Unintentional Threats to Information Systems

Information systems are vulnerable to many potential hazards and threats, as you can see in Figure below. The two major categories of threats are unintentional threats and deliberate threats. This section discusses unintentional threats, and the next section addresses deliberate threats.

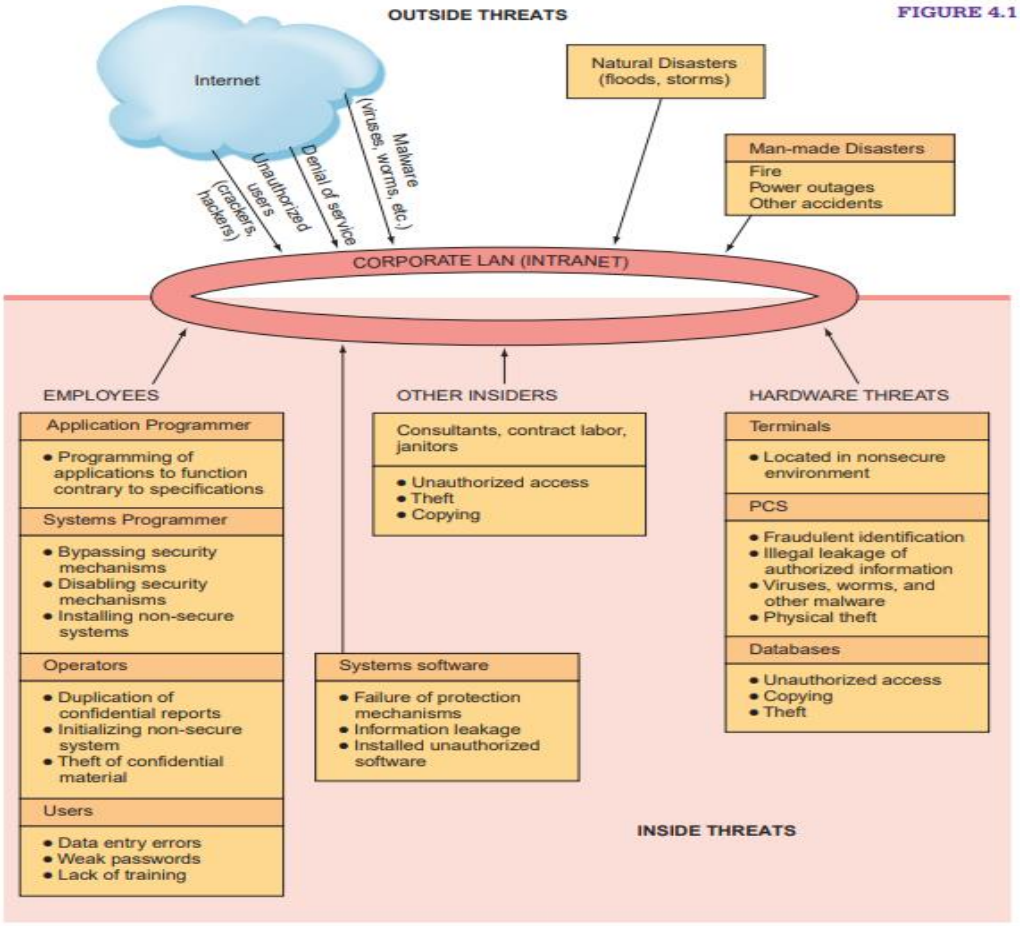

FIGURE 4.1 Security threats.

Unintentional threats are acts performed without malicious intent that nevertheless represent a serious threat to information security. A major category of unintentional threats is human error.

Human Errors

Human Errors Organizational employees span the breadth and depth of the organization, from mail clerks to the CEO, and across all functional areas. There are two important points to be made about employees. First, the higher the level of employee, the greater the threat he or she poses to information security. This is true because higher-level employees typically have greater access to corporate data, and they enjoy greater privileges on organizational information systems.

