Chapter- 8

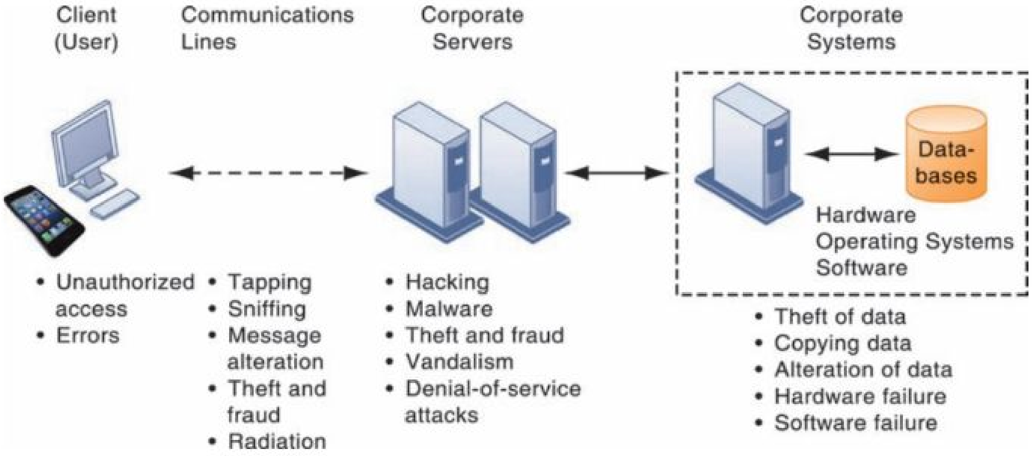
Securing Information Systems

🔖 Topic- 13.1: Why are information systems vulnerable to destruction, error, and abuse?

Security refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems. Controls are methods, policies, and organizational procedures that ensure the safety of the organization's assets, the accuracy and reliability of its records, and operational adherence to management standards.

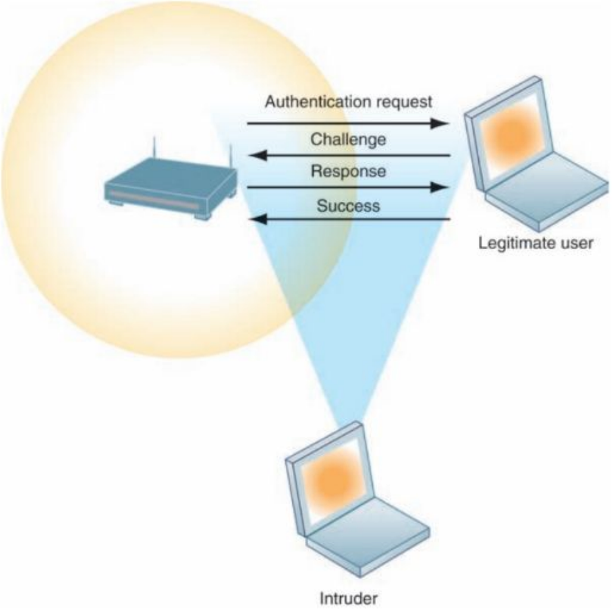
13.1.1: Why Systems are Vulnerable

When large amounts of data are stored in electronic form, they are vulnerable to many kinds of threats. Through communications networks, information systems in different locations are interconnected. The potential for unauthorized access, abuse, or fraud is not limited to a single location but can occur at any access point in the network. Figure 8. 1illustrates the most common threats against contemporary information systems. They can stem from technical, organizational, and environmental factors compounded by poor management decisions. In the multitier client/server computing environment illustrated here, vulnerabilities exist at each layer and in the communications between the layers. Users at the client layer can cause harm by introducing errors or by accessing systems without authorization. It is possible to access data flowing over networks, steal valuable data during transmission, or alter data without authorization. Radiation may disrupt a network at various points as well. Intruders can launch denial-of-service attacks or malicious software to disrupt the operation of websites. Those capable of penetrating corporate systems can steal, destroy, or alter corporate data stored in databases or files.



