore, must be protected from unauthorized disclosure or tampering.

After the information that needs to be protected has been identified, the next step, as discussed in the Control Objectives for Information and Related Technology (COBIT) control objective PO 2.3, is to classify the information in terms of its value to the organization. Information classification is not a task to be delegated solely to information systems professionals; to properly recognize the information's value, the process also needs input from senior management. Once the information has been classified, the appropriate set of controls can be deployed to protect it.

### Protecting Confidentiality with Encryption

Encryption (to be discussed later in this chapter) is an extremely important and effective tool to protect confidentiality. It is the only way to protect information in transit over the Internet. It is also a necessary part of defense-in-depth to protect information stored on Web sites or in a public cloud. For example, many accounting firms have created secure portals that they use to share sensitive audit, tax, or consulting information with clients. The security of such portals, however, is limited by the strength of the authentication methods used to restrict access. In most cases, this

involves only single factor authentication via a password. Encrypting the client's data that is stored on the portal provides an additional layer of protection in the event of unauthorized access to the portal. Similarly, encrypting information stored in a public cloud protects it from unauthorized access by employees of the cloud service provider or by anyone else who is using that same cloud.

Encryption, however, is not a panacea. Some sensitive information, particularly "know-how" such as process shortcuts, may not be stored digitally and, therefore, cannot be protected by being encrypted. In addition, encryption protects information only in specific situations. For example, full disk encryption protects the information stored on a laptop in the event that it is lost or stolen. The person who steals or finds such a laptop will not be able to read any of the encrypted information, *unless* he or she can log on as the legitimate owner. That is why strong authentication is also needed. In addition, the information on the laptop is decrypted whenever the owner has logged on, which means that anyone who can sit down at the keyboard can view the sensitive information. Therefore, physical access controls are also needed. Similarly, in enterprise systems, encrypting information while it is stored in the database protects it from being viewed by people who have access to the system but not to the database. However, the database has to decrypt the information in order to process it; therefore, anyone who can log on to the database can potentially see confidential information. That is why strong access controls are also needed. In summary, sensitive information is exposed in plain view whenever it is being processed by a program, displayed on a monitor, or included in printed reports. Consequently, protecting confidentiality requires application of the principle of defense-in-depth: supplementing encryption with access controls and training.

## Controlling Access to Sensitive Information

Chapter 8 discussed how organizations use authentication and authorization controls to restrict access to information systems that contain sensitive information. ***Information rights management (IRM)*** software provides an additional layer of protection to specific information resources, offering the capability not only to limit access to specific files or documents, but also to specify the actions (read, copy, print, download to USB devices, etc.) that individuals who are granted access to that resource can perform. Some IRM software even has the capability to limit those privileges to a specific period of time and to remotely erase protected files. Either the creator of the information or the person responsible for managing it must assign the access rights. To access an IRM-protected resource, a person must first authenticate to the IRM server, which then downloads code containing the access-limiting instructions to that person's computer.

COBIT control objectives DS 12.2 and DS 12.3 address physical access controls, which are also important in preventing someone with unsupervised access from quickly downloading and copying gigabytes of confidential information onto a USB drive, an iPod, a cell phone, or other portable device. It is especially important to restrict access to rooms that contain printers, digital copiers, and fax machines because such devices typically possess large amounts of RAM, which may store any confidential information that was printed. Laptops and workstations should run password-protected screen savers automatically after a few minutes of inactivity, to prevent unauthorized viewing of sensitive information. Screen protection devices that limit the distance and angle from which information on a laptop or workstation monitor can be seen are also useful.

In addition, COBIT control objective DS 11.4 addresses the importance of controlling the *disposal* of information resources. Printed reports and microfilm containing confidential information should be shredded before being thrown out. Special procedures are needed to destroy information stored on magnetic and optical media. Using built-in operating system commands to delete that information is insufficient, because many utility programs exist that can recover such deleted files. Frequently, people who have purchased used computers, cell phones, digital copy machines, and other devices discover information that the previous owner thought had been deleted. Proper disposal of computer media requires use of special software designed to "wipe" the media clean by repeatedly overwriting the disk or drive with random patterns of data. Probably the safest alternative is to physically destroy (e.g., by incineration) magnetic and optical media that have been used to store extremely sensitive data.

Today, organizations constantly exchange information with their business partners and customers. Therefore, protecting confidentiality also requires controls over outbound communications. One tool for accomplishing that is ***data loss prevention (DLP)*** software, which works like

antivirus programs in reverse, blocking outgoing messages (whether e-mail, IM, or other means) that contain key words or phrases associated with the intellectual property or other sensitive data the organization wants to protect. DLP software is a preventive control. It can and should be supplemented by embedding code called a ***digital watermark*** in documents. The digital watermark is a detective control that enables an organization to identify confidential information that has been disclosed. When an organization discovers documents containing its digital watermark on the Internet, it has evidence that the preventive controls designed to protect its sensitive information have failed. It should then investigate how the compromise occurred and take appropriate corrective action.

Access controls designed to protect confidentiality must be continuously reviewed and modified to respond to new threats created by technological advances. For example, the incorporation of digital cameras in cell phones makes it possible for visitors to surreptitiously capture confidential information. Consequently, many organizations now prohibit visitors from using cell phones while touring manufacturing facilities or other areas likely to contain confidential information. Because camera phones are so easy to hide, most organizations also require that visitors always be escorted by employees to further reduce the risk that the visitors photograph sensitive information.

Telephone conversations are another area affected by advances in technology. In the past, wiretaps were the only serious threat to the confidentiality of telephone conversations, and the difficulty of setting them up meant that the risk of that threat was relatively low. The use of voice-over-the-Internet (VoIP), however, means that telephone conversations are now routed as packets over the Internet. This means that VoIP telephone conversations are as vulnerable to interception as any other information sent over the Internet. Therefore, VoIP conversations about sensitive topics should be encrypted.

Virtualization and cloud computing also affect the risk of unauthorized access to sensitive or confidential information. An important control in virtual environments, including internally managed "private" clouds, is to use virtual firewalls to restrict access between different virtual machines that coexist on the same physical server. In addition, virtual machines that store highly sensitive or confidential data should not be hosted on the same physical server with virtual machines that are accessible via the Internet because of the risk that a skilled attacker might be able to break out of the latter and compromise the former. With public clouds, the data is stored elsewhere, and access occurs over the Internet via browsers. Therefore, all communication between users and the cloud must be encrypted. Browser software, however, often contains numerous vulnerabilities. Consequently, highly sensitive and confidential data probably should not be stored in a public cloud because of lack of control over where that information is actually stored and because of the risk of unauthorized access by other cloud customers, who may include competitors, or even by employees of the cloud provider.



## Training

Training is arguably the most important control for protecting confidentiality. Employees need to know what information they can share with outsiders and what information needs to be protected. They also need to be taught how to protect confidential data. For example, employees need to know how to use encryption software. They also need to learn to always log out of applications before leaving their laptop or workstation unattended, to prevent other employees from obtaining unauthorized access to that information. Employees also need to know how to code reports they create to reflect the importance of the information contained therein so that other employees will know how to handle those reports. They also need to be taught not to leave reports containing sensitive information in plain view on their desks when they leave.

Training is particularly important concerning the proper use of e-mail, instant messaging (chat), and blogs because it is impossible to control the subsequent distribution of information once it has been sent or posted through any of those methods. For example, it is important to teach employees not to routinely use the "reply all" option with e-mail because doing so may disclose sensitive information to people who should not see it. Employees also need to be taught how to participate in discussions at conferences or professional education courses so that they do not inadvertently disclose information that might compromise their employer's competitive advantage. Employees often do not realize the importance of information they possess, such as time-saving steps or undocumented features they have discovered when using a particular

software program. Therefore, it is important for management to inform employees who will attend external training courses, trade shows, or conferences whether they can discuss such information or whether it should be protected because it provides the company a cost savings or quality improvement advantage over its competitors.

With proper training, employees can play an important role in protecting the confidentiality of an organization's information and enhance the effectiveness of related controls. For example, if employees understand their organization's data classification scheme, they may recognize situations in which sensitive information has not been properly protected and proactively take appropriate corrective actions. Training in how to protect the confidentiality of an organization's intellectual property can also enhance its efforts to protect the privacy of personal information it collects from its customers.

## Privacy

The Trust Services framework privacy principle is closely related to the confidentiality principle, differing primarily in that it focuses on protecting personal information about customers rather than organizational data. Consequently, the controls that need to be implemented to protect privacy are the same ones used to protect confidentiality: identification of the information that needs to be protected, encryption, access controls, and training.

