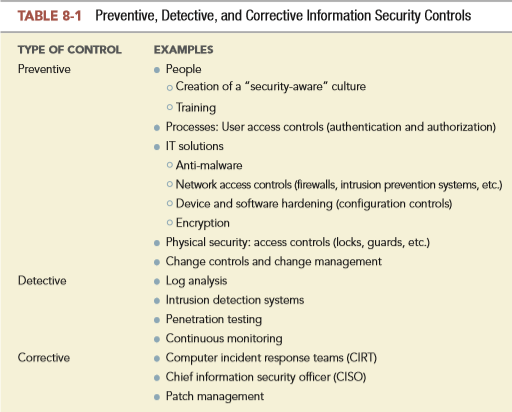
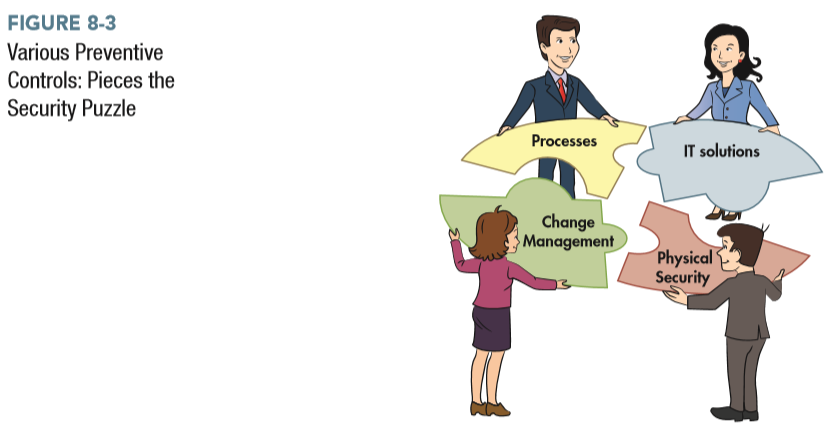
TOPIC 4: READING3 – PREVENTIVE CONTROLS

This section discusses the preventive controls listed in Table 8-1 that organizations commonly use to restrict access to information resources. As Figure 8-3 shows, these various preventive controls fit together like pieces in a puzzle to collectively provide defense-in-depth. Although all of the pieces are necessary, the “people” component is the most important. Management must create a “security-conscious” culture and employees must be trained to follow security policies and practice safe computing behaviors.





PEOPLE: CREATION OF A “SECURITY-CONSCIOUS” CULTURE

The discussion of the COSO and COSO-ERM (Enterprise Risk Management) frameworks in Chapter 7 stressed how top management’s risk attitudes and behaviors create either an internal environment that supports and reinforces sound internal control or one that effectively negates written control policies. The same principle holds regarding information security. Indeed, COBIT 5 specifically identifies an organization’s culture and ethics as one of the critical enablers for effective information security. To create a security-conscious culture in which employees comply with organizational policies, top management must not only communicate the organization’s security policies, but must also lead by example. Employees are more likely to comply with information security policies when they see their managers do so. Conversely, if employees observe managers violating an information security policy, for example by writing down a password and affixing it to a monitor, they are likely to imitate that behavior.

PEOPLE: TRAINING

COBIT 5 identifies employee skills and competencies as another critical enabler for effective information security. Employees must understand how to follow the organization’s security policies. Thus, training is a critical preventive control. Indeed, its importance is reflected in the fact that security awareness training is discussed as a key practice to support several of COBIT 5’s 32 management processes.

All employees should be taught why security measures are important to the organization’s long-run survival. They also need to be trained to follow safe computing practices, such as never opening unsolicited e-mail attachments, using only approved software, not sharing passwords, and taking steps to physically protect laptops. Training is especially needed to educate employees about social engineering attacks. For example, employees should be taught never to divulge passwords or other information about their accounts or their workstation configurations to anyone who contacts them by telephone, e-mail, or instant messaging and claims to be part of the organization’s information systems security function. Employees also need to be trained not to allow other people to follow them through restricted access entrances. This social engineering attack, called piggybacking, can take place not only at the main entrance to the building but also at any internal locked doors, especially to rooms that contain computer equipment. Piggybacking may be attempted not only by outsiders but also by other employees who are not authorized to enter a particular area. Piggybacking often succeeds because many people feel it is rude to not let another person come through the door with them or because they want to avoid confrontations. Role-playing exercises are particularly effective for increasing sensitivity to and skills for dealing with social engineering attacks.

