Information Security Controls/ Security Controls

To protect their information assets, organizations implement controls, or defense mechanisms (also called countermeasures). These controls are designed to protect all of the components of an information system, including data, software, hardware, and networks. Because there are so many diverse threats, organizations utilize layers of controls, or defense-in-depth

Controls are intended to prevent accidental hazards, deter intentional acts, detect problems as early as possible, enhance damage recovery, and correct problems. Before you study controls in more detail, it is important to emphasize that the single most valuable control is user education and training. Effective and ongoing education makes every member of the organization aware of the vital importance of information security

In the next section, you will learn about three major types of controls:

physical controls,

access controls, and

communications controls.

Figure 4.2 illustrates these controls. In addition to applying controls, organizations plan for business continuity in case of a disaster, and they periodically audit their information resources to detect possible threats. You will study these topics in the next section as well

Physical Controls

Physical controls prevent unauthorized individuals from gaining access to a company's facilities. Common physical controls include walls, doors, fencing, gates, locks, badges, guards, and alarm systems. More sophisticated physical controls include pressure sensors, temperature sensors, and motion detectors. One shortcoming of physical controls is that they can be inconvenient to employee

Guards deserve special mention because they have very difficult jobs, for at least two reasons. First, their jobs are boring and repetitive and generally do not pay well. Second, if guards perform their jobs thoroughly, the other employees harass them, particularly if they slow up the process of entering the facility.

Organizations also implement physical security measures that limit computer users to acceptable login times and locations. These controls also limit the number of unsuccessful login attempts, and they require all employees to log off their

computers when they leave for the day. In addition, they set the employees' computers to automatically log off the user after a certain period of disuse

Access Controls

Access controls restrict unauthorized individuals from using information resources. These controls involve two major functions: authentication and authorization. Authentication confi rms the identity of the person requiring access. After the person is authenticated (identified the next step is authorization. Authorization determines which actions, rights, or privileges the person has, based on his or her verifi ed identity. Let's examine these functions more closely.