### Privacy Controls

As is the case for confidential information, the first step to protect the privacy of personal information collected from customers is to identify what information is collected, where it is stored, and who has access to it. It is then important to implement controls to protect that information because incidents involving the unauthorized disclosure of customers' personal information, whether intentional or accidental, can be costly. For example, the Massachusetts Data Security Law (201 CMR 17.00) fines companies $5,000 per record for data breaches. Governments may also restrict the daily business operations of companies that suffer a breach. For example, after Citibank's online credit card application in Taiwan was hacked and personal customer data compromised in November 2003, the Taiwanese government imposed a one-month moratorium on issuing new credit cards and a three-month suspension of the online application, until Citibank's online security could be independently verified.

Encryption is a fundamental control for protecting the privacy of personal information that organizations collect from their customers. That information needs to be encrypted both while it is in transit over the Internet and while it is in storage (indeed, the Massachusetts law mandates encryption of personal information at all times, whether in transit or in storage). Encrypting customers' personal information not only protects it from unauthorized disclosure, but also can save organizations money. Many states have passed data breach notification laws that require organizations to notify customers after any event, such as the loss or theft of a laptop or portable media device, that may have resulted in the unauthorized disclosure of customer personal information. This can be expensive for businesses that have hundreds of thousands or millions of customers. The costly notification requirement is usually waived, however, if the lost or stolen customer information was encrypted.

However, customers' personal information is not encrypted during processing or when it is displayed either on a monitor or in a printed report. Consequently, as with confidentiality, protecting customers' privacy requires supplementing encryption with access controls and training. Strong authentication and authorization controls restrict who can access systems that contain customers' personal information and the actions the users can perform once they are granted access. It is especially important to prevent programmers from having access to personal information, such as credit card numbers, telephone numbers, and Social Security numbers. In developing new applications, programmers often have to use "realistic" data to test the new system. It is tempting, and easy, to provide them with a copy of the data in the organization's transaction processing system. Doing so, however, gives programmers access to customers' personal information. To protect privacy, organizations should run ***data masking*** programs that replace

customers' personal information with fake values (e.g., replace a real Social Security number with a different set of numbers that have the same characteristics, such as 123-45-6789) before sending that data to the program development and testing system.

Organizations also need to train employees on how to manage and protect personal information collected from customers. This is especially important for medical and financial information. Obviously, intentional misuse of such information can have serious negative economic consequences, including significant declines in stock prices. Unintentional disclosure of such personal information can also create costly problems, however. For example, someone denied health or life insurance because of improper disclosure of personal information is likely to sue the organization that was supposed to restrict access to that data.

## Privacy Concerns

Two major privacy-related concerns are spam and identity theft.

**SPAM** *Spam* is unsolicited e-mail that contains either advertising or offensive content. Spam is a privacy-related issue because recipients are often targeted as a result of unauthorized access to e-mail address lists and databases containing personal information. The volume of spam is overwhelming many e-mail systems. Spam not only reduces the efficiency benefits of e-mail but also is a source of many viruses, worms, spyware programs, and other types of malware. To deal with this problem, the U.S. Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act in 2003. CAN-SPAM provides both criminal and civil penalties for violations of the law. CAN-SPAM applies to commercial e-mail, which is defined as any e-mail that has the primary purpose of advertising or promotion. This covers much of the legitimate e-mail that many organizations send to their customers, suppliers, and, in the case of nonprofit organizations, their donors. Thus, organizations need to be sure to follow CAN-SPAM's guidelines or risk sanctions. Key provisions include the following:

- The sender's identity must be clearly displayed in the header of the message.
- The subject field in the header must clearly identify the message as an advertisement or solicitation.
- The body of the message must provide recipients with a working link that can be used to opt out of future e-mail. After receiving an opt-out request, organizations have 10 days to implement steps to ensure they do not send any additional unsolicited e-mail to that address. This means that organizations need to assign someone responsibility for processing opt-out requests.
- The body of the message must include the sender's valid postal address. Although not required, best practice would be to also include full street address, telephone, and fax numbers.
- Organizations should not send commercial e-mail to randomly generated addresses, nor should they set up Web sites designed to "harvest" e-mail addresses of potential customers. Experts recommend that organizations redesign their own Web sites to include a visible means for visitors to opt in to receive e-mail, such as checking a box.

**IDENTITY THEFT** Another privacy-related issue that is of growing concern is identity theft. ***Identity theft*** is the unauthorized use of someone's personal information for the perpetrator's benefit. Often, identity theft is a financial crime, in which the perpetrator obtains loans or opens new credit cards in the victim's name and sometimes loots the victim's bank accounts. However, a growing portion of identity theft cases involve fraudulently obtaining medical care and services. Medical identity theft can have life-threatening consequences because of errors it may create in the victim's medical records, such as changing information about drug allergies or prescriptions. It may even cause victims to lose their insurance coverage if the thief has used up their annual or lifetime cap for coverage of a specific illness.

Focus 9-1 discusses the steps that individuals should take to minimize the risk of identity theft. Organizations, however, also have a role to play in preventing identity theft. Customers entrust them with personal information. Organizations economically benefit from having access to that information. Therefore, organizations have an ethical and moral obligation to implement controls to protect the personal information that they collect from and about their customers.

## FOCUS 9-1 Protecting Yourself from Identity Theft

Victims of identity theft often spend much time and money to recover from it. Fortunately, there are a number of simple steps you can take to minimize your risk of becoming a victim of identity theft.

- Shred all documents that contain personal information, especially unsolicited credit card offers, before discarding them. Cross-cut shredders are much more effective than strip-cut shredders.
- Never send personal information (Social Security number, passport number, etc.) in unencrypted e-mail.
- Beware of e-mail, telephone, and print requests to "verify" personal information that the requesting party should already possess. For example, credit card companies will never need to ask you for the three- or four-digit security code on your card. Similarly, the IRS will never e-mail you asking you to send personally identifying information in response to an audit.
- Do not carry your Social Security card with you. Be wary of requests to reveal the last four digits of your Social Security number. The first three and middle two digits are assigned based on the location and date you applied for a Social Security number and, therefore, can be discovered through research, but the last four digits are assigned randomly.
- Print only your initials and last name, rather than your full name, on checks. This prevents a thief from knowing how you sign your name.
- Limit the amount of other information (address and phone number) preprinted on checks, and consider totally eliminating such information.
- Do not place outgoing mail containing checks or personal information in your mailbox for pickup.
- Do not carry more than a few blank checks with you.
- Use special software to thoroughly clean any digital media prior to disposal, or physically destroy the media. It is especially important to thoroughly erase or destroy hard drives (for computers, printers, *and* copy machines) prior to donating or disposing of obsolete equipment because they likely contain information about online financial transactions.
- Monitor your credit reports regularly.
- File a police report as soon as you discover that your purse or wallet was lost or stolen.
- Make photocopies of driver's licenses, passports, and credit cards. Store this information, along with the telephone numbers of all your credit cards, in a safe location to facilitate notifying appropriate authorities in the case that those documents are lost or stolen.
- Immediately cancel any stolen or lost credit cards.

### Privacy Regulations and Generally Accepted Privacy Principles

Concerns about spam, identity theft, and protecting individual privacy have resulted in numerous government regulations. In addition to state disclosure laws, a number of federal regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Financial Services Modernization Act (commonly referred to as the Gramm–Leach–Bliley Act, representing the names of its three Congressional sponsors), impose specific requirements on organizations to protect the privacy of their customers' personal information. Many other countries also have regulations concerning the use and protection of customers' personal information.

To help organizations cost-effectively comply with these myriad requirements, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) jointly developed a framework called *Generally Accepted Privacy Principles (GAPP)*. GAPP identifies and defines the following 10 internationally recognized best practices for protecting the privacy of customers' personal information:

1. *Management.* Organizations need to establish a set of procedures and policies for protecting the privacy of personal information they collect from customers, as well as information about their customers obtained from third parties such as credit bureaus. They should assign responsibility and accountability for implementing those policies and procedures to a specific person or group of employees.
2. *Notice.* An organization should provide notice about its privacy policies and practices at or before the time it collects personal information from customers, or as soon as practicable thereafter. The notice should clearly explain what information is being collected, the reasons for its collection, and how the information will be used.
3. *Choice and consent.* Organizations should explain the choices available to individuals and obtain their consent prior to the collection and use of their personal information. The

nature of the choices offered differs across countries. In the United States, the default policy is called opt-out, which allows organizations to collect personal information about customers unless the customer explicitly objects. In contrast, the default policy in Europe is opt-in, meaning that organizations cannot collect personally identifying information unless customers explicitly give them permission to do so. However, even in the United States, GAPP recommends that organizations follow the opt-in approach and obtain explicit positive consent prior to collecting and storing sensitive personal information, such as financial or health records, political opinions, religious beliefs, and prior criminal history.