Security awareness training is important for senior management, too, because in recent years many social engineering attacks, such as spear phishing, have been targeted at them. Training of information security professionals is also important. New developments in technology continuously create new security threats and make old solutions obsolete. Therefore, it is important for organizations to support continuing professional education for their security specialists.

However, an organization’s investment in security training will be effective only if management clearly demonstrates that it supports employees who follow prescribed security policies. This is especially important for combating social engineering attacks, because countermeasures may sometimes create embarrassing confrontations with other employees. For example, one of the authors heard an anecdote about a systems professional at a major bank who refused to allow a person who was not on the list of authorized employees to enter the room housing the servers that contained the bank’s key financial information. The person denied entry happened to be a new executive who was just hired. Instead of reprimanding the employee, the executive demonstrated the bank’s commitment to and support for strong security by writing a formal letter of commendation for meritorious performance to be placed in the employee’s performance file. It is this type of visible top management support for security that enhances the effectiveness of all security policies. Top management also needs to support the enforcement of sanctions, up to and including dismissal, against employees who willfully violate security policies. Doing so not only sends a strong message to other employees but also may sometimes lessen the consequences to the organization if an employee engages in illegal behavior.

**PROCESS: USER ACCESS CONTROLS**

It is important to understand that “outsiders” are not the only threat source. An employee may become disgruntled for any number of reasons (e.g., being passed over for a promotion) and seek revenge, or may be vulnerable to being corrupted because of financial difficulties, or may be blackmailed into providing sensitive information. Therefore, organizations need to implement a set of controls designed to protect their information assets from unauthorized use and access by employees. To accomplish that objective, COBIT 5 management practice DSS05.04 stresses the need for controls to manage user identity and logical access so that it is possible to uniquely identify everyone who accesses the organization’s information system and track the actions that they perform. Implementing DSS05.04 involves the use of two related but distinct types of user access controls: authentication controls and authorization controls. Authentication controls restrict who can access the organization’s information system. Authorization controls limit what those individuals can do once they have been granted access.

**AUTHENTICATION CONTROLS**

Authentication is the process of verifying the identity of the person or device attempting to access the system. The objective is to ensure that only legitimate users can access the system. Three types of credentials can be used to verify a person’s identity:

1. Something they know, such as passwords or personal identification numbers (PINs)

2. Something they have, such as smart cards or ID badges

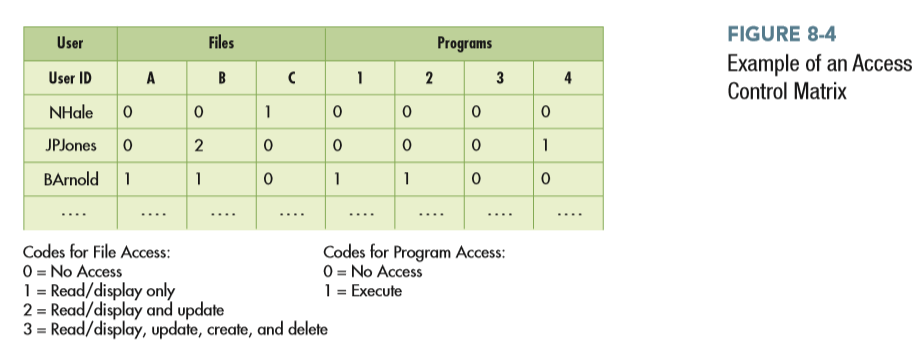
3. Some physical or behavioral characteristic (referred to as a biometric identifier), such as fingerprints or typing patterns.

Passwords are probably the most commonly used authentication method, and also the most controversial. Focus 8-1 discusses some of the requirements for creating strong passwords as well as the ongoing debate about their continued use in the future.

Individually, each authentication method has its limitations. Passwords can be guessed, lost, written down, or given away. Physical identification techniques (cards, badges, USB devices, etc.) can be lost, stolen, or duplicated. Even biometric techniques are not yet 100% accurate, sometimes rejecting legitimate users (e.g., voice recognition systems may not recognize an employee who has a cold) and sometimes allowing access to unauthorized people. Moreover, some biometric techniques, such as fingerprints, carry negative connotations that may hinder their acceptance. There are also security concerns about storage of the biometric information itself. Biometric templates, such as the digital representation of an individual’s fingerprints or voice, must be stored somewhere. The compromising of those templates would create serious, lifelong problems for the donor because biometric characteristics, unlike passwords or physical tokens, cannot be replaced or changed.

