Chapter 7
Securing Information Systems

As our society and the world come to depend on computers and information systems more and more, firms must put better effort in making their systems less vulnerable and more reliable. The systems must also be more secure when processing transactions and maintaining data.

System Vulnerability and Abuse

As firms become more technologically oriented, they must become more aware of **security** and **control** issues surrounding their information systems and protect the resources.

Why Systems Are Vulnerable?

Vulnerability is weakness or flaw in a computer system that can be exploited by a threat. Security **threat** is a possible danger that might exploit **vulnerabilities** in a computer system to breach security and thus cause possible harm. Information systems are vulnerable to technical, organizational, and environmental threats from internal and external sources. If managers at all levels don't make security and reliability their number one priority, then the threats to an information system can easily become real. The figure below gives you an idea of some of the threats to each component of a typical network.

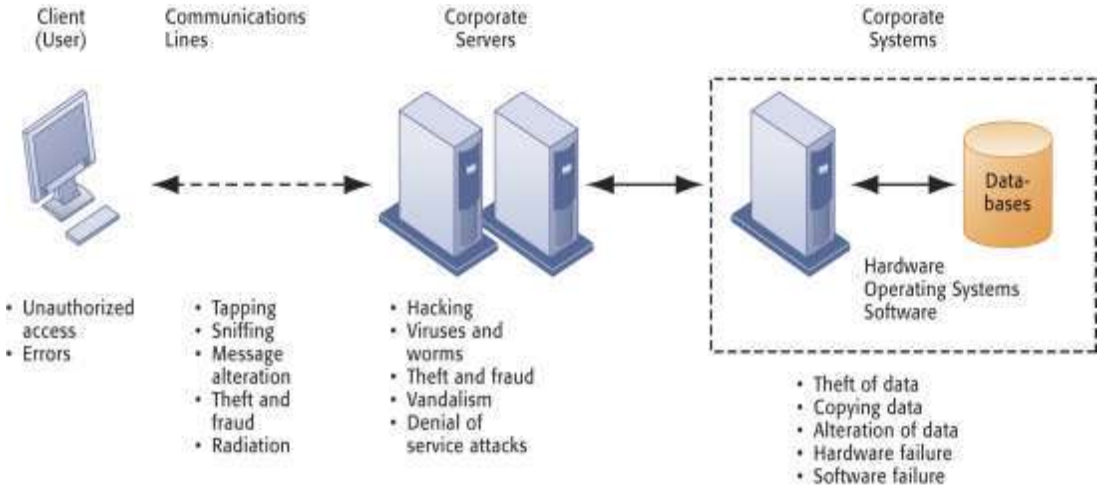

Figure: Contemporary Security Challenges and Vulnerabilities

Businesses that partner with outside companies are more vulnerable. Partnering companies may not protect information as strictly. Employees of the partnering firm may not view security as diligently as the primary business. In today's business environment, it's not enough to protect hardware and software physically located within an organization. Mobile computing devices like smartphones, cell phones, netbooks, and laptops, add to the vulnerability of information systems by creating new points of entry into information systems.

Internet Vulnerabilities

If you connect to the Internet with a cable modem or DSL you are much more vulnerable to hackers on your home PC than if you connect with a dial-up modem. That's because you are always connected, with a permanent IP address, which makes it easier for hackers to find you. The only smart thing to do is keep your software up-to-date and include firewall protection.

Because distributed computing is used extensively in network systems, you have more points of entry, which can make attacking the system easier. The more people you have using the system, the more potential for fraud and abuse of the information maintained in that system. That's why you have to make it everybody's business to protect the system.

Malicious Software

Malicious software, commonly known as malware, is any software that brings harm to a computer system. It can be used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware can be in the form of worms, viruses, Trojans etc., which steal protected data, delete documents or add software not approved by a user. Malware takes partial to full control of our computer to do whatever the malware creator wants. Most malware requires the user to initiate its operation. Some form of attacks includes attachments in e-mails, browsing a malicious website that installs software after the user clicks ok on a pop-up.