4. *Collection.* An organization should collect only the information needed to fulfill the purposes stated in its privacy policies. One particular issue of concern is the use of cookies on Web sites. A ***cookie*** is a text file created by a Web site and stored on a visitor's hard disk. Cookies store information about what the user has done on the site. Most Web sites create multiple cookies per visit in order to make it easier for visitors to navigate to relevant portions of the Web site. It is important to note that cookies are text files, which means that they cannot "do" anything besides store information. They do, however, contain personal information that may increase the risk of identity theft and other privacy threats. Browsers can be configured to not accept cookies, and GAPP recommends that organizations employ procedures to accede to such requests and not surreptitiously use cookies.
5. *Use and retention.* Organizations should use customers' personal information only in the manner described in their stated privacy policies and retain that information only as long as it is needed to fulfill a legitimate business purpose. This means that organizations need to create retention policies and assign someone responsibility for ensuring compliance with those policies.
6. *Access.* An organization should provide individuals with the ability to access, review, correct, and delete the personal information stored about them.
7. *Disclosure to third parties.* Organizations should disclose their customers' personal information to third parties only in the situations and manners described in the organization's privacy policies and only to third parties who provide the same level of privacy protection as does the organization which initially collected the information. This principle has implications for using cloud computing, because storing customers' personal information in the cloud may make it accessible to the cloud provider's employees; hence such information should be encrypted at all times.
8. *Security.* An organization must take reasonable steps to protect its customers' personal information from loss or unauthorized disclosure. Indeed, it is not possible to protect privacy without adequate information security. Therefore, organizations must use the various preventive, detective, and corrective controls discussed in Chapter 8 to restrict access to their customers' personal information. However, achieving an acceptable level of information security is not sufficient to protect privacy. It is also necessary to train employees to avoid practices that can result in the unintentional or inadvertent breach of privacy. One sometimes overlooked issue concerns the disposal of computer equipment. It is important to follow the suggestions presented in the section on protecting confidentiality for properly erasing all information stored on computer media. Perhaps one of the most famous incidents of failing to properly erase information on a hard drive involved the disposal of an obsolete personal computer by a British bank. It was sold at an auction; the buyer found that it contained personal information about the financial affairs of Paul McCartney. E-mail presents a second threat vector to consider. For example, in 2002 drug manufacturer Eli Lilly sent an e-mail about its antidepressant drug Prozac to 669 patients. However, because it used the cc: function to send the message to all patients, the e-mails revealed the identities of other patients. A third often overlooked area concerns the release of electronic documents. Just as special procedures are used to black out (redact) personal information on paper documents, organizations should train employees to use procedures to remove such information on electronic documents in a manner that prevents the recipient of the document from recovering the redacted information.
9. *Quality.* Organizations should maintain the integrity of their customers' personal information and employ procedures to ensure that it is reasonably accurate. Providing customers with a way to review the personal information stored by the organization (GAPP principle 6) can be a cost-effective way to achieve this objective.

10. *Monitoring and enforcement.* An organization should assign one or more employees to be responsible for ensuring compliance with its stated privacy policies. Organizations must also periodically verify that their employees are complying with stated privacy policies. In addition, organizations should establish procedures for responding to customer complaints, including the use of a third-party dispute resolution process.

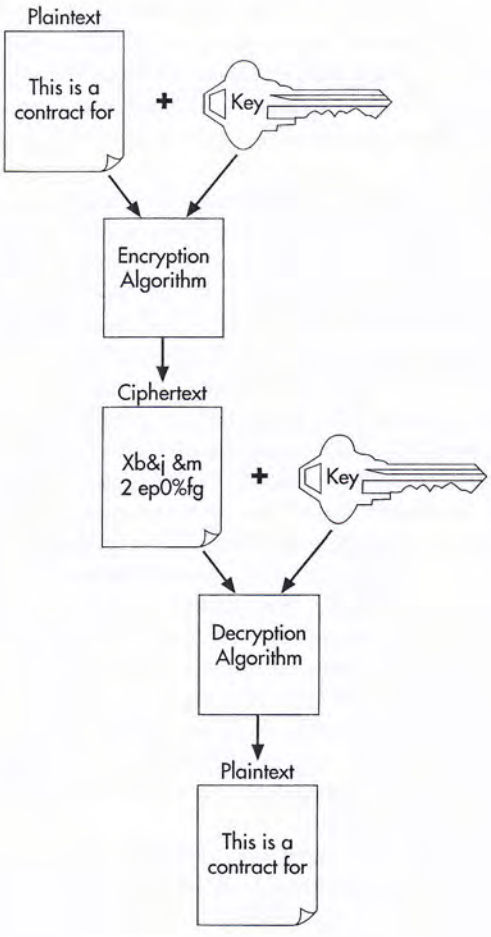
In summary, GAPP shows that protecting the privacy of customers' personal information requires first implementing a combination of policies, procedures, and technology, then training everyone in the organization to act in accordance with those plans, and subsequently monitoring compliance. Only senior management possesses the authority and the resources to accomplish this, which reinforces the fact that all aspects of systems reliability are, at bottom, a managerial issue and not just an IT issue. Because accountants and auditors serve as trusted advisors to senior management, they too need to be knowledgeable about these issues.

## Encryption

Encryption is a preventive control that can be used to protect both confidentiality and privacy. Encryption protects data that is being sent over the Internet and it provides one last barrier that must be overcome by an intruder who has obtained unauthorized access to stored information. As we will see later, encryption also strengthens authentication procedures and plays an essential role in ensuring and verifying the validity of e-business transactions. Therefore, it is important for accountants, auditors, and systems professionals to understand encryption.

As shown in Figure 9-1, ***encryption*** is the process of transforming normal content, called ***plaintext,*** into unreadable gibberish, called ***ciphertext. Decryption*** reverses this process,

**FIGURE 9-1**
**Steps in the Encryption and Decryption Process**



transforming ciphertext back into plaintext. Both encryption and decryption involve use of a key and an algorithm. Computers represent both plaintext and ciphertext as a series of binary digits (0s and 1s). The key is also a string of binary digits of a fixed length; for example, a 128-bit key consists of a string of 128 0s and 1s. The algorithm is a formula for combining the key and the text. Most documents are longer than the key, so the encryption process begins by dividing the plaintext into blocks, each block being of equal length to the key. Then the algorithm is applied to the key and the block of plaintext. For example, if a 128-bit key is being used, the computer first divides the document or file into 128-bit-long blocks and then combines each block with the key in the manner specified by the algorithm (for example, by adding them). The result is a ciphertext version of the document or file, equal in size to the original. To reproduce the original document, the computer first divides the ciphertext into 128-bit blocks and then applies the decryption key to each block.

## Factors that Influence Encryption Strength

Three important factors determine the strength of any encryption system: (1) key length, (2) encryption algorithm, and (3) policies for managing the cryptographic keys.

**KEY LENGTH** Longer keys provide stronger encryption by reducing the number of repeating blocks in the ciphertext. This makes it harder to spot patterns in the ciphertext that reflect patterns in the original plaintext. For example, a 24-bit key encrypts plaintext in blocks of 24 bits. In English, each letter is represented by 8 bits. Thus, a 24-bit key encrypts English plaintext in chunks of three letters. This makes it easy to use information about relative word frequencies, such as the fact that *the* is one of the most common three-letter words in English, to "guess" that the most commonly recurring pattern of 24 bits in the ciphertext probably represents the English word *the* and proceed to "break" the encryption. That's why most encryption keys are at least 256 bits long (corresponding to 42 English letters), and are often 1024 bits or longer.

**ENCRYPTION ALGORITHM** The nature of the algorithm used to combine the key and the plaintext is important. A strong algorithm is difficult, if not impossible, to break by using brute-force guessing techniques. Secrecy is not necessary for strength. Indeed, the procedures used by the most accepted and widely used encryption algorithms are publicly available. Their strength is due not to the secrecy of their procedures, but to the fact that they have been rigorously tested and demonstrated to resist brute-force guessing attacks. Therefore, organizations should not attempt to create their own "secret" encryption algorithm, but instead should purchase products that use widely accepted standard algorithms whose strength has been proven.