Internet Vulnerabilities: Large public networks, such as the Internet, are more vulnerable than internal networks because they are virtually open to anyone. The Internet is so huge that when abuses do occur, they can have an enormously widespread impact. When the Internet becomes part of the corporate network, the organization's information systems are even more vulnerable to actions from outsiders. Most

Voice over IP (VoIP) traffic over the Internet is not encrypted. Hackers can intercept conversations or shut down voice service by flooding servers supporting VoIP with bogus traffic.



Wireless Security Challenges: Wi-Fi transmission technology was designed to make it easy for stations to find and hear one another. The service set identifiers (SSIDs) that identify the access points in a Wi-Fi network are broadcast multiple times and can be picked up fairly easily by intruders' sniffer programs (see Figure 8. 2). Wireless networks in many locations do not have basic protections against war driving, in which eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic.

An intruder who has associated with an access point by using the correct SSID is capable of accessing other resources on the network. For example, the intruder could use the Windows operating system to determine which other users are connected to the network, access their computer hard drives, and open or copy their files. Intruders also use the information they have gleaned to set up rogue access points on a different radio channel in physical locations close to users to force a user's radio network interface controller (NIC) to associate with the rogue access point. Once this association occurs, hackers using the rogue access point can capture the names and passwords of unsuspecting users.

13.1.2:Malicious Software: Viruses, Worms, Trojan Horses, and Spyware

Malicious software programs are referred to as malware and include a variety of threats such as computer viruses, worms, and Trojan horses. (See Table 8.1.) A computer virus is a rogue software program that attaches itself to other software programs or data files to be executed, usually without user knowledge or permission. Most computer viruses deliver a payload. The payload may be relatively benign, such as instructions to display a message or image, or it may be highly destructive—destroying programs or data, clogging computer memory, reformatting a computer's hard drive, or causing programs to run improperly.

Viruses typically spread from computer to computer when humans take an action, such as sending an e-mail attachment or copying an infected file. Most recent attacks have come from worms, which are independent computer programs that copy themselves from one computer to other computers over a network. Unlike viruses, worms can operate on their own without attaching to other computer program files and rely less on human behavior to spread from computer to computer. This explains why computer worms spread much more rapidly than computer viruses. Worms destroy data and programs as well as disrupt or even halt the operation of computer networks.

Worms and viruses are often spread over the Internet from files of downloaded software; from files attached to e-mail transmissions; or from compromised e-mail messages, online ads, or instant messaging. Viruses have also invaded computerized information systems from infected disks or infected machines. Especially prevalent today are drive-by downloads, consisting of malware that comes with a downloaded file that a user intentionally or unintentionally requests.

Blogs, wikis, and social networking sites such as Facebook, Twitter, and LinkedIn have emerged as new conduits for malware. Members are more likely to trust messages they receive from friends, even if this communication is not legitimate. One malware scam in spring 2015 appeared to be a video link from a friend saying something like, "This is awesome." If the recipient clicked the link. a pop-up window appeared and prompted that person to click an Adobe Flash Player update to continue. Instead of downloading the player, the malware took over the user's computer, looking for bank account numbers, medical records, and other personal data (Thompson, 2015).