Second, employees in two areas of the organization pose especially signifi cant threats to information security: human resources and information systems. Human resources employees generally have access to sensitive personal information about all employees. Likewise, IS employees not only have access to

sensitive organizational data, but they often control the means to create, store, transmit, and modify that data

Other employees include contract labor, consultants, and janitors and guards. Contract labor, such as temporary hires, may be overlooked in information security arrangements. However, these employees often have access to the company's network, information systems, and information assets. Consultants, although technically not employees, perform work for the company. Depending on the nature of their work, they may also have access to the company's network, information systems, and information assets.

Finally, janitors and guards are the most frequently ignored people in information security systems. Companies frequently outsource their security and janitorial services. As with contractors, then, these individuals work for the company although they technically are not employees. Moreover, they are usually present when most—if not all—other employees have gone home. They typically have keys to every offi ce, and nobody questions their presence in even the most sensitive parts of the building. In fact, an article from 2600: The Hacker Quarterly described how to get a job as a janitor for the purpose of gaining physical access to an organization. Human errors or mistakes by employees pose a large problem as the result of laziness, carelessness, or a lack of awareness concerning information security. This lack of awareness comes from poor education and training efforts by the organization. Human mistakes manifest themselves in many different ways, as shown in below Table

Human Mistake	Description and Examples
Carelessness with laptops	Losing or misplacing laptops, leaving them in taxis, and so on.
Carelessness with computing devices	Losing or misplacing these devices, or using them carelessly so that malware is introduced into an organization's network.
Opening questionable e-mails	Opening e-mails from someone unknown, or clicking on links embedded in e-mails (see *phishing attack* in Table 4.2).
Careless Internet surfing	Accessing questionable Web sites; can result in malware and/or alien software being introduced into the organization's network.
Poor password selection and use	Choosing and using weak passwords (see *strong passwords* in the "Authentication" section later in this chapter).
Carelessness with one's office	Unlocked desks and filing cabinets when employees go home at night; not logging off the company network when gone from the office for any extended period of time.
Carelessness using unmanaged devices	Unmanaged devices are those outside the control of an organization's IT department and company security procedures. These devices include computers belonging to customers and business partners, computers in the business centers of hotels, and computers in Starbucks, Panera Bread, and so on.
Carelessness with discarded equipment	Discarding old computer hardware and devices without completely wiping the memory; includes computers, cell phones, BlackBerry® units, and digital copiers and printers.
Careless monitoring of environmental hazards	These hazards, which include dirt, dust, humidity, and static electricity, are harmful to the operation of computing equipment.

The human errors that you have just studied, although unintentional, are committed entirely by employees. However, employees also can make unintentional mistakes as a result of actions by an attacker. Attackers often employ social engineering to induce individuals to make unintentional mistakes and disclose sensitive information

Social Engineering

Social engineering is an attack in which the perpetrator uses social skills to trick or manipulate legitimate employees into providing confidential company information such as passwords. The most common example of social engineering occurs when the attacker impersonates someone else on the telephone, such as a company manager or an information systems employee. The attacker claims he forgot his password and asks the legitimate employee to give him a password to use. Other common ploys include posing as an exterminator, an air-conditioning technician, or a fi remarshal. Examples of social engineering abound. In one company, a perpetrator entered a company building wearing a company ID card that looked legitimate. He walked around and put up signs on bulletin boards reading "The help desk telephone number has been changed. The new number is 555-1234." He then exited the building and began receiving calls from legitimate employees thinking they were calling the company help desk. Naturally, the first thing the perpetrator asked for was user name and password. He now had the information necessary to access the company's information systems. Two other social engineering techniques are tailgating and shoulder surfing. Tailgating is a technique designed to allow the perpetrator to enter restricted areas that are controlled with locks or card entry. The perpetrator follows closely behind a legitimate employee and, when the employee gains entry, the attacker asks him or her to "hold the door." Shoulder surfing occurs when a perpetrator watches an employee's computer screen over the employee's shoulder. This technique is particularly successful in public areas such as in airports and on commuter trains and airplanes

Deliberate/intentional Threats to Information Systems

There are many types of deliberate threats to information systems. We provide a list of ten common types for your convenience.