Worms

This type of **Malware** uses network resources for spreading. This class was called **worms** because of its peculiar feature to creep from computer to computer using network, mail and other informational channels. Worms intrude our computer, calculate network addresses of other computers and send to these addresses its copies. Many worms that have been created are designed only to spread, and do not attempt to change the systems they pass through. The biggest danger with a worm is its capability to replicate itself on your system, so it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line. Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing web servers, network servers and individual computers to stop responding.
Father Christmas is an example of worm. It was distributed in 1987 and was designed for IBM networks. It was an electronic letter instructing recipient to save it and run it as a program that drew Christmas tree, printed "Merry Christmas!" It also checked address book, list of previously received email and sent copies to each address. The worm quickly overwhelmed the IBM networks and forced the networks and systems to be shut down

Virus
A *computer virus* is a program that inserts itself into one or more files and then performs some (possibly null) action. Computer virus works in two phases. The first phase, in which the virus inserts itself into a file, is called the insertion phase. The second phase, in which it performs some action, is called the execution phase. Almost all viruses are attached to an executable, which means the virus may exist on our computer but it actually cannot infect your computer unless we run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action people will unknowingly continue the spread of a computer virus by sharing infecting files or sending emails with viruses as attachments in the email.

The *Brain (or Pakistani) virus*, written for IBM PCs is an example of this category. It is thought to have been created in early 1986 but was first reported in the United States in October 1987. It alters the boot sectors of floppy disks, possibly corrupting files in the process. It also spreads to any uninfected floppy disks inserted into the system.

Torjan Horse
Trojan horses are the files that claim to be something desirable but, in fact, are malicious code or logic. The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Receivers of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious like changing our desktop, adding silly active desktop icons etc. Sometimes they can cause serious damage by deleting files and destroying information on your system.

Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. A program named "waterfalls.scr" serves as a simple example of a Trojan Horse. The author claims it is a free waterfall screensaver. When run, it instead unloads hidden programs, commands, scripts, or any number of commands without the user's knowledge or consent.

Spyware

Spyware is any software installed on your PC that collects your information without your knowledge, and sends that information back to the creator so they can use your personal information in some nefarious way. This could include keylogging to learn your passwords, watching your searching habits, changing out your browser home and search pages, adding obnoxious browser toolbars, or just stealing your passwords and credit card numbers.

Since spyware is primarily meant to make money at your expense, it doesn't usually kill your PC—in fact, many people have spyware running without even realizing it, but generally those that have one spyware application installed also have a dozen more. Once you've got that many pieces of software spying on you, your PC is going to become slow.

Did you know? What is backdoor?

A backdoor in a computer system is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plain text, and so on, while attempting to remain undetected.

Hackers and Computer Crime

A hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment, or to evaluate those weaknesses to assist in removing them. Hacking practice can either be ethical or unethical. The activity where one breaks into the system but do not violate its security and credentials is called *Ethical Hacking*. Ethical hackers aim to bring into the administrator's notice and vulnerabilities in the system thereby, improvising the robustness and security. Thus term *hacker* does not mean criminal or bad guy. Actually, hackers are the persons with flawless programming skills and hands-on knowledge on both computer hardware and software.

On the other hand, there are people who can though break into systems, get access to secured accounts but their actions are usually unauthorized while they make a backdoor entry into your system. These people (often misinterpreted as hackers) are called as *crackers*. They try and crack passwords, security codes, etc

using various hacking software's which are already available. Such software's are meant to break the code using millions of trials programmed into it by other hackers.

Spoofing and Sniffing

These are two methods that hackers and criminals use to gain improper or illegal access to computer systems. **Spoofing** is becoming a common way to steal financial information through fake Web sites. The spoofed site is almost a mirror image of the real site and unless the unsuspecting user examines the spoof closely, he/she may inadvertently give out important personal and financial information.

Using a **sniffer** program is a popular way to "grab" information as it passes over transmission lines regardless of whether they are hard-wired or wireless. It is almost impossible to detect and encryption is about the only way to safeguard against it.

