UNIT-V

INFORMATION SYSTEM SECURITY AND CONTROL

System Vulnerability – Malicious Software – Establishing A Framework for Security and Control – Information System Control – Risk Assessment – Security policy, the role of Auditing Technologies and Tools for Protecting Information Resources: Access control, firewalls, Intrusion Detection Systems Computer Virus – Security Threads.

INFORMATION SYSTEM SECURITY AND CONTROL

As computers and other digital devices have become essential to business and commerce, they have also increasingly become a target for attacks. In order for a company or an individual to use a computing device with confidence, they must first be assured that the device is not compromised in any way and that all communications will be secure.

The Information Security Triad: Confidentiality, Integrity, Availability (CIA)

Figure 1 The Information Security Triad

Confidentiality

When protecting information, we want to be able to restrict access to those who are allowed to see it; everyone else should be disallowed from learning anything about its contents. This is the essence of confidentiality. For example, federal law requires that universities restrict access to private student information. The university must be sure that only those who are authorized have access to view the grade records.

Integrity

Integrity is the assurance that the information being accessed has not been altered and truly represents what is intended. Just as a person with integrity means what he or she says and can be trusted to consistently represent the truth, information integrity means information truly

represents its intended meaning. Information can lose its integrity through malicious intent, such as when someone who is not authorized makes a change to intentionally misrepresent something. An example of this would be when a hacker is hired to go into the university's system and change a grade.

Integrity can also be lost unintentionally, such as when a computer power surge corrupts a file or someone authorized to make a change accidentally deletes a file or enters incorrect information.

Availability

Information availability is the third part of the CIA triad. *Availability* means that information can be accessed and modified by anyone authorized to do so in an appropriate timeframe. Depending on the type of information, *appropriate timeframe* can mean different things. For example, a stock trader needs information to be available immediately, while a sales person may be happy to get sales numbers for the day in a report the next morning. Companies such as Amazon.com will require their servers to be available twenty-four hours a day, seven days a week. Other companies may not suffer if their web servers are down for a few minutes once in a while.

Concept of Information Security

Information security ensures good data management. It involves the use of technologies, protocols, systems and administrative measures to protect the confidentiality, integrity and availability of information. Information is the most valuable asset of an organization, and any breach can destroy its reputation and continuity.

Need for Information Security

Companies have realized the need and importance of information security and taken steps to be included among organizations known to have the most secure IT infrastructure. As a result, enormous capital is spent every year from companies' budgets to protect the critical information that forms the foundation of their business. Below are a few reasons why information security is critical to the success of any organization.

1) To prevent data breaches

A data breach resulting in the loss of critical business information is quite common. Due to a large amount of data stored on company servers, businesses often become the main target of

cyber-criminals if the network is unprotected. The breaches involving business secrets, confidential health information, and intellectual property can greatly impact the overall health of a business.

2) To check for compromised credentials and broken authentication

Data breaches and other cyber-attacks are usually a result of lax authentication, weak passwords, and poor certificate or key management. Companies often struggle with assigning permissions to appropriate users or departments, resulting in identity theft.

3) To avoid account hijacking

Phishing, fraud, and software exploitations are still very common. Companies relying on cloud services are especially at risk because they are an easy target for cybercriminals, who can eavesdrop on activities, modify data and manipulate transactions. These third-party applications can be used by attackers to launch other attacks as well.

4) To mitigate cyber threats from malicious insiders

An existing or former employee, a cunning business partner, a system administrator or an intruder can destroy the whole information infrastructure or manipulate data for their own purpose. Therefore, it is the responsibility of an organization to take effective measures to control the encryption process and keys. Effective monitoring, logging, and auditing activities are extremely important to keep everything under control.

Types of Information Security Controls

There are three different types of information security controls used to protect data.

- **Physical Control:** Physical controls are the simplest form of information security. These are the things that can actually be touch and seen, such as password-protected locks to avoid unauthorized entry to a secure server room, alarm systems, fences and more.
- **Administrative Control:** These controls mainly involve manual efforts to ensure data security. These include enforcing policies, standards, guidelines and following procedures to ensure business continuity and data protection. Some of the examples of administrative controls include disaster recovery plans, internet usage policies and termination procedures.