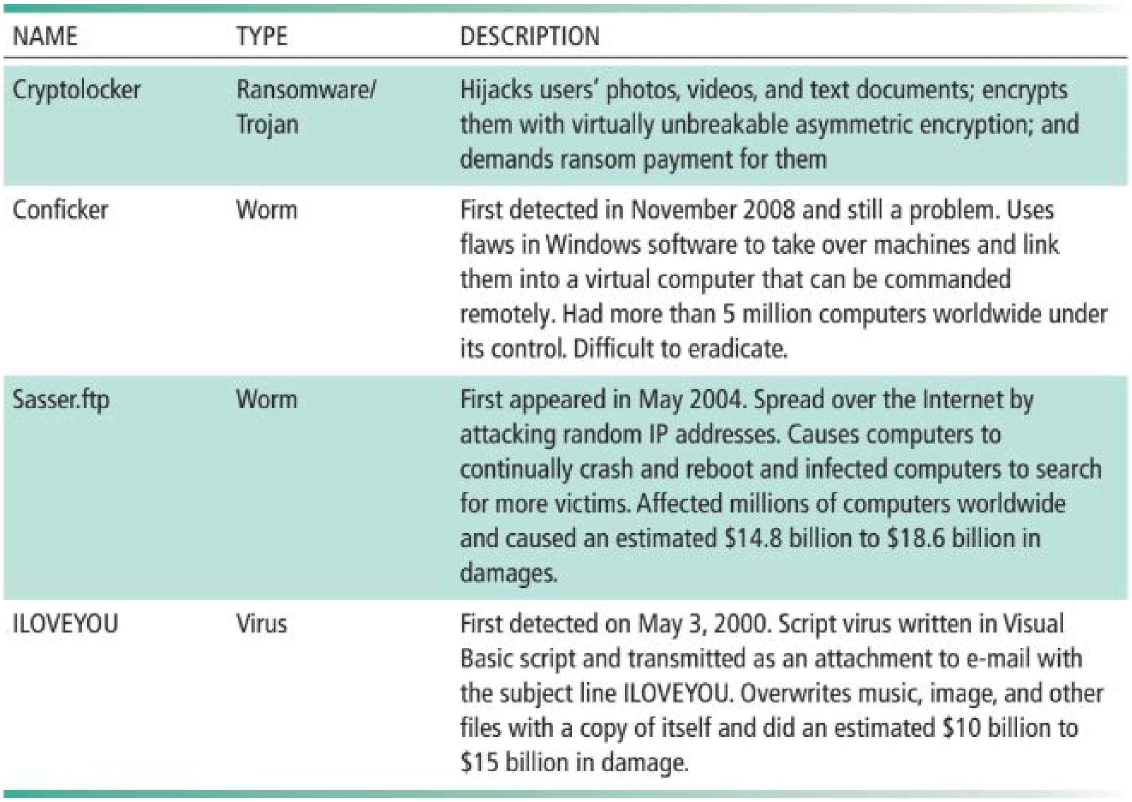
A Trojan horse is a software program that appears to be benign but then does something other than expected. The Trojan horse is not itself a virus because it does not replicate, but it is often a way for viruses or other malicious code to be introduced into a computer system. The term Trojan horse is based on the huge wooden horse the Greeks used to trick the Trojans into opening the gates to their fortified city during the Trojan War. Once inside the city walls, Greek soldiers hidden in the horse revealed themselves and captured the city. An example of a modern-day Trojan horse is the Zeus Trojan. It is often used to steal login credentials for banking by surreptitiously capturing people's keystrokes as they use their computers. Zeus is spread mainly through drive-by downloads and phishing, and recent variants are hard for anti-malware tools to detect.

SQL injection attacks have become a major malware threat. SQL injection attacks take advantage of vulnerabilities in poorly coded web application software to introduce malicious program code into a company's systems and networks.

Malware known as ransomware is proliferating on both desktop and mobile devices. Ransomware tries to extort money from users by taking control of their computers or displaying annoying pop-up messages. One nasty example, CryptoLocker, encrypts an infected computer's files, forcing users to pay hundreds of dollars to regain access. You can get ransomware from downloading an infected attachment, clicking a link inside an e-mail, or visiting the wrong website.

Some types of spyware also act as malicious software. These small programs install themselves surreptitiously on computers to monitor user web-surfing activity and serve up advertising. Thousands of forms of spyware have been documented.

Many users find such spyware annoying, and some critics worry about its infringement on computer users' privacy. Some forms of spyware are especially nefarious. Keyloggers record every keystroke made on a computer to steal serial numbers for software, to launch Internet attacks, to gain access to e-mail accounts, to obtain passwords to protected computer systems, or to pick up personal information such as credit card or bank account numbers. The Zeus Trojan described earlier uses keylogging. Other spyware programs reset web browser home pages, redirect search requests, or slow performance by taking up too much memory.