**POLICIES FOR MANAGING CRYPTOGRAPHIC KEYS** COBIT control objective DS 5.8 stresses the importance of sound practices for managing cryptographic keys. Indeed, this is often the most vulnerable aspect of encryption systems. No matter how long the keys are, or how strong an encryption algorithm is, if the keys have been compromised, the encryption can be easily broken. Therefore, cryptographic keys must be stored securely and protected with strong access controls. Best practices include not storing cryptographic keys in a browser or any other file that other users of that system can readily access and using a strong (and long) passphrase to protect the keys.

Organizations must also have a way to decrypt the data in the event that the employee who encrypted it is no longer present. One way to do this is to use encryption software that creates a built-in master key that can be used to decrypt anything encrypted by that software. An alternative is a process called ***key escrow,*** which involves making copies of all encryption keys used by employees and storing those copies securely. Organizations also need sound policies and procedures for issuing and revoking keys. Keys should be issued only to employees who handle sensitive data and, therefore, need the ability to encrypt it. It is also important to promptly revoke (cancel) keys when an employee leaves or when there is reason to believe the key has been compromised and to notify everyone who has relied upon those keys that they are no longer valid.

## Types of Encryption Systems

There are two basic types of encryption systems. ***Symmetric encryption systems*** use the same key both to encrypt and to decrypt. DES and AES are examples of symmetric encryption systems. ***Asymmetric encryption systems*** use two keys. One key, called the ***public key,*** is widely

distributed and available to everyone; the other, called the ***private key,*** is kept secret and known only to the owner of that pair of keys. Either the public or private key can be used to encrypt, but only the other key can decrypt the ciphertext. RSA and PGP are examples of asymmetric encryption systems.

Symmetric encryption is much faster than asymmetric encryption, but it has two major problems. First, both parties (sender and receiver) need to know the shared secret key. This means that the two parties need to have some method for securely exchanging the key that will be used to both encrypt and decrypt. E-mail is not a solution, because anyone who can intercept the e-mail would know the secret key. Thus, some other method of exchanging keys is needed. Although this could be done by telephone, postal mail, or private delivery services, such techniques quickly become cost-prohibitive, particularly for global communications. The second problem is that a separate secret key needs to be created for use by each party with whom the use of encryption is desired. For example, if company A wants to encrypt information it shares with companies B and C, but prevent B and C from having access to the other's information, it needs to create two encryption keys, one for use with company B and the other for use with company C. Otherwise, if Company A shared only one common secret key with both B and C, either company could decrypt any information to which it obtained access, even if intended for the other company. Thus, secure management of keys quickly becomes more complex as the number of participants in a symmetric encryption system increases.

Asymmetric encryption systems solve these problems. It does not matter who knows the public key, because any text encrypted with it can be decrypted only by using the corresponding private key. Therefore, the public key can be distributed by e-mail or even be posted on a Web site so that anyone who wants to can send encrypted information to the owner of that public key. Also, any number of parties can use the same public key to send encrypted messages because only the owner of the corresponding private key can decrypt the messages. In addition, information can be encrypted with the private key and then decrypted with the corresponding public key. Since only one party possesses the private key, asymmetric encryption systems make it possible to prove who created a document, thereby providing a means for creating legally binding electronic agreements.

The main drawback to asymmetric encryption systems is speed. Asymmetric encryption is much (thousands of times) slower than symmetric encryption, making it impractical for use to exchange large amounts of data over the Internet. Consequently, e-business uses both types of encryption systems. Symmetric encryption is used to encode most of the data being exchanged, and asymmetric encryption is used to safely send the symmetric key to the recipient for use in decrypting the ciphertext. In addition, as will be discussed later, asymmetric encryption is also used in combination with a process called hashing to create digital signatures.

## Hashing

*Hashing* is a process that takes plaintext of any length and transforms it into a short code called a ***hash***. For example, the SHA-256 algorithm creates a 256-bit hash, regardless of the size of the original plaintext. As Table 9-1 shows, hashing differs from encryption in two important aspects. First, encryption always produces ciphertext similar in length to the original plaintext, but hashing always produces a hash that is of a fixed short length, regardless of the length of the original

**TABLE 9-1 Comparison of Hashing and Encryption**

| Hashing | Encryption |
|---|---|
| 1. One-way function (cannot reverse, or "unhash"). | 1. Reversible (can decrypt back to plaintext). |
| 2. Any size input yields same fixed-size output. For example, SHA-256 hashing algorithm produces a 256-bit hash for each of the following:<br>+ a one-sentence document<br>+ a one-page document<br>+ a ten-page document | 2. Output size approximately the same as input size. For example:<br>+ a one-sentence document becomes a one-sentence encrypted document<br>+ a one-page document becomes a one-page encrypted document<br>+ a ten-page document becomes a ten-page encrypted document |

plaintext. The second difference is that encryption is reversible, but hashing is not. Given the decryption key and the algorithm, ciphertext can be decrypted back into the original plaintext. In contrast, it is not possible to transform a hash back into the original plaintext, because hashing throws away information. For example, using SHA-256 to hash a 10,000-character document produces a string of 256 bits. There is no way to recover the 79,744 bits that were discarded and convert the short 256-bit hash back into the original document.

Hashing algorithms have another interesting property: They use every bit in the original plaintext to calculate the hash value. Therefore, changing any character in the document being hashed, such as replacing a 1 with a 7, adding or removing a single space, or even switching from upper- to lowercase produces a different hash value. This property of hashing algorithms provides a means to verify that the contents of a message have not been altered.

## Digital Signatures

An important issue for business transactions has always been ***nonrepudiation,*** or how to create legally binding agreements that cannot be unilaterally repudiated by either party. Traditionally, this has been accomplished by signing contracts and other documents and then making photocopies so that each party can retain an identical copy. Today, however, many business transactions occur digitally using the Internet. How can businesses obtain the same level of assurance about the enforceability of a digital transaction that a signed original or photocopy provides for a paper-based transaction? The answer is to use both hashing and asymmetric encryption to create a digital signature.

As Figure 9-2 shows, a ***digital signature*** is a hash of a document (or file) that is encrypted using the document creator's private key. Digital signatures provide proof about two important issues: (1) that a copy of a document or file has not been altered, and (2) who created the original version of a digital document or file. Thus, digital signatures provide assurance that someone cannot enter into a digital transaction and then subsequently deny they had done so and refuse to fulfill their side of the contract.

How do digital signatures provide this assurance? First, remember that an important property of a hash is that it reflects every bit in a document. Therefore, if two hashes are identical, it means that two documents or files are identical. Consequently, just as a photocopy can be compared to an original to verify that it has not been altered, comparing a hash of a document on one computer to a hash of a document on another computer provides a way to determine whether two documents are identical. Second, remember that in asymmetric encryption systems, something encrypted with a private key can only be decrypted with the corresponding public key. Therefore, if something can be decrypted with an entity's public key, it must have been encrypted with the corresponding private key, which proves that it had to have been encrypted by the owner of that pair of public and private keys.

Let us now see how both of these facts work together to provide nonrepudiation. For example, a supplier receives a purchase order along with a digital signature of that purchase order from a customer. The supplier can hash its copy of the purchase order using the same hashing algorithm that the customer used to create its digital signature. The supplier can then use the customer's public key to decrypt the digital signature, thereby producing a hash of some document that must have existed in the customer's information system. If the hash resulting from decrypting the customer's digital signature matches the hash of the purchase order in the supplier's possession, it proves that (1) the supplier's copy of the purchase order is an exact copy of a purchase order that exists on some other system (otherwise, the two hashes would not match) and (2) that

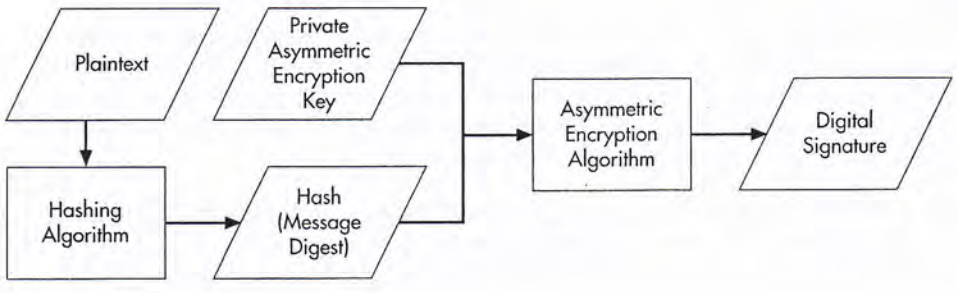



**FIGURE 9-2**
**Creating a Digital Signature**

the purchase order must have existed on the *customer's* information system (otherwise, decrypting the digital signature with the customer's public key would not have produced the hash).