- **Technical Control**: These controls are considered the most effective of all because they make use of the latest technologies and systems to limit access to information. Some of the examples of technical controls include firewalls, anti-virus software, file permissions, access control lists and cutting-edge data security technologies that are hard to penetrate.

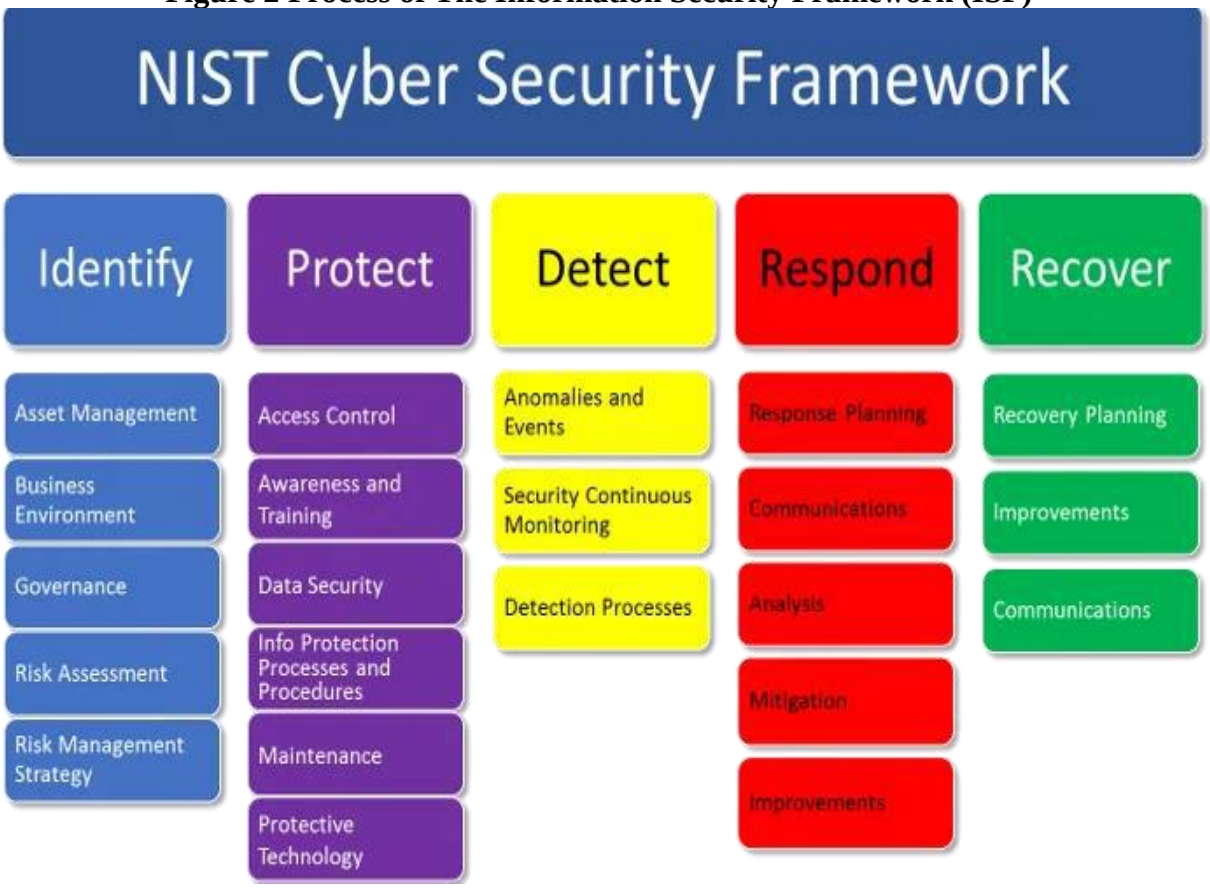
Establishing A Framework for Security and Control

The Information Security Framework (ISF) defines the approach, guiding principles, roles and responsibilities set forth by the organisation to manage an information security risk, in order to protect the information and information systems against loss of confidentiality, integrity and availability.

All technical, organizational and legal rules and measures aiming to ensure the security of information and information systems shall be guided by the Information Security Framework. The Information Security Framework applies to all information managed by the organisation and to all information systems managed or approved by organisation and used by internal staff, partners and beneficiaries.

