# INTRODUCTION

## DEFINITION OF TERMS

**ICT Security** is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable.

Security rests on **confidentiality**, **integrity**, and **availability**.

**Computer security** aims to protect a single, connected, machine.

**Network security** aims to protect the communication and all its participants.

A **threat** is a potential violation of security e.g. Flaws in design, implementation, and operation.

An **attack** is any action that violates security i.e. Active adversary.

An attack has an implicit concept of **“intent”** e.g. Router mis-configuration or server crash can also cause loss of availability, but they are not attacks.

A **vulnerability** is a bug in the software that creates unexpected computer behaviour when exploited, such as enabling access without login, running unauthorized code or crashing the computer.

An **exploit** is an input to the buggy program that makes use of the existing vulnerability.

## SECURITY ATTACKS, SERVICES AND MECHANISMS

To assess the security needs of an organization effectively, the manager responsible for **security needs** some systematic way of **defining the requirements for security and characterization of approaches to satisfy those requirements**. One approach is to consider three aspects of information security:

**Security attack** – Any **action that compromises** the security of information owned by an organization.

**Security mechanism** – A **mechanism that is designed to detect, prevent or recover** from a security attack.

**Security service** – A **service that enhances the security of the data processing systems** and the **information transfers of an organization**. The **services are intended to counter security attacks** and they make use of **one or more security mechanisms** to provide the service.

## SECURITY SERVICES

The classification of security services are as follows:

**Confidentiality:** Ensures that the information in a computer system and transmitted information are **accessible only for reading by authorized parties.** E.g. Printing, displaying and other forms of disclosure.

**Authentication:** Ensures that the