Denial of Service Attacks

As companies and organizations expand their business to Web sites, they are opening another point of vulnerability through **denial of service attacks.** Using **botnets** to launch **distributed denial of service attacks** is becoming all too common. The hackers seem to enjoy attacking the most popular Web sites like Facebook and Twitter.

Denial of service attacks are at the core of some of the most serious forms of cyberwarfare being played out across the world between countries and governments. From Russia to Iran to South Korea, government networks are being targeted through these kinds of attacks. The use of botnets makes it very difficult to determine the origin of the attacks and pinpoint responsibility.

Computer Crime

Computer crime is a growing national and international threat to the continued development of e-business and e-commerce. When the Internet was first created in the late 1960s, the designers intentionally built it to be open and easily accessible. Little did they know 40 years later, that structure would be the very cause of so much crime and vandalism. Table below lists the best known examples of computer crime.

TABLE 8-2 EXAMPLES OF COMPUTER CRIME

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 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 using a computer

It's very difficult for our society and our governments to keep up with the rapid changes in the types of computer crime being committed. Many laws have to be rewritten and many new laws must be implemented to accommodate the changes.

Identity Theft

The fastest growing crime off or on the Internet is **identity theft**. Even though identity theft is most likely to occur in an offline environment, once your personal information has been stolen it's easy to use it in an online environment.

There are many precautions people can take to help prevent identity theft. One way is to scrutinize emails or phone calls that ask for your personal information or financial account information. No legitimate financial institution will ever send an email requesting you to supply your account information. That is the number one indicator that the email is a **phishing** email. You should ignore and delete the email immediately.

Click Fraud

All those ads you see on Web sites cost the sponsor money. Every time someone clicks on an ad, the sponsor is charged a pay-per-click fee. The fee is

based on the popularity of the search words that generated the ad. What if your company is paying for an ad with little or no resultant traffic to your Web site? That's what happens in the case of click fraud. A person or a software program continually hits on the ad, driving up the advertising fees, without any intention of actually visiting the site.

Internal Threats: Employees

It is surprising to learn that most computer crime against companies is committed by current or former employees. They know the system best, are entrusted with huge amounts of data, and have the easiest access. Managers and executives need to be aware of potential internal threats to their systems and put special measures in place to safeguard systems and data. They also need to impress upon all employees how important security is throughout the system right down to the last person.

Password theft is the easiest way for hackers to gain access to a system. No, they don't come into your office at night and look at the piece of paper in your desk drawer that has your password written on it. They generally use specially written software programs that can build various passwords to see if any of them will work. That's why you should use odd combinations of letters and numbers not easily associated with your name to create your password. The longer the password, the harder it is to replicate. The same password should not be used for more than one access point. Using multiple passwords limits the damage done if a hacker does manage to obtain a single password.

Safeguarding individual passwords from **social engineering** maliciousness is the responsibility of everyone in the organization. An effective way of limiting access to data is to establish computer-generated logs that show every employee who logged on, what they did, what part of the system they accessed, and whether any data were used or updated. Logs are easily created by system software programs and should be periodically reviewed by the information technology staff and department managers. If nothing else, it gives them an idea of what their employees are doing.

Business Value of Security and Control

Transactions worth billions and trillions of dollars are carried out on networks every day. Think of the impact if the networks experience downtime for even a few minutes. It may create serious harm to business reputation of the organization.

If a business doesn't adequately protect its systems for any other reason, it should just to avoid expensive and time-consuming legal action. The national retailer T.J. Maxx was forced to spend about $200 million in court case and damage costs after it experienced a serious security breach in 2008.

Legal and Regulatory Requirements for Electronic Records Management

Because so much of our personal and financial information is now maintained electronically, the government needs to pass laws mandating how the data will be protected from unauthorized or illegal misuse. Govt. of Nepal has already passed a cyber law outlining the requirements for electronic records management and is in process of modifying the law and creating new laws.
All of these laws are in response to computer crimes and abuses that businesses or individuals have committed or experienced.