Process of The Information Security Framework (ISF)

Figure 2 Process of The Information Security Framework (ISF)



As security of information and information systems are continuously evolving, with new systems, technologies, processes, vulnerabilities and threats, the internal staff responsible for managing information and information systems must establish clear processes to secure information and systems, assess and mitigate any risks to the extent possible.

Given the constantly evolving information security landscape, such processes must be reviewed on a regular basis and revised as necessary. Internal staff responsible for managing information and information systems must apply the following five core steps in a continuous process and cycle in any information and information systems management process:

Identify

"Identify" refers to the first step necessary to understand the business requirements and environment, as well as the risks, threats and vulnerabilities related to the management of information and information systems, in order to manage these risks. It is essential to understand risks in the context in which they arise, so that the most appropriate mitigation measures can be taken. To identify means to:

• Understand the business context, purpose and requirements of the different métiers to use or develop information systems, processes, capabilities or services;

• Identify the organisation's most critical information assets, and protect them in accordance with the level of risk they are exposed to;

• Undertake risk assessments on a regular basis in order to identify any risks and the appropriate legal, organizational and technical measures which must be taken in order to mitigate them.

Protect

"Protect" means implementing the appropriate safeguards to address the risks identified in step 1. This step of the information and systems management process must take into account four safeguards: protective technologies (e.g., antivirus software, firewalls), organizational aspects (e.g., information and systems security procedures, formalized responsibilities), legal safeguards (e.g., Headquarters Status Agreements, contracts with suppliers, etc.) and people (e.g., training, awareness-raising). These safeguards are implemented at different stages of the process:

• During the development of new projects, with controls at the project's gates;

• In response to specific initiatives and requests, such as innovation initiatives; or new processes involving internal data processing or data sharing with third parties;

• During normal operations and maintenance.

Detect

"Detect" refers to the appropriate activities required to identify the occurrence of an information security incident. It includes the use of technical means to detect a suspicious activity and an information security incident in a timely manner and understand the potential risks they pose. This step of the management process demands continuous monitoring of activities with appropriate processes and means (e.g., tools and resources) of detection.

Respond

"Respond" refers to all the appropriate activities to take following the detection of a security incident. It includes actions taken immediately to ensure timely response to detected security incidents and complementary activities such as communication (e.g., to inform relevant or

affected stakeholders including managers and staff, partners, beneficiaries and law agencies), analysis (to ensure the appropriateness of the response), mitigation measures (to limit impact), improvements (e.g., following a 'lessons learned' exercise).

Recover

"Recover" includes all necessary activities and recovery plans to restore in a timely manner any capability or services that were impaired due to a security incident. In addition to recovery processes, improvements and communications may be also be appropriate.

Tools for Information Security or Tools for Protecting Information Resources

In order to ensure the confidentiality, integrity, and availability of information, organizations can choose from a variety of tools. Each of these tools can be utilized as part of an overall information-security policy, which will be discussed in the next section.

Authentication

The authentication is done by confirming something that the user knows (their ID and password). But this form of authentication is easy to compromise and stronger forms of authentication are sometimes needed. Identifying someone only by something they have, such as a key or a card, can also be problematic. When that identifying token is lost or stolen, the identity can be easily stolen. The final factor, something you are, is much harder to compromise. This factor identifies a user through the use of a physical characteristic, such as an eye-scan or fingerprint. Identifying someone through their physical characteristics is called biometrics.

Access Control

Once a user has been authenticated, the next step is to ensure that they can only access the information resources that are appropriate. This is done through the use of access control. Access control determines which users are authorized to read, modify, add, and/or delete information. Several different access control models exist. Access control can be performed by the access control list (ACL) and role-based access control (RBAC).

For each information resource that an organization wishes to manage, a list of users who have the ability to take specific actions can be created. This is an access control list, or ACL. For each user, specific capabilities are assigned, such as *read*, *write*, *delete*, or *add*. Only users

with those capabilities are allowed to perform those functions. If a user is not on the list, they have no ability to even know that the information resource exists.

Encryption

Many times, an organization needs to transmit information over the Internet or transfer it on external media such as a CD or flash drive. In these cases, even with proper authentication and access control, it is possible for an unauthorized person to get access to the data. Encryption is a process of encoding data upon its transmission or storage so that only authorized individuals can read it. This encoding is accomplished by a computer program, which encodes the plain text that needs to be transmitted; then the recipient receives the cipher text and decodes it (decryption). In order for this to work, the sender and receiver need to agree on the method of encoding so that both parties can communicate properly. Both parties share the encryption key, enabling them to encode and decode each other's messages. This is called symmetric key encryption. This type of encryption is problematic because the key is available in two different places.