NAME	TYPE	DESCRIPTION
Cryptolocker	Ransomware/ Trojan	Hijacks users' photos, videos, and text documents; encrypts them with virtually unbreakable asymmetric encryption; and demands ransom payment for them
Conficker	Worm	First detected in November 2008 and still a problem. Uses flaws in Windows software to take over machines and link them into a virtual computer that can be commanded remotely. Had more than 5 million computers worldwide under its control. Difficult to eradicate.
Sasser.ftp	Worm	First appeared in May 2004. Spread over the Internet by attacking random IP addresses. Causes computers to continually crash and reboot and infected computers to search for more victims. Affected millions of computers worldwide and caused an estimated $14.8 billion to $18.6 billion in damages.
ILOVEYOU	Virus	First detected on May 3, 2000. Script virus written in Visual Basic script and transmitted as an attachment to e-mail with the subject line ILOVEYOU. Overwrites music, image, and other files with a copy of itself and did an estimated $10 billion to $15 billion in damage.

Hackers and Computer Crime A hacker is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term cracker is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker are used interchangeably. Hackers gain unauthorized access by finding weaknesses in the security protections websites and computer systems employ, often taking advantage of various features of the Internet that make it an open system and easy to use. Hacker activities have broadened beyond mere system intrusion to include theft of goods and information as well as system damage and cybervandalism, the intentional disruption, defacement, or even destruction of a website or corporate information system.