- Espionage or trespass

- Information extortion
- Sabotage or vandalism
- Theft of equipment or information
- Identity theft
- Compromises to intellectual property
- Software attacks
- Alien software
- Supervisory control and data acquisition (SCADA) attacks
- Cyberterrorism and cyberwarfare

Espionage or Trespass Espionage or trespass occurs when an unauthorized individual attempts to gain illegal access to organizational information. It is important to distinguish between competitive intelligence and industrial espionage. Competitive intelligence consists of legal information-gathering techniques, such as studying a company's Web site and press releases, attending trade shows, and so on. In contrast, industrial espionage crosses the legal boundary.

Information Extortion Information extortion occurs when an attacker either threatens to steal, or actually steals, information from a company. The perpetrator demands payment for not stealing the information, for returning stolen information, or for agreeing not to disclose the information.

Sabotage or Vandalism Sabotage and vandalism are deliberate acts that involve defacing an organization's Web site, possibly damaging the organization's image and causing its customers to lose faith. One form of online vandalism is a hacktivist or cyberactivist operation. These are cases of high-tech civil disobedience to protest the operations, policies, or actions of an organization or government agency.

Theft of Equipment or Information

Computing devices and storage devices are becoming smaller yet more powerful with vastly increased storage (e.g., laptops, BlackBerry® units, personal digital assistants, smart phones, digital cameras, thumb drives, and iPods). As a result, these devices are becoming easier to steal and easier for attackers to use to steal information.

Human Mistake	Description and Examples
Carelessness with laptops	Losing or misplacing laptops, leaving them in taxis, and so on.
Carelessness with computing devices	Losing or misplacing these devices, or using them carelessly so that malware is introduced into an organization's network.
Opening questionable e-mails	Opening e-mails from someone unknown, or clicking on links embedded in e-mails (see *phishing attack* in Table 4.2).
Careless Internet surfing	Accessing questionable Web sites; can result in malware and/or alien software being introduced into the organization's network.
Poor password selection and use	Choosing and using weak passwords (see *strong passwords* in the "Authentication" section later in this chapter).
Carelessness with one's office	Unlocked desks and filing cabinets when employees go home at night; not logging off the company network when gone from the office for any extended period of time.
Carelessness using unmanaged devices	Unmanaged devices are those outside the control of an organization's IT department and company security procedures. These devices include computers belonging to customers and business partners, computers in the business centers of hotels, and computers in Starbucks, Panera Bread, and so on.

Above Table points out that one type of human mistake is carelessness with laptops. In fact, many laptops have been stolen due to such carelessness. The cost of a stolen laptop includes the loss of data, the loss of intellectual property, laptop replacement, legal and regulatory costs, investigation fees, and loss productivity

The human errors that you have just studied, although unintentional, are committed entirely by employees. However, employees also can make unintentional mistakes as a result of actions by an attacker. Attackers often employ social engineering to induce individuals to make unintentional mistakes and disclose sensitive information.

Social Engineering

Social engineering is an attack in which the perpetrator uses social skills to trick or manipulate legitimate employees into providing confi dential company information such as passwords. The most common example of social engineering occurs when the attacker impersonates someone else on the telephone, such as a company manager or an information systems employee. The attacker claims he forgot his password and asks the legitimate employee to give him a password to use. Other common ploys include posing as an exterminator, an air-conditioning technician, or a fi re marshal. Examples of social engineering abound. In one company, a perpetrator entered a company building wearing a company ID card that looked legitimate. He walked around and put up signs on bulletin boards reading "The help desk telephone number has been changed. The new number is 555-1234." He then exited the building and began receiving calls from legitimate employees thinking they were calling the company help desk. Naturally, the fi rst thing the perpetrator asked for was user name and password. He now had the information necessary to access the company's information systems. Two other social engineering techniques are tailgating and shoulder surfi ng. Tailgating is a technique designed to allow the

perpetrator to enter restricted areas that are controlled with locks or card entry. The perpetrator follows closely behind a legitimate employee and, when the employee gains entry, the attacker asks him or her to "hold the door." Shoulder surfing occurs when a perpetrator watches an employee's computer screen over the employee's shoulder. This technique is particularly successful in public areas such as in airports and on commuter trains and airplanes