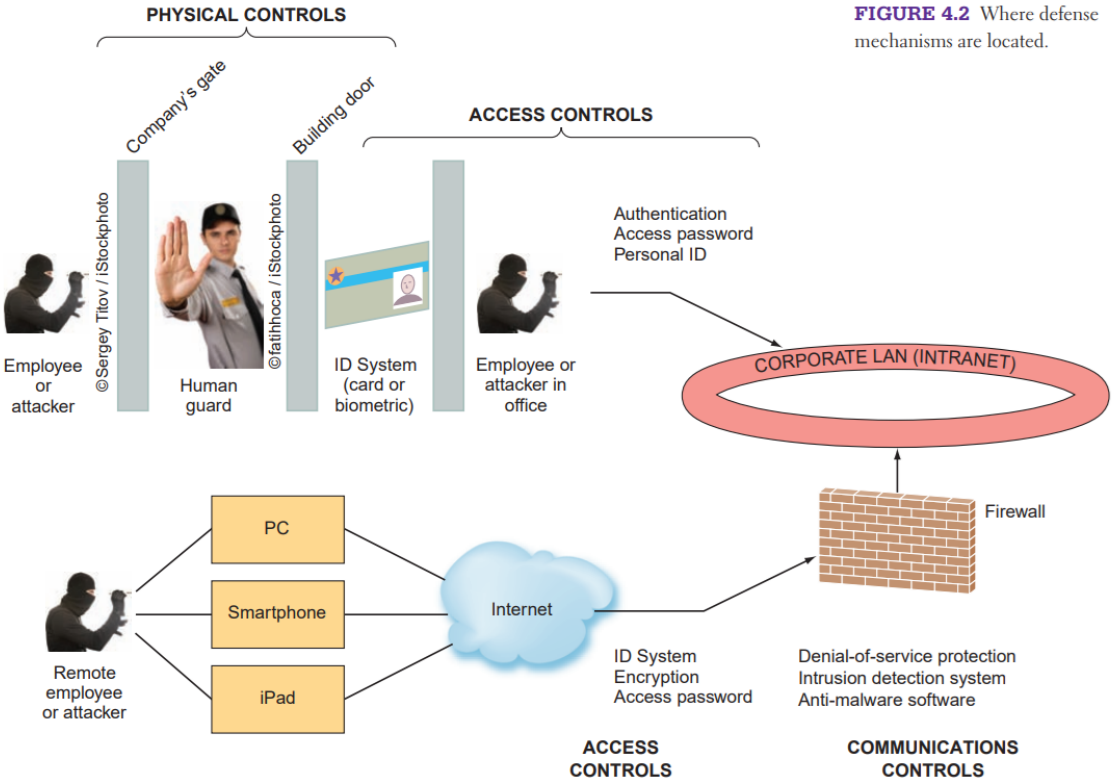

FIGURE 4.2 Where defense mechanisms are located.

Authentication. To authenticate (identify) authorized personnel, an organization can use one or more of the following methods: something the user is, something the user has, something the user does, and/or something the user knows. Something the user is, also known as biometrics, is an authentication method that examines a person's innate physical characteristics. Common biometric applications are fi ngerprint scans, palm scans, retina scans, iris recognition, and facial recognition. Of these applications, fi ngerprints, retina scans, and iris recognition provide the most defi nitive identifi cation. The following example shows how powerful biometrics can be for identifi cation purposes

Example

The Biometric Identification Project of India

India has vast numbers of anonymous poor citizens. To address this problem, the nation instituted its Unique Identification Project, also known as Aadhaar, which means "the foundation" in several Indian languages. The goal of the Unique Identifi cation Project is to issue identifi - cation numbers linked to the fingerprints and iris scans of every single person in India. This process will ultimately encompass some 1.2 billion people who speak more than 300 languages and dialects. The biometrics and the Aadhaar identifi cation number will serve as a verifi able, portable, and unique national ID. This project seeks to remedy a key problem that relates to poor people. The Indian government does not offi cially acknowledge the existence of many poor citizens because these

individuals do not possess birth certificates and other official documentation. Therefore, they cannot access government services to which they are entitled, nor can they open bank accounts. For example, in mid-2012, fewer than half of Indian households had an associated bank account. The rest of households are "unbanked," meaning they must stash their savings in cash around their homes. Aadhaar went into operation in September 2010, when officials armed with iris scanners, fingerprint scanners, digital cameras, and laptops began registering the first few villagers as well as slum dwellers in the country's capital city, Delhi. The government plans to enter 600 million people into its biometric database by 2014. Each individual record contains 4–8 megabytes. Consequently, the database will ultimately hold roughly 20 petabytes. A database of this scale is unprecedented, and managing it will be extraordinarily difficult. One of the most daunting challenges confronting the project is to ensure that each record in the database is matched to one and only one person. For this process, Aadhaar must check all 10 fingerprints and both irises of each person against those of everyone else in the country. Using 10 prints and both irises boosts the accuracy rate to 99 percent. However, in a country the size of India, 99 percent accuracy means that 12 million people could end up with faulty records. Additionally, Aadhaar faces enormous physical and technical challenges: reaching millions of illiterate Indians who have never seen a computer, persuading them to have their irises scanned, ensuring that their scanned information is accurate, and safeguarding the resulting massive amounts of data. Another problem is that civil libertarians object to the project on privacy grounds. As an example of the potential impact of this project, consider Kiran, a poor citizen of India. She thinks she is 32, but she is not sure. She has no birth certificate or ID of any kind—no driver's license, no voting card, nothing at all to document her existence. When she was 24, she left her home in a destitute farming village and ended up in a Delhi slum. She and

her children were among the first individuals to have their personal information entered into the Aadhaar system. The first thing Kiran plans to use her Aadhaar number for is to obtain a city government card that will entitle her to subsidized groceries. “I’ve tried very hard to get one before, but they wouldn’t give it to me because I couldn’t prove I live in Delhi,” she explains. In sum, the Aadhaar project should enable millions of poor Indian citizens to access government services that previously were out of reach to them.