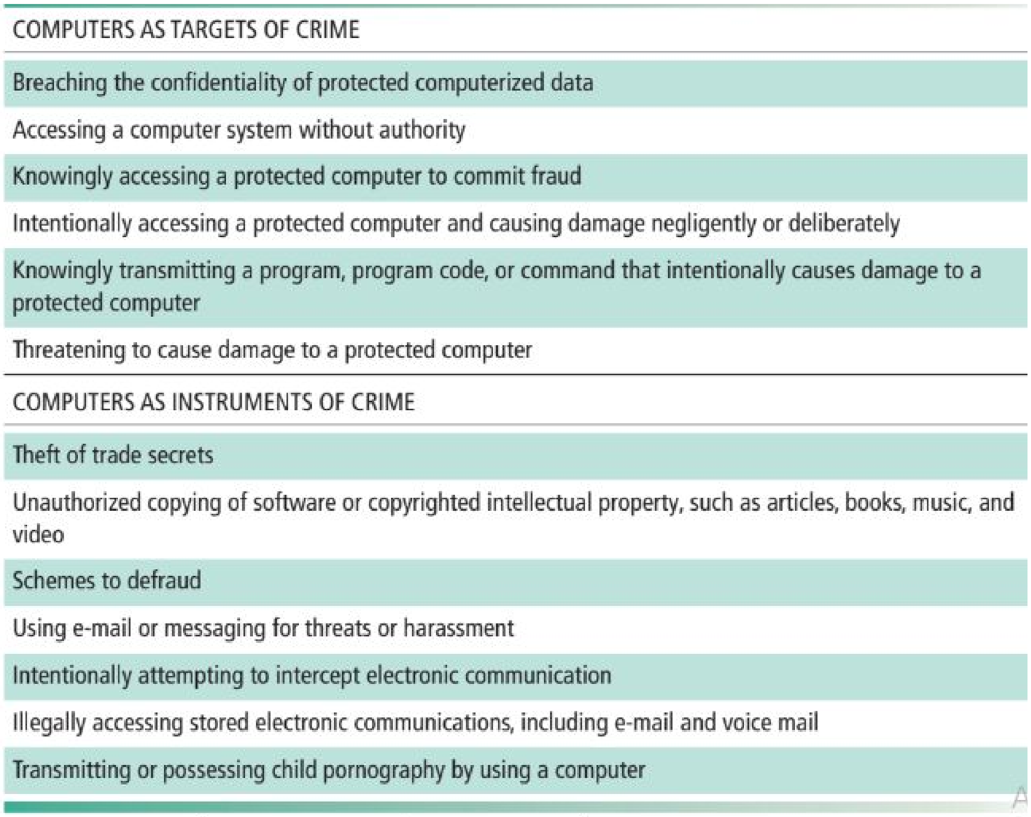
Spoofing and Sniffing,

Hackers attempting to hide their true identities often spoof, or misrepresent, themselves by using fake e-mail addresses or masquerading as someone else. Spoofing may also involve redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination. For example, if hackers redirect customers to a fake website that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business as well as sensitive customer information from the true site. We will provide more detail about other forms of spoofing in our discussion of computer crime.

A sniffer is a type of eavesdropping program that monitors information traveling over a network. When used legitimately, sniffers help identify potential network trouble spots or criminal activity on networks, but when used for criminal purposes, they can be damaging and very difficult to detect. Sniffers enable hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports.

Denial-of-Service Attacks: In a denial-of-service (DoS) attack, hackers flood a network server or web server with many thousands of false communications or requests for services to crash the network. The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate requests. A distributed denial-of-service (DDoS) attack uses numerous computers to inundate and overwhelm the network from numerous launch points.

Computer Crime Most hacker activities are criminal offenses, and the vulnerabilities of systems we have just described make them targets for other types of computer crime as well.



COMPUTERS AS TARGETS OF CRIME
Breaching the confidentiality of protected computerized data
Accessing a computer system without authority
Knowingly accessing a protected computer to commit fraud
Intentionally accessing a protected computer and causing damage negligently or deliberately
Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer
Threatening to cause damage to a protected computer
COMPUTERS AS INSTRUMENTS OF CRIME
Theft of trade secrets
Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video
Schemes to defraud
Using e-mail or messaging for threats or harassment
Intentionally attempting to intercept electronic communication
Illegally accessing stored electronic communications, including e-mail and voice mail
Transmitting or possessing child pornography by using a computer

<u>Identity Theft</u>

1. Identity theft is a crime in which an imposter obtains key pieces of personal information, such as social security numbers, driver’s license numbers, or credit card numbers, to impersonate someone else. The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials.

2. One increasingly popular tactic is a form of spoofing called phishing. Phishing involves setting up fake websites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data.
3. Phishing techniques called evil twins and pharming are harder to detect. Evil twins are wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet, such as those in airport lounges, hotels, or coffee shops.
4. Pharming redirects users to a bogus web page, even when the individual types the correct web page address into his or her browser. This is possible if pharming perpetrators gain access to the Internet address information Internet service providers (ISPs) store to speed up web browsing and the ISP companies have flawed software on their servers that allows the fraudsters to hack in and change those addresses.

Click Fraud: When you click an ad displayed by a search engine, the advertiser typically pays a fee for each click, which is supposed to direct potential buyers to its products. Click fraud occurs when an individual or computer program fraudulently clicks an online ad without any intention of learning more about the advertiser or making a purchase. Click fraud has become a serious problem at Google and other websites that feature pay-per-click online advertising.

🔖 Topic- 13.2: What are the components of an organizational framework for security and control?

13.2.1: Information systems controls

Information systems controls are both manual and automated and consist of general and application controls. General controls govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure. On the whole, general controls apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment.

General controls include software controls, physical hardware controls, computer operations controls, data security controls, controls over the systems development process, and administrative controls. Table 8. 4describes the functions of each of these controls.

Application controls are specific controls unique to each computerized application, such as payroll or order processing. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application. Application controls can be classified as (1) input controls, (2) processing controls, and (3) output controls.

Input controls check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing, and error handling. Processing controls establish that data are complete and accurate during updating. Output controls ensure that the results of computer processing are accurate, complete, and properly distributed. You can find more detail about application and general controls in our Learning Tracks.