Electronic Evidence and Computer Forensics

Several things are happening in the corporate worlds that are changing the requirements for how companies handle their electronic documents:

- Companies are communicating more and more with email and other forms of electronic transmissions, and
- Courts are allowing all forms of communication to be held as evidence.

Therefore businesses must develop methods of capturing, storing, and presenting any and all electronic communications including email, instant messaging, and e-commerce transactions.

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. **Computer forensics** is a growing field because of the increasing digitization of documents and communications. Many people believe that just because they delete a file from a computer file directory that it's no longer available or recoverable. That's a false belief. Data remains on hard drives in magnetic form long after it's apparently been deleted. People trained in computer forensics are able to uncover ambient data and other forms of electronic evidence that can be used in courts of law. Businesses and employees must increase their awareness of the necessity for keeping good records.

Establishing a Framework for Security and Control

To prevent security related problems one of the best ways is to institute controls into our information system through methods, policies, and procedures.

Information Systems Controls

These are just a few examples to get you to think about the fact that the company designs the security into the building from the beginning. It doesn't wait until everything is built. You should do the same thing with an information system. It's no different from any other system that requires planning and well-thought-out policies and procedures *before* construction begins.

The two types of information system controls are:

- **General controls:** Software, physical hardware, computer operations, data security, implementation process, and administrative. Table given below describes each of these.
- **Application controls**: Input, processing, and output.

TABLE 8.4 GENERAL CONTROLS

TYPE OF GENERAL CONTROL	DESCRIPTION
Software controls	Monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs.
Hardware controls	Ensure that computer hardware is physically secure, and check for equipment malfunction. Organizations that are critically dependent on their computers also must make provisions for backup or continued operation to maintain constant service.
Computer operations controls	Oversee the work of the computer department to ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs and backup and recovery procedures for processing that ends abnormally.
Data security controls	Ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.
Implementation controls	Audit the systems development process at various points to ensure that the process is properly controlled and managed.
Administrative controls	Formalize standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced.

Risk Assessment

Companies and government systems constantly use **risk assessment** to determine weak links in their physical building security. You can use the same methodology to assess the risk in your information system. Use risk assessment to set up cost comparisons for developing and maintaining security against the loss potential. It's done all the time in other systems, so use it for your information system as well.

Security Policy

Because of the increasing liability for security breaches, many companies are now establishing a chief security officer position to help ensure the firm maximizes the protection of information resources. Some tools available to the CSO are:

- **Security policy:** Principle document that determines security goals and how they will be achieved.
- **Acceptable use policy:** Outlines acceptable and unacceptable uses of hardware and telecommunications equipment.
- **Identity management system:** Manages access to each part of the information system.

Identity management is one of the most important principles of a strong, viable security policy. It includes:

- Business processes and software tools for identifying valid system users.
- Controlling access to system resources.
- Policies for identifying and authorizing different categories of system users.
- Specifying what systems or portions of systems each user is allowed to access.
- Processes and technologies for authenticating users and protecting their identities

Disaster Recovery Planning and Business Continuity Planning

Floods, fires, hurricanes, even tsunamis, happen without a moment's notice. Perhaps the most important element of a successful system is a **disaster recovery plan.** Those firms that had completed **business continuity planning** were able to carry on business, while those that hadn't, spent days and weeks recovering from the terrorist attacks. It's important that managers and employees work with information system technicians to develop these plans.

The Role of Auditing

Companies audit their financial data using outside firms to make sure there aren't any discrepancies in their accounting processes. Perhaps they audit their supply systems on a periodic basis to make sure everything is on the up-and-up. They should also audit their information systems. After all, information is as an important resource as any other in the organization. **MIS audits** verify that the system was developed according to specifications, that the input, processing, and output systems are operating according to requirements, and that the data is

protected against theft, abuse, and misuse. In essence, an MIS audit checks all the controls we've discussed in this chapter.

Note:- This note was provided by Plos Shah.

Information Department,
Complete BBA Solution