An alternative to symmetric key encryption is public key encryption. In public key encryption, two keys are used: a public key and a private key. To send an encrypted message, you obtain the public key, encode the message, and send it. The recipient then uses the private key to decode it. The public key can be given to anyone who wishes to send the recipient a message. Each user simply needs one private key and one public key in order to secure messages. The private key is necessary in order to decrypt something sent with the public key.

Backups

Another essential tool for information security is a comprehensive backup plan for the entire organization. Not only should the data on the corporate servers be backed up, but individual computers used throughout the organization should also be backed up. A good backup plan should consist of several components.

Firewalls

Another method that an organization should use to increase security on its network is a firewall. A firewall can exist as hardware or software (or both). A hardware firewall is a device that is connected to the network and filters the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they arrive to a

computer. A firewall protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria. A firewall may also be configured to restrict the flow of packets leaving the organization.

Intrusion Detection Systems

Another device that can be placed on the network for security purposes is an intrusion detection system, or IDS. An IDS does not add any additional security; instead, it provides the functionality to identify if the network is being attacked. An IDS can be configured to watch for specific types of activities and then alert security personnel if that activity occurs. An IDS also can log various types of traffic on the network for analysis later. An IDS is an essential part of any good security setup.

Physical Security

An organization can implement the best authentication scheme in the world, develop the best access control, and install firewalls and intrusion prevention, but its security cannot be complete without implementation of physical security. Physical security is the protection of the actual hardware and networking components that store and transmit information resources. To implement physical security, an organization must identify all of the vulnerable resources and take measures to ensure that these resources cannot be physically tampered with or stolen.

Security Policies

Besides the technical controls listed above, organizations also need to implement security policies as a form of administrative control. In fact, these policies should really be a starting point in developing an overall security plan. A good information-security policy lays out the guidelines for employee use of the information resources of the company and provides the company recourse in the case that an employee violates a policy.

VULNERABILITY

In computer security, a **vulnerability** is a weakness which can be exploited by a Threat Actor, such as an attacker, to perform unauthorised actions within a computer system. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems.

A security risk is often incorrectly classified as a vulnerability. The use of vulnerability with the same meaning of risk can lead to confusion. The risk is the potential of a significant impact resulting from the exploit of a vulnerability. Then there are vulnerabilities without risk: for example, when the affected asset has no value. A vulnerability with one or more known instances of working and fully implemented attacks is classified as an exploitable vulnerability—a vulnerability for which an exploit exists. The **window of vulnerability** is the time from when the security hole was introduced or manifested in deployed software, to when access was removed, a security fix was available/deployed, or the attacker was disabled—see zero-day attack.

Security bug (security defect) is a narrower concept: there are vulnerabilities that are not related to software: hardware, site, personnel vulnerabilities are examples of vulnerabilities that are not software security bugs.

Constructs in programming languages that are difficult to use properly can be a large source of vulnerabilities.

Definitions

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Vulnerability—Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Features

1. A weakness in automated system security procedures, administrative controls, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

2. A weakness in system security procedures, hardware design, internal controls, etc., which could be exploited to gain unauthorized access to classified or sensitive information.
3. A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to the ADP system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow the ADP system or activity to be harmed by an attack.
4. An assertion primarily concerning entities of the internal environment (assets); we say that an asset (or class of assets) is vulnerable (in some way, possibly involving an agent or collection of agents); we write: V(i,e) where: e may be an empty set.
5. Susceptibility to various threats.
6. A set of properties of a specific internal entity that, in union with a set of properties of a specific external entity, implies a risk.
7. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.