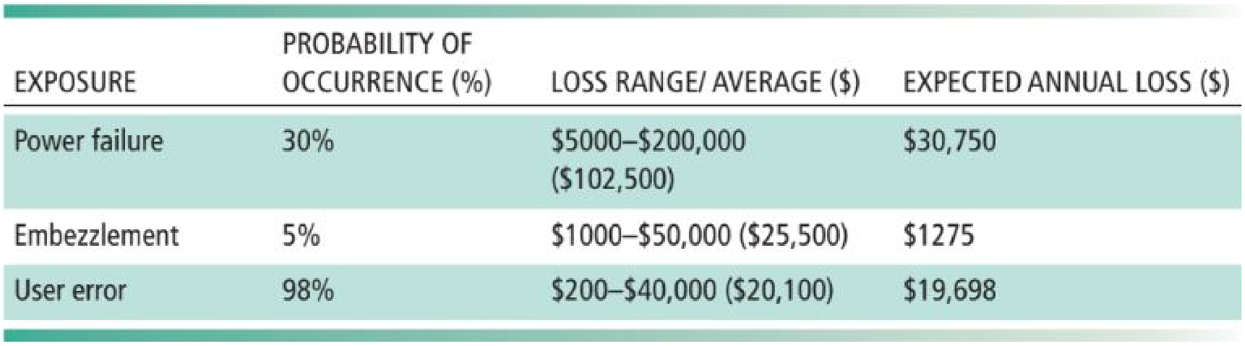
Information systems controls should not be an afterthought. They need to be incorporated into the design of a system and should consider not only how the system will perform under all possible conditions but also the behavior of organizations and people using the system.

13.2.2: Risk Assessment

A risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled. Not all risks can be anticipated and measured, but most businesses will be able to acquire some understanding of the risks they face. Business managers working with information systems specialists should try to determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage.

Table 8. 5illustrates sample results of a risk assessment for an online order processing system that processes 30,000 orders per day. The likelihood of each exposure occurring over a one-year period is expressed as a percentage. The next column shows the highest and lowest possible loss that could be expected each time the exposure occurred and an average loss calculated by adding the highest and lowest figures and dividing by two. The expected annual loss for each exposure can be determined by multiplying the average loss by its probability of occurrence.

This risk assessment shows that the probability of a power failure occurring in a one-year period is 30 percent. Loss of order transactions while power is down could range from $5000 to $200,000 (averaging $102,500) for each occurrence, depending on how long processing is halted. The probability of embezzlement occurring over a yearly period is about 5 percent, with potential losses ranging from $1000 to $50,000 (and averaging $25,500) for each occurrence. User errors have a 98 percent chance of occurring over a yearly period, with losses ranging from $200 to $40,000 (and averaging $20,100) for each occurrence.



EXPOSURE	PROBABILITY OF OCCURRENCE (%)	LOSS RANGE/ AVERAGE ($)	EXPECTED ANNUAL LOSS ($)
Power failure	30%	$5000–$200,000 ($102,500)	$30,750
Embezzlement	5%	$1000–$50,000 ($25,500)	$1275
User error	98%	$200–$40,000 ($20,100)	$19,698

Security Policy

A security policy consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals. What are the firm's most important information assets? Who generates and controls this information in the firm? What existing security policies are in place to protect the information? What level of risk is management willing to accept for each of these assets? Is it willing, for instance, to lose customer credit data once every 10 years? Or will it build a security system for credit card data that can withstand the once-in-a-hundred-year disaster? Management must estimate how much it will cost to achieve this level of acceptable risk.

The security policy drives other policies determining acceptable use of the firm's information resources and which members of the company have access to its information assets. An acceptable use policy (AUP) defines acceptable uses of the firm's information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the Internet. A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance.

Security policy also includes provisions for identity management. Identity management consists of business processes and software tools for identifying the valid users of a system and controlling their access to system resources. It includes policies for identifying and authorizing different categories of system users, specifying what systems or portions of systems each user is allowed to access, and the processes and technologies for authenticating users and protecting their identities.

Disaster Recovery Planning and Business Continuity

Disaster recovery planning devises plans for the restoration of disrupted computing and communications services. Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.

Business continuity planning focuses on how the company can restore business operations after a disaster strikes. The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down.