Although none of the three basic authentication credentials, by itself, is foolproof, the use of two or all three types in conjunction, a process referred to as multifactor authentication, is quite effective. For example, requiring a user both to insert a smart card in a card reader and enter a password provides much stronger authentication than using either method alone. In some situations, using multiple credentials of the same type, a process referred to as multimodal authentication, can also improve security. For example, many online banking sites use several things that a person knows (password, user ID, and recognition of a graphic image) for authentication. Similarly, because most laptops now are equipped with a camera and a microphone, plus a fingerprint reader, it is possible to employ multimodal biometric authentication involving a combination of face, voice, and fingerprint recognition to verify identity. Both multifactor authentication and multimodal authentication are examples of applying the principle of defense-in-depth.

It is important to authenticate not only people, but also every device attempting to connect to the network. Every workstation, printer, or other computing device needs a network interface card (NIC) to connect to the organization’s internal network. Each NIC has a unique identifier, referred to as its media access control (MAC) address. Therefore, an organization can restrict network access to only corporate-owned devices by comparing the device’s MAC to a list of recognized MAC addresses. There exists software, however, that can be used to change a device’s MAC address, thereby enabling malicious users to “spoof” their device’s identity. Therefore, a stronger way to authenticate devices involves the use of digital certificates that employ encryption techniques to assign unique identifiers to each device. Digital certificates and encryption are discussed in Chapter 9.



AUTHORIZATION CONTROLS Authorization is the process of restricting access of authenticated users to specific portions of the system and limiting what actions they are permitted to perform. As COBIT 5 management practice DSS06.03 explains, the objective is to structure an individual employee’s rights and privileges in a manner that establishes and maintains adequate segregation of duties. For example, a customer service representative should not be authorized to access the payroll system. In addition, customer service representatives should be permitted only to read, but not to change, the prices of inventory items.

Authorization controls are often implemented by creating an access control matrix (Figure 8-4). Then, when an employee attempts to access a particular information systems resource, the system performs a compatibility test that matches the user’s authentication credentials against the access control matrix to determine whether that employee should be allowed to access that resource and perform the requested action. It is important to regularly update the access control matrix to reflect changes in job duties due to promotions or transfers. Otherwise, over time an employee may accumulate a set of rights and privileges that is incompatible with proper segregation of duties.

Figure 8-5 shows how the information contained in an access control matrix is used to implement authorization controls in an ERP system. The upper portion of the screenshot shows that for each employee role, the system provides a number of predefined combinations of permissions to enforce common access restrictions. For example, the first entry (Do Not Restrict Employee Fields) opens a dialog box asking whether employees in this role can view records for other employees (appropriate for managers) or only their own. The lower portion of the screenshot shows that controls can be designed for each specific activity performed by this employee role. Clicking on the word “Edit” to the right of a specific activity brings up another screen where specific permissions (read, edit, create, delete) can be assigned to specific subsets of records and even to fields within those records.

It is possible to achieve even greater control and segregation of duties by using business process management systems to embed authorization into automated business processes, rather than relying on a static access control matrix. For example, authorization can be granted only to perform a specific task for a specific transaction. Thus, a particular employee may be permitted to access credit information about the customer who is currently requesting service, but simultaneously prevented from “browsing” through the rest of the customer file. In addition, business process management systems enforce segregation of duties because employees can perform only the specific tasks that the system has assigned them. Employees cannot delete tasks from their assigned task list, and the system sends reminder messages until the task is completed—two more measures that further enhance control. Business process management software also can instantly route transactions that require specific authorization (such as a credit sale above a certain amount) electronically to a manager for approval. The transaction cannot continue until authorization is granted, but because the need for such approval is indicated and granted or denied electronically, this important control is enforced without sacrificing efficiency.

Like authentication controls, authorization controls can and should be applied not only to people but also to devices. For example, including MAC addresses or digital certificates in the access control matrix makes it possible to restrict access to the payroll system and payroll master files to only payroll department employees and only when they log in from their desktop or assigned laptop computer. After all, why would a payroll clerk need to log in from a workstation located in the warehouse or attempt to establish dial-in access from another country? Applying authentication and authorization controls to both humans and devices is another way in which defense-in-depth increases security.