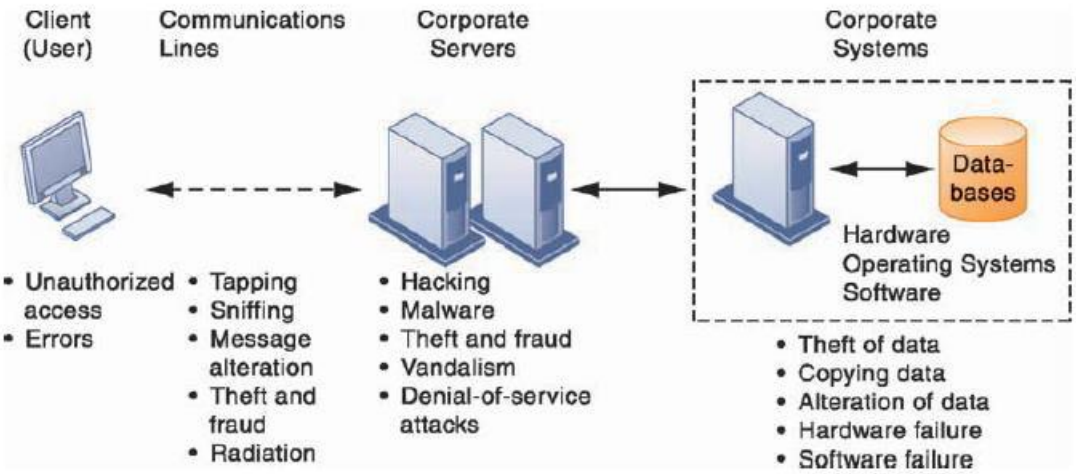
Vulnerability and Risk Factor Models

A resource (either physical or logical) may have one or more vulnerabilities that can be exploited by a threat agent in a threat action. The result can potentially compromise the confidentiality, integrity or availability of resources (not necessarily the vulnerable one) belonging to an organization and/or other parties involved (customers, suppliers). The so-called CIA triad is the basis of Information Security.

An attack can be *active* when it attempts to alter system resources or affect their operation, compromising integrity or availability. A "*passive attack*" attempts to learn or make use of information from the system but does not affect system resources, compromising confidentiality.

Classification Vulnerabilities

FIGURE 8.1 CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES



Vulnerabilities are classified according to the asset class they are related to:

Hardware

- susceptibility to humidity
- susceptibility to dust
- susceptibility to soiling
- susceptibility to unprotected storage

Software

- insufficient testing
- lack of audit trail
- design flaw

Network

- unprotected communication lines
- insecure network architecture

Personnel

- inadequate recruiting process
- inadequate security awareness

Physical Site

- area subject to flood
- unreliable power source

Organizational

- lack of regular audits
- lack of continuity plans
- lack of security

FIREWALL

a **firewall** is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

Firewalls are often categorized as either **network firewalls** or **host-based firewalls**. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

THE NEED FOR FIREWALLS

Information systems in corporations, government agencies, and other organizations have undergone a steady evolution. The following are notable developments:

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals
- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN)
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN

FIREWALL CHARACTERISTICS

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this chapter.
3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications

Techniques of Firewalls

1. Service control: Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.
2. Direction control: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
3. User control: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPsec
4. Behavior control: Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

TYPES OF FIREWALLS

A firewall may act as a packet filter. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. In this section, we look at the principal types of firewalls.

Packet Filtering Firewall A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.

The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- Source IP address: The IP address of the system that originated the IP packet (e.g., 192.178.1.1)
- Destination IP address: The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2) Source and destination transport-level address: The transport-level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET
- IP protocol field: Defines the transport protocol
- Interface: For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for

SYSTEMS AUDIT

An **information technology audit**, or **information systems audit**, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

IT audits are also known as "automated data processing (ADP) audits" and "computer audits". They were formerly called "electronic data processing (EDP) audits".

Definition

Information systems audit is a process to collect and evaluate evidence to determine whether the information systems safeguard assets, maintain data integrity, achieve organizational goals effectively and consume resources efficiently.

AIMS OF INFORMATION SYSTEM AUDIT

Auditing is a systematic and independent examination of information systems environment to ascertain whether the objectives, set out to be achieved, have been met or not. Auditing is also described as a continuous search for compliance. The objective of the IS audit is to identify risks that an organization is exposed to in the computerized environment. IS audit evaluating the adequacy of the security controls and informs the management with suitable conclusions and recommendations. IS audit being an independent subset of the normal audit

exercise. Information systems audit is an ongoing process of evaluating controls; suggest security measures for the purpose of safeguarding assets/resources, maintaining data integrity, improve system effectiveness and system efficiency for the purpose of attaining organization goals. Well-planned and structured audit is essential for risk management and monitoring and control of information systems in any organization.