One question still remains, however. Successfully using a public key to decrypt a document or file proves that it was created by the party possessing the corresponding private key. But how can the recipient be sure of the other party's identity? Returning to our prior example, how can a supplier know that the public key purportedly belonging to a customer really belongs to a legitimate customer and not to a criminal who created that pair of public and private keys? For that matter, how does the supplier obtain the customer's public key? The answers to these questions involve the use of digital certificates and a public key infrastructure.

## Digital Certificates and Public Key Infrastructure

A ***digital certificate*** is an electronic document that contains an entity's public key and certifies the identity of the owner of that particular public key. Thus, digital certificates function like the digital equivalent of a driver's license or passport. Just as passports and drivers licenses are issued by a trusted independent party (the government) and employ mechanisms such as holograms and watermarks to prove that they are genuine, digital certificates are issued by an organization called a ***certificate authority*** and contain the certificate authority's digital signature to prove that they are genuine. Digital certificates intended for e-business use are typically issued by commercial certificate authorities, such as Thawte and VeriSign. These certificate authorities charge a fee to issue a pair of public and private keys and collect evidence to verify the claimed identity of the person or organization purchasing those keys and the corresponding digital certificate.

This system for issuing pairs of public and private keys and corresponding digital certificates is called a ***public key infrastructure (PKI)***. The entire PKI system hinges on trusting the certificate authorities that issue the keys and certificates. The AICPA's Trust Services framework contains a list of criteria that can be used to evaluate the overall reliability of a particular certificate authority. One important factor concerns the procedures the certificate authority uses to verify the identity of an applicant for a digital certificate. Several classes of digital certificates exist. The cheapest, and least trustworthy, may involve nothing more than verifying the applicant's e-mail address. The most expensive certificates may require verification of the applicant's identity through use of credit reports and tax returns. Digital certificates are valid for only a specified period of time. Thus, a second important criterion for assessing the reliability of a certificate authority is the procedures it uses to update certificates and revoke expired digital certificates.

Digital certificates provide a mechanism for securely obtaining and verifying the validity of another party's public key. Organizations can store their digital certificates on their Web sites. Browsers are designed to automatically obtain a copy of a Web site's digital certificate to acquire the site's public key. (You can manually examine the contents of a Web site's digital certificate by double-clicking on the lock icon that appears in your browser window when you visit a Web site). Browsers also are designed to automatically check the validity of a Web site's digital certificate. Recall that a digital certificate is signed by the issuing certificate authority. All browsers come preloaded with the public keys of widely recognized certificate authorities. (In Internet Explorer, you can view the list of certificate authorities trusted by your browser by opening your browser, selecting Internet Options on the Tools menu, then moving to the Content tab and then clicking the Publishers button). The browser uses that key to decrypt the certificate authority's digital signature, which yields a hash of the digital certificate. The browser then creates its own hash of the digital certificate; if the two hashes match, the certificate is valid.

## Illustrative Example: The Role of Encryption and Hashing in E-Business

To illustrate how hashing, symmetric encryption, and asymmetric encryption techniques are all used together in an e-business transaction, Figure 9-3 uses the example of Northwest Industries submitting a competitive bid to provide services to a local government agency. The example assumes that both Northwest Industries and the government agency have previously acquired digital certificates from a mutually trusted certificate authority.

**Step 1.** A Northwest Industries employee connects to the government agency's Web site and clicks on the button for submitting bids on open contracts. *The browser moves to a secure Web page displaying the familiar lock icon. The browser software on the*

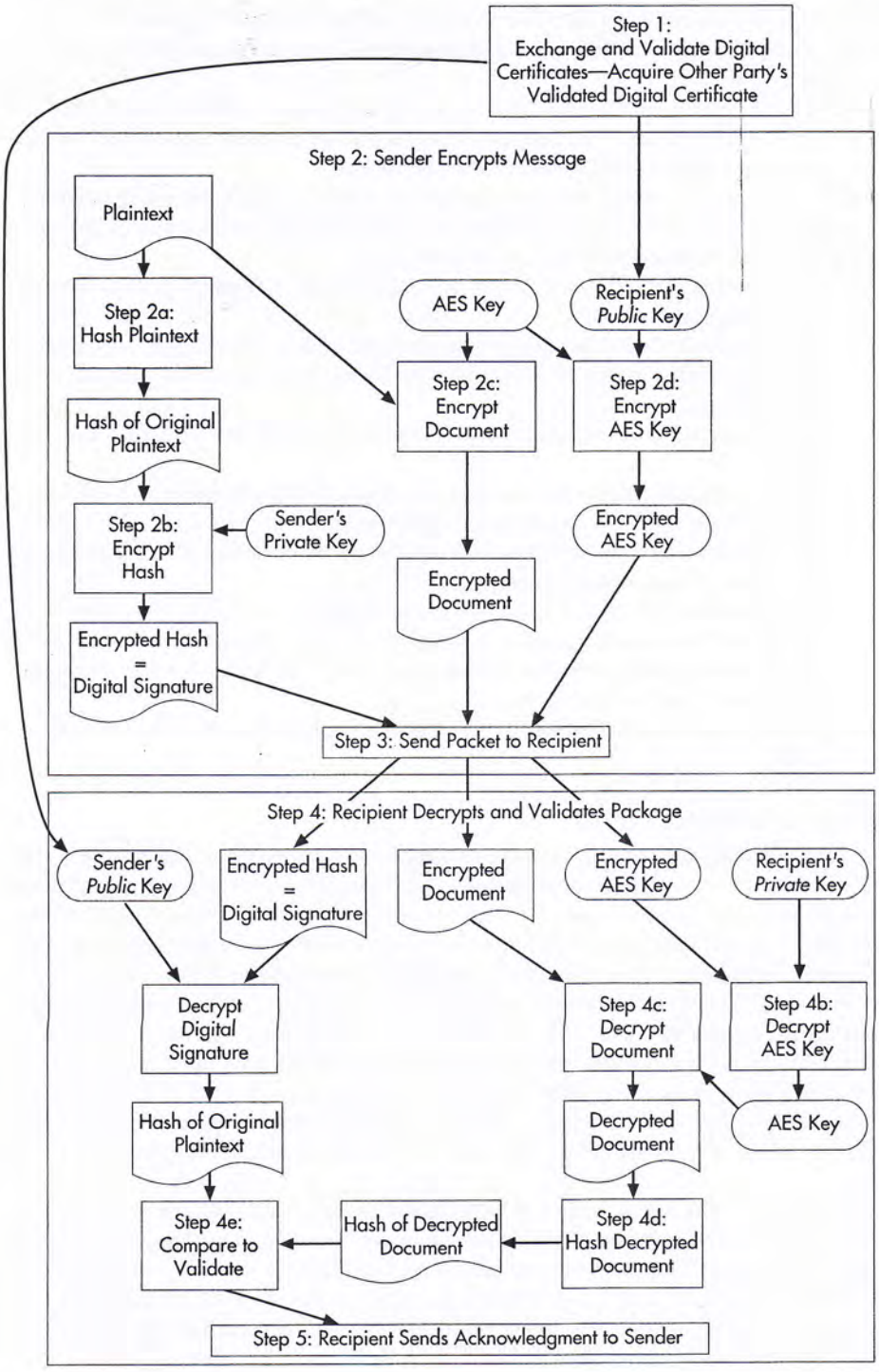



**FIGURE 9-3**
**Using Encryption and Hashing for E-Business**

*employee's computer obtains the Web site's digital certificate, verifies its validity, and opens it to get the agency's public key. The government Web site software follows similar steps to acquire Northwest Industries' public key.*

**Step 2.** The employee clicks a button to attach and submit the company's bid. *Behind the scenes, the encryption software performs the following actions:*

**a.** Uses a hashing algorithm, such as SHA-256, to create a hash of the bid.

**b.** Encrypts the hash using Northwest Industries' private key. This creates a digital signature for the bid.

c. Encrypts the bid using the AES symmetric key algorithm. This protects the confidentiality of the bid, because only someone who knows the AES key can decrypt it.
d. Uses the government agency's public key to encrypt the AES key used in step 2c. This ensures that only the intended recipient (the government agency) will be able to decrypt the AES key needed to decrypt the bid.

**Step 3.** The encrypted bid (created in step 2c), the AES key needed to decrypt that bid (created in step 2d), and Northwest Industries' digital signature (created in step 2b) are all sent over the Internet to the government agency.