Safeguarding IS assets

The Information systems assets of the organization must be protected by a system of internal controls. It includes protection of hardware, software, facilities, people, data, technology, system documentation and supplies. This is because hardware can be damaged maliciously, software and data files may be stolen, deleted or altered and supplies of negotiable forms can be used for unauthorized purposes. The IS auditor will be requiring to review the physical security over the facilities, the security over the systems software and the adequacy of the internal controls. The IT facilities must be protected against all hazards. The hazards can be accidental hazards or intentional hazards.

Maintenance of Data Integrity

a) **Data integrity** includes the safeguarding of the information against unauthorized addition, deletion, modification or alteration. The desired features of the data are described here under:
b) **Accuracy:** Data should be accurate. Inaccurate data may lead to wrong decisions and thereby hindering the business development process.
c) **Confidentiality:** Information should not lose its confidentiality. It should be protected from being read or copied by anyone who is not authorized to do so.
d) **Completeness:** Data should be complete
e) **Reliability:** Data should be reliable because all business decision is taken on the basis of the current database.
f) **Efficiency:** The ratio of the output to the input is known as efficiency. If output is more with the same or less actual input, system efficiency is achieved, or else system is inefficient. If computerization results in the degradation of efficiency, the effort for making the process automated stands defeated. IS auditors are responsible to examine how efficient the application in relation to the users and workload.

Types of IT audits

Various authorities have created differing taxonomies to distinguish the various types of IT audits. Goodman & Lawless state that there are three specific systematic approaches to carry out an IT audit:

- **Technological innovation process audit**. This audit constructs a risk profile for existing and new projects. The audit will assess the length and depth of the company's experience in its chosen technologies, as well as its presence in relevant markets, the organization of each project, and the structure of the portion of the industry that deals with this project or product, organization and industry structure.
- **Innovative comparison audit.** This audit is an analysis of the innovative abilities of the company being audited, in comparison to its competitors. This requires examination of company's research and development facilities, as well as its track record in actually producing new products.
- **Technological position audit**: This audit reviews the technologies that the business currently has and that it needs to add. Technologies are characterized as being either "base", "key", "pacing" or "emerging".

Others describe the spectrum of IT audits with five categories of audits:

- **Systems and Applications**: An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity. System and process assurance audits form a subtype, focusing on business process-centric business IT systems. Such audits have the objective to assist financial auditors.
- **Information Processing Facilities**: An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.
- **Systems Development**: An audit to verify that the systems under development meet the objectives of the organization, and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
- **Management of IT and Enterprise Architecture**: An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

- **Client/Server, Telecommunications, Intranets, and Extranets**: An audit to verify that telecommunications controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

IT Audit process

The following are basic steps in performing the Information Technology Audit Process

1. Planning
2. Studying and Evaluating Controls
3. Testing and Evaluating Controls
4. Reporting
5. Follow-up
6. Reports

System Security

Information security means protecting information (data) and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Information Security management is a process of defining the security controls in order to protect the information assets.

Security of an Information System

Information system security refers to the way the system is defended against unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

There are two major aspects of information system security:

- Security of the information technology used - securing the system from malicious cyber-attacks that tend to break into the system and to access critical private information or gain control of the internal systems.
- Security of data - ensuring the integrity of data when critical issues, arise such as natural disasters, computer/server malfunction, physical theft etc. Generally, an off-site backup of data is kept for such problems.

Guaranteeing effective information security has the following key aspects:

- Preventing the unauthorized individuals or systems from accessing the information.
- Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

- Ensuring that the computing systems, the security controls used to protect it and the communication channels used to access it, functioning correctly all the time, thus making information available in all situations.
- Ensuring that the data, transactions, communications or documents are genuine.
- Ensuring the integrity of a transaction by validating that both parties involved are genuine, by incorporating authentication features such as "digital signatures".
- Ensuring that once a transaction takes place, none of the parties can deny it, either having received a transaction, or having sent a transaction. This is called 'non-repudiation'.
- Safeguarding data and communications stored and shared in network systems.

COMPUTER SECURITY RISK

A **computer security risk** is really anything on your computer that may damage or steal your data or allow someone else to access your computer, without your knowledge or consent. There are a lot of different things that can create a computer risk, including **malware**, a general term used to describe many types of bad software. We commonly think of computer viruses, but, there are several types of bad software that can create a computer security risk, including viruses, worms, ransomware, spyware, and Trojan horses. Misconfiguration of computer products as well as unsafe computing habits also pose risks.