**Step 4.** The government agency's computer receives the package of information and performs the following steps:
a. Uses Northwest Industries' public key, obtained in step 1, to decrypt the digital signature created in step 2b. This yields the hash of the original bid that was created by the sender.
b. Uses its private key to decrypt the AES key sent by Northwest Industries in step 2d.
c. Uses the AES key from step 4b to decrypt the encrypted bid produced in step 2c. This produces a plaintext version of Northwest Industries' bid.
d. Uses the same hashing algorithm used by Northwest Industries in step 2a to hash the plaintext copy of the bid created in step 4c.
e. Compares the hash created in step 4d to that produced by step 4a. If the two match, the government agency knows that (1) the copy of the bid it recreated in step 4c was created by Northwest Industries, and (2) the bid has not been altered or garbled during transmission.

**Step 5.** The agency sends Northwest Industries an acknowledgement that its bid has been received.

## Virtual Private Networks (VPNs)

To protect confidentiality and privacy, information must be encrypted not only within a system, but also when it is in transit over the Internet. As Figure 9-4 shows, encrypting information while it traverses the Internet creates a ***virtual private network (VPN)***, so named because it provides the functionality of a privately owned secure network without the associated costs of leased telephone lines, satellites, and other communication equipment. Using VPN software to encrypt information while it is in transit over the Internet in effect creates private communication channels, often referred to as *tunnels*, which are accessible only to those parties possessing the appropriate encryption and decryption keys. VPNs also include controls to authenticate the parties exchanging information and to create an audit trail of the exchange. Thus, VPNs satisfy COBIT control objective DS 5.11, which identifies the need to ensure that sensitive information is exchanged securely and in a manner that can provide proof of its authenticity.

Organizations typically use two types of VPNs. One type uses SSL and browser software to give employees remote access to the corporate network when traveling or working at home. The other type of VPN uses IPSec, a version of the IP protocol that incorporates encryption, to securely connect two offices. Both types of VPNs provide a secure means of exchanging sensitive information over the Internet but create problems for other components of information security. For example, recall from Chapter 8 that firewalls function by inspecting the contents of packets. Firewalls, however, cannot examine packets that are encrypted. There are three

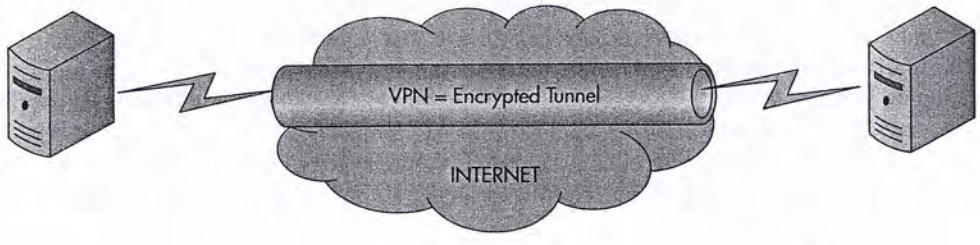



**FIGURE 9-4**
**Virtual Private Networks (VPNs)**

commonly used approaches to dealing with this problem. One is to configure the firewall to send encrypted packets to a computer in the DMZ that decrypts them; that computer then sends the decrypted packets back through the firewall for filtering before being allowed into the internal network. Although this approach allows the firewall to screen all incoming packets, it means that sensitive information is unencrypted both in the DMZ and within the internal network. A second approach is to configure the main firewall to allow encrypted packets to enter the internal network and decrypt them only at their final destination. Although this approach protects the confidentiality of sensitive information until it reaches the appropriate destination, it creates potential holes in access controls because not all incoming packets are filtered by the firewall. The third approach is to have the firewall also function as the VPN termination point, decrypting all incoming traffic and then inspecting the content. This approach is costly, creates a single point of failure (if the firewall goes down, so too does the VPN), and means that sensitive information is not encrypted while traveling on the internal corporate network. Thus, organizations must choose which systems reliability objective is more important: confidentiality (privacy) or security. Unfortunately, this type of dilemma is not limited to firewalls; antivirus programs, intrusion prevention systems, and intrusion detection systems also have difficulty in dealing with encrypted packets. This necessity of making trade-offs among different components of systems reliability is another reason that information security and controls is a managerial concern, and not just an IT issue.

## Summary and Case Conclusion

Jason Scott reviewed what he had learned about Northwest Industries' information systems controls to protect confidentiality and privacy. Confidential information about business plans and personal information collected from customers was encrypted both in storage and whenever it was transmitted over the Internet. Employee laptops were configured with VPN software so that they could securely access the company's information systems when they worked at home or while traveling on business. Northwest Industries employed a key escrow system to manage the encryption keys; Jason had tested and verified that it worked as planned. The CISO had used GAPP to develop procedures to protect personal information collected from customers. Jason verified that employees received detailed training on how to handle such information when initially hired and attended mandatory "refresher" courses every six months. Multifactor authentication was used to control access to the company's databases. Jason also verified that Northwest Industries digitally signed transactions with its business partners and required customers to digitally sign all orders that exceeded $10,000.

Based on his report, Jason's supervisor and the CIO were satisfied with Northwest Industries' measures to protect confidentiality and privacy. They asked Jason next to examine the controls in place to achieve the remaining two principles of systems reliability in the AICPA's Trust Services framework: processing integrity and availability.

## Key Terms

information rights management (IRM) 272
data loss prevention (DLP) 272
digital watermark 273
data masking 274
spam 275
identity theft 275
cookie 277
encryption 278
plaintext 278
ciphertext 278
decryption 278
key escrow 279
symmetric encryption systems 279
asymmetric encryption systems 279
public key 279
private key 280
hashing 280
hash 280
nonrepudiation 281
digital signature 281
digital certificate 282
certificate authority 282
public key infrastructure (PKI) 282
virtual private network (VPN) 284

# AIS IN ACTION

## Chapter Quiz

1. Which of the following statements is true?
   a. Encryption is sufficient to protect confidentiality and privacy.
   b. Cookies are text files that only store information. They cannot perform any actions.
   c. The controls for protecting confidentiality are not effective for protecting privacy.
   d. All of the above are true.

2. A digital signature is _____.
   a. created by hashing a document and then encrypting the hash with the signer's private key
   b. created by hashing a document and then encrypting the hash with the signer's public key
   c. created by hashing a document and then encrypting the hash with the signer's symmetric key
   d. none of the above

3. Able wants to send a file to Baker over the Internet and protect the file so that only Baker can read it and can verify that it came from Able. What should Able do?
   a. Encrypt the file using Able's public key, and then encrypt it again using Baker's private key.
   b. Encrypt the file using Able's private key, and then encrypt it again using Baker's private key.
   c. Encrypt the file using Able's public key, and then encrypt it again using Baker's public key.
   d. Encrypt the file using Able's private key, and then encrypt it again using Baker's public key.

4. Which of the following statements is true?
   a. Encryption and hashing are both reversible (can be decoded).
   b. Encryption is reversible, but hashing is not.
   c. Hashing is reversible, but encryption is not.
   d. Neither hashing nor encryption is reversible.

5. Confidentiality focuses on protecting _____.
   a. personal information collected from customers
   b. a company's annual report stored on its Web site
   c. merger and acquisition plans
   d. all of the above

6. Which of the following statements about obtaining consent to collect and use a customer's personal information is true?
   a. The default policy in Europe is opt-out, but in the United States the default is opt-in.
   b. The default policy in Europe is opt-in, but in the United States the default is opt-out.
   c. The default policy in both Europe and the United States is opt-in.
   d. The default policy in both Europe and the United States is opt-out.

7. One of the ten Generally Accepted Privacy Principles concerns security. According to GAPP, what is the nature of the relationship between security and privacy?
   a. Privacy is a necessary, but not sufficient, precondition to effective security.
   b. Privacy is both necessary and sufficient to effective security.
   c. Security is a necessary, but not sufficient, precondition to protect privacy.
   d. Security is both necessary and sufficient to protect privacy.

8. Which of the following statements is true?
   a. Symmetric encryption is faster than asymmetric encryption and can be used to provide nonrepudiation of contracts.
   b. Symmetric encryption is faster than asymmetric encryption but cannot be used to provide nonrepudiation of contracts.

c. Asymmetric encryption is faster than symmetric encryption and can be used to provide nonrepudiation of contracts.
d. Asymmetric encryption is faster than symmetric encryption but cannot be used to provide nonrepudiation of contracts.

9. Which of the following statements is true?
a. VPNs protect the confidentiality of information while it is in transit over the Internet.
b. Encryption limits firewalls' ability to filter traffic.
c. A digital certificate contains that entity's public key.
d. All of the above are true.

10. Which of the following can organizations use to protect the privacy of a customer's personal information when giving programmers a realistic data set with which to test a new application?
a. digital signature
b. digital watermark
c. data loss prevention
d. data masking

## Discussion Questions

9.1. From the viewpoint of the customer, what are the advantages and disadvantages to the opt-in versus the opt-out approaches to collecting personal information? From the viewpoint of the organization desiring to collect such information?

9.2. What risks, if any, does offshore outsourcing of various information systems functions pose to satisfying the principles of confidentiality and privacy?

9.3. Should organizations permit personal use of e-mail systems by employees during working hours?

9.4. What privacy concerns might arise from the use of biometric authentication techniques? What about the embedding of radio frequency identification (RFID) tags in products such as clothing? What other technologies might create privacy concerns?

9.5. What do you think an organization's duty or responsibility to protect the privacy of its customers' personal information should be? Why?

9.6. Assume you have interviewed for a job online and now receive an offer of employment. The job requires you to move across the country. The company sends you a digital signature along with the contract. How does this provide you with enough assurance to trust the offer so that you are willing to make the move?

## Problems

9.1. Match the terms with their definitions:

| | | |
|---|---|---|
| ____ | 1. Virtual private network (VPN) | a. A hash encrypted with the creator's private key |
| ____ | 2. Data loss prevention (DLP) | b. A company that issues pairs of public and private keys and verifies the identity of the owner of those keys |
| ____ | 3. Digital signature | c. A secret mark used to identify proprietary information |
| ____ | 4. Digital certificate | d. An encrypted tunnel used to transmit information securely across the Internet |
| ____ | 5. Data masking | e. Replacing real data with fake data |
| ____ | 6. Symmetric encryption | f. Unauthorized use of facts about another person to commit fraud or other crimes |

| | |
|---|---|
| ____ 7. Spam | g. The process of turning ciphertext into plaintext |
| ____ 8. Plaintext | h. Unwanted e-mail |
| ____ 9. Hashing | i. A document or file that can be read by anyone who accesses it |
| ____ 10. Ciphertext | j. Used to store an entity's public key, often found on Web sites |
| ____ 11. Information rights management | k. A procedure to filter outgoing traffic to prevent confidential information from leaving |
| ____ 12. Certificate authority | l. A process that transforms a document or file into a fixed-length string of data |
| ____ 13. Nonrepudiation | m. A document or file that must be decrypted to be read |
| ____ 14. Digital watermark | n. A copy of an encryption key stored securely to enable decryption if the original encryption key becomes unavailable |
| ____ 15. Asymmetric encryption | o. An encryption process that uses a pair of matched keys, one public and the other private; either key can encrypt something, but only the other key in that pair can decrypt |
| ____ 16. Key escrow | p. An encryption process that uses the same key to both encrypt and decrypt |
| | q. The inability to unilaterally deny having created a document or file or having agreed to perform a transaction |
| | r. Software that limits what actions (read, copy, print, etc.) that users granted access to a file or document can perform. |

**9.2.** Cost-effective controls to provide confidentiality require valuing the information that is to be protected. This involves classifying information into discrete categories. Propose a minimal classification scheme that could be used by any business, and provide examples of the type of information that would fall into each of those categories.

**9.3.** Download a hash calculator from the course web site that can create hashes for both files and text input. Use it to create SHA-256 (or any other hash algorithm your instructor assigns) hashes for the following:

a. A document that contains this text: "Congratulations! You earned an A+"
b. A document that contains this text: "Congratulations! You earned an A−"
c. A document that contains this text: "Congratulations! You earned an a−"
d. A document that contains this text: "Congratulations! You earned an A+" (this message contains two spaces between the exclamation point and the capital letter Y).
e. Make a copy of the document used in step a, and calculate its hash value.
f. Hash any multiple-page text file on your computer.

**9.4.** Accountants often need to print financial statements with the words "CONFIDENTIAL" or "DRAFT" appearing in light type in the background.

a. Create a watermark with the word "CONFIDENTIAL" in a Word document. Print out a document that displays that watermark.
b. Create the same watermark in Excel, and print out a spreadsheet page that displays that watermark.
c. Can you make your watermark "invisible" so that it can be used to detect whether a document containing sensitive information has been copied to an unauthorized location? How? How could you use that "invisible" watermark to detect violation of copying policy?

**9.5.** Create a spreadsheet to compare current monthly mortgage payments versus the new monthly payments if the loan were refinanced, as shown:

**Refinancing Calculator**

Instructions: Only enter data into borderless cells; DO NOT enter data into cells with borders

| | |
|---|---|
| Current loan amount | 500000 |
| Current term (years) | 30 |

| | |
|---|---|
| Current interest rate | 5% |
| Current monthly payment | $2,684.11 |
| New Loan amount | 400000 |
| New Loan term (years) | 25 |
| New interest rate | 4.50% |
| New monthly payment | $2,223.33 |

**Required**

a. Restrict access to the spreadsheet by encrypting it.
b. Further protect the spreadsheet by limiting users to the ability to select and enter data only in the six cells without borders.

*Hint:* The article "Keeping Secrets: How to Protect Your Computer from Snoops and Spies," by Theo Callahan in the July 2007 issue of the *Journal of Accountancy* explains how to do this using Excel 2003. Review the article, and then use Excel's built-in help function to learn how to do this with later versions of Excel.

9.6. Research the information rights management software that may be available for your computer. What are its capabilities for limiting access rights? Write a report of your findings.

*Optional:* If you can download and install IRM software from Microsoft, use it to prevent anyone from being able to copy or print your report.

9.7. The principle of confidentiality focuses on protecting an organization's intellectual property. The flip side of the issue is ensuring that employees respect the intellectual property of other organizations. Research the topic of software piracy and write a report that explains the following:

a. What software piracy is
b. How organizations attempt to prevent their employees from engaging in software piracy
c. How software piracy violations are discovered
d. The consequences to both individual employees and to organizations who commit software piracy

9.8. Practice encryption.

**Required**

a. Use your computer operating system's built-in encryption capability to encrypt a file. Create another user account on your computer, and log in as that user. Which of the following actions can you perform?
   1. Open the file
   2. Copy the file to a USB drive
   3. Move the file to a USB drive
   4. Rename the file
   5. Delete the file
b. TrueCrypt is one of several free software programs that can be used to encrypt files stored on a USB drive. Download and install a copy of TrueCrypt (or another program recommended by your professor) from the course web site. Use it to encrypt some files on a USB drive. Compare its functionality to that of the built-in encryption functionality provided by your computer's operating system.

9.9. Research the problem of identity theft and write a report that explains the following:

a. Whether the problem of identity theft is increasing or decreasing
b. What kind of identity theft protection services or insurance products are available. Compare and contrast at least two products

9.10. Certificate authorities are an important part of a public key infrastructure (PKI). Research at least two certificate authorities, and write a report that explains the different types of digital certificates that they offer.

**9.11.** Obtain a copy of COBIT (available at www.isaca.org), and read the control objectives that relate to encryption (DS5.8 and DS5.11). What are the essential control procedures that organizations should implement when using encryption?

## Case 9-1 Protecting Privacy of Tax Returns

The department of taxation in your state is developing a new computer system for processing individual and corporate income-tax returns. The new system features direct data input and inquiry capabilities. Taxpayers are identified by Social Security number (for individuals) and federal tax identification number (for corporations). The new system should be fully implemented in time for the next tax season.

The new system will serve three primary purposes:

1. Tax return data will automatically input into the system either directly (if the taxpayer files electronically) or by a clerk at central headquarters scanning a paper return received in the mail.
2. The returns will be processed using the main computer facilities at central headquarters. Processing will include four steps:
   a. Verifying mathematical accuracy
   b. Auditing the reasonableness of deductions, tax due, and so on, through the use of edit routines, which also include a comparison of current and prior years' data
   c. Identifying returns that should be considered for audit by department revenue agents
   d. Issuing refund checks to taxpayers
3. Inquiry services. A taxpayer will be allowed to determine the status of his or her return or get information from the last three years' returns by calling or visiting one of the department's regional offices or by accessing the department's Web site and entering his or her Social Security number.

The state commissioner of taxation and the state attorney general are concerned about protecting the privacy of personal information submitted by taxpayers. They want to have potential problems identified *before* the system is fully developed and implemented so that the proper controls can be incorporated into the new system.