However, this computer security is threatened by many risks and dangers, which are called computer security risks. Those are “any event or action that could cause a loss or damage the computer hardware, software, data, or information.

SECURITY THREADS

A computer system threat is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure. Knowing how to identify computer security threats is the first step in protecting computer systems. The threats could be intentional, accidental or caused by natural disasters.

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack. In these tutorial series,

we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.

Physical Threats

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

The following list classifies the physical threats into three (3) main categories;

- **Internal**: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- **External**: These threats include Lightning, floods, earthquakes, etc.
- **Human**: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

To protect computer systems from the above mentioned physical threats, an organization must have physical security control measures.

The following list shows some of the possible measures that can be taken:

- **Internal**: Fire threats could be prevented by the use of automatic fire detectors and extinguishers that do not use water to put out a fire. The unstable power supply can be prevented by the use of voltage controllers. An air conditioner can be used to control the humidity in the computer room.
- **External**: Lightning protection systems can be used to protect computer systems against such attacks. Lightning protection systems are not 100% perfect, but to a certain extent, they reduce the chances of Lightning causing damage. Housing computer systems in high lands are one of the possible ways of protecting systems against floods.
- **Humans**: Threats such as theft can be prevented by use of locked doors and restricted access to computer rooms.

Non-physical threats

A non-physical threat is a potential cause of an incident that may result in;

- Loss or corruption of system data

- Disrupt business operations that rely on computer systems
- Loss of sensitive information
- Illegal monitoring of activities on computer systems
- Cyber Security Breaches
- Others

The non-physical threats are also known as logical threats. The following list is the common types of non-physical threats;

- Virus
- Trojans
- Worms
- Spyware
- Key loggers
- Adware
- Denial of Service Attacks
- Distributed Denial of Service Attacks
- Unauthorized access to computer systems resources such as data
- Phishing
- Other Computer Security Risks

To protect computer systems from the above-mentioned threats, an organization must have **logical security measures** in place. The following list shows some of the possible measures that can be taken to protect cyber security threats.

To protect against viruses, Trojans, worms, etc. an organization can use anti-virus software. In additional to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visiting the website that is most likely to download unauthorized programs onto the user's computer.

Unauthorized access to computer system resources can be prevented by the use of authentication methods. The authentication methods can be, in the form of user ids and strong passwords, smart cards or biometric, etc.

Intrusion-detection/prevention systems can be used to protect against denial of service attacks. There are other measures too that can be put in place to avoid denial of service attacks.

COMPUTER VIRUS

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.

A computer virus is a rogue software program that attaches itself to other software programs or data files in order 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 in order 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.

Hackers can do to a smartphone just about anything they can do to any Internet device: request malicious files without user intervention, delete files, transmit files, install programs running in the background to monitor user actions, and potentially convert the smartphone into a robot in a botnet to send e-mail and text messages to anyone.

With smartphones starting to outsell PCs, and smartphones increasingly used as payment devices, they are becoming a major avenue for malware.

Malware targeting mobile devices is not yet as extensive as that targeting larger computers, but nonetheless is spreading using e-mail, text messages, Bluetooth, and file downloads from the Web via Wi-Fi or cellular networks.

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.

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 and crackers gain unauthorized access by finding weaknesses in the security protections employed by Web sites and computer systems, 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 **cyber-vandalism**, the intentional disruption, defacement, or even destruction of a Web site 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** also may involve redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination.

A **sniffer** is a type of eavesdropping program that monitors information traveling over a network. When used legitimately, sniffers help identifies 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.

Identity Theft

With the growth of the Internet and electronic commerce, identity theft has become especially troubling. **Identity theft** is a crime in which an imposter obtains key pieces of personal information, such as social security identification 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.

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

phishing.

Phishing involves setting up fake Web sites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data. The e-mail message instructs recipients to update or confirm records by providing social security numbers, bank and credit card information, and other confidential data either by responding to the e-mail message, by entering the information at a bogus Web site, or by calling a telephone number.

Pharming

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 stored by Internet service providers 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

Click fraud occurs when an individual or computer program fraudulently clicks on 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 Web sites that feature pay-per-click online advertising.