**Required**

Describe the potential privacy problems that could arise in each of the following three areas of processing, and recommend the corrective action(s) to solve each problem identified:

a. Data input
b. Processing of returns
c. Data inquiry

*(CMA examination, adapted)*

## Case 9-2 Generally Accepted Privacy Principles

Obtain the practitioner's version of Generally Accepted Privacy Principles from the AICPA's Web site (www.aicpa.org). Use it to answer the following questions:

1. What is the difference between confidentiality and privacy?
2. How many categories of personal information exist? Why?
3. In terms of the principle of choice and consent, what does GAPP recommend concerning opt-in versus opt-out?
4. Can organizations outsource their responsibility for privacy?
5. What does principle 1 state concerning top management's and the board of directors' responsibility for privacy?
6. What does principle 1 state concerning the use of customers' personal information when organizations test new applications?
7. Obtain a copy of your university's privacy policy statement. Does it satisfy GAPP criterion 2.2.3? Why?
8. What does GAPP principle 3 say about the use of cookies?
9. What are some examples of practices that violate management criterion 4.2.2?
10. What does management criterion 5.2.2 state concerning retention of customers' personal information? How can organizations satisfy this criterion?
11. What does management criterion 5.2.3 state concerning the disposal of personal information? How can organizations satisfy this criterion?
12. What does management criterion 6.2.2 state concerning access? What controls should organizations use to achieve this objective?
13. According to GAPP principle 7, what should organizations do if they wish to share personal information they collect with a third party?
14. What does GAPP principle 8 state concerning the use of encryption?
15. What is the relationship between GAPP principles 9 and 10?

# AIS IN ACTION SOLUTIONS

## Quiz Key

1. Which of the following statements is true?
   a. Encryption is sufficient to protect confidentiality and privacy. (Incorrect. Encryption is not sufficient, because sensitive information cannot be encrypted at all times—it must be decrypted during processing, when displayed on a monitor, or included in a printed report.)
   ▶ b. Cookies are text files that only store information. They cannot perform any actions. (Correct. Cookies are text files, not executable programs. They can, however, store sensitive information, so they should be protected.)
   c. The controls for protecting confidentiality are not effective for protecting privacy. (Incorrect. The same set of controls—encryption, access controls, and training—can be used to protect both confidentiality and privacy.)
   d. All of the above are true. (Incorrect. Statements a and c are false.)

2. A digital signature is _____.
   ▶ a. created by hashing a document and then encrypting the hash with the signer's private key (Correct. Creating a hash provides a way to verify the integrity of a document, and encrypting it with the signer's private key provides a way to prove that the sender created the document.)
   b. created by hashing a document and then encrypting the hash with the signer's public key (Incorrect. Anyone could encrypt something with the signer's public key. Therefore, this process cannot be used to prove who created a document.)
   c. created by hashing a document and then encrypting the hash with the signer's symmetric key (Incorrect. A symmetric key is possessed by more than one party, so encrypting something with it does not provide a means to prove who created a document).
   d. none of the above (Incorrect. Only choices b and c are incorrect; choice a is correct.)

3. Able wants to send a file to Baker over the Internet and protect the file so that only Baker can read it and can verify that it came from Able. What should Able do?
   a. Encrypt the file using Able's public key, and then encrypt it again using Baker's private key. (Incorrect. Able does not know Baker's private key.)
   b. Encrypt the file using Able's private key, and then encrypt it again using Baker's private key. (Incorrect. Able does not know Baker's private key.)
   c. Encrypt the file using Able's public key, and then encrypt it again using Baker's public key. (Incorrect. Baker does not know Able's private key and therefore cannot decrypt the file encrypted with Able's public key.)
   ▶ d. Encrypt the file using Able's private key, and then encrypt it again using Baker's public key. (Correct. Encrypting it with Baker's public key means that only Baker can decrypt it. Then, Baker can use Able's public key to decrypt the file—if the result is understandable, it had to have been created by Able and encrypted with Able's private key.)

4. Which of the following statements is true?
   a. Encryption and hashing are both reversible (can be decoded). (Incorrect. Hashing is irreversible.)
   ▶ b. Encryption is reversible, but hashing is not. (Correct. Encryption can be reversed to decrypt the ciphertext, but hashing cannot be reversed.)
   c. Hashing is reversible, but encryption is not. (Incorrect. Hashing is irreversible, but encryption is reversible.)
   d. Neither hashing nor encryption is reversible. (Incorrect. Encryption is reversible, a process called decryption.)

5. Confidentiality focuses on protecting _____.
   a. personal information collected from customers (Incorrect. Protecting customers' personal information relates to the principle of privacy.)

b. a company's annual report stored on its Web site (Incorrect. A company's annual report is meant to be available to the public.)
▶ c. merger and acquisition plans (Correct. Merger and acquisition plans are sensitive information that should not be made public until the deal is consummated.)
d. all of the above (Incorrect. Statements a and b are false.)

6. Which of the following statements about obtaining consent to collect and use a customer's personal information is true?
a. The default policy in Europe is opt-out, but in the United States the default is opt-in. (Incorrect. The default policy in Europe is opt-in, and in the United States it is opt-out.)
▶ b. The default policy in Europe is opt-in, but in the United States the default is opt-out. (Correct.)
c. The default policy in both Europe and the United States is opt-in. (Incorrect. The default policy in Europe is opt-in, and in the United States it is opt-out.)
d. The default policy in both Europe and the United States is opt-out. (Incorrect. The default policy in Europe is opt-in and in the U.S. it is opt-out.)

7. One of the ten Generally Accepted Privacy Principles concerns security. According to GAPP, what is the nature of the relationship between security and privacy?
a. Privacy is a necessary, but not sufficient, precondition to effective security. (Incorrect. Security is one of the ten criteria in GAPP because you need security in order to have privacy. Security alone, however, is not enough—that is why there are nine other criteria in GAPP.)
b. Privacy is both necessary and sufficient to effective security. (Incorrect. Security is one of the ten criteria in GAPP because you need security in order to have privacy. Security alone, however, is not enough—that is why there are nine other criteria in GAPP.)
▶ c. Security is a necessary, but not sufficient, precondition to protect privacy. (Correct.)
d. Security is both necessary and sufficient to protect privacy. (Incorrect. Security is one of the ten criteria in GAPP because you need security in order to have privacy. Security alone, however, is not enough—that is why there are nine other criteria in GAPP.)

8. Which of the following statements is true?
a. Symmetric encryption is faster than asymmetric encryption and can be used to provide nonrepudiation of contracts. (Incorrect. Symmetric encryption cannot be used for nonrepudiation because both parties share the key, so there is no way to prove who created and encrypted a document.)
▶ b. Symmetric encryption is faster than asymmetric encryption but cannot be used to provide nonrepudiation of contracts. (Correct. Symmetric encryption is faster than asymmetric encryption, but it cannot be used for nonrepudiation; the key is shared by both parties, so there is no way to prove who created and encrypted a document.)
c. Asymmetric encryption is faster than symmetric encryption and can be used to provide nonrepudiation of contracts. (Incorrect. Symmetric encryption is faster than asymmetric encryption.)
d. Asymmetric encryption is faster than symmetric encryption but cannot be used to provide nonrepudiation of contracts. (Incorrect. Symmetric encryption is faster than asymmetric encryption. Also, asymmetric encryption can be used to provide nonrepudiation, because encrypting a contract with the creator's private key proves that the encrypter did indeed create the contract.)

9. Which of the following statements is true?
a. VPNs protect the confidentiality of information while it is in transit over the Internet. (Incorrect. This statement is true, but so are the others.)
b. Encryption limits firewalls' ability to filter traffic. (Incorrect. This statement is true—firewalls cannot apply their rules to encrypted packets—but so are the others.)
c. A digital certificate contains that entity's public key. (Incorrect. This statement is true, but so are the others.)
▶ d. All of the above are true. (Correct. All three statements are true.)

10. Which of the following can organizations use to protect the privacy of a customer's personal information when giving programmers a realistic data set with which to test a new application?
    a. digital signature (Incorrect. A digital signature is used for nonrepudiation. However, because it is an encrypted hash, it cannot be used to test programming logic.)
    b. digital watermark (Incorrect. A digital watermark is used to identify proprietary data, but it does not protect privacy.)
    c. data loss prevention (Incorrect. Data loss prevention is designed to protect confidentiality by filtering outgoing messages to prevent sensitive data from leaving the company.)
    ▶ d. data masking (Correct. Masking replaces actual values with fake ones, but the result is still the same type of data, which can then be used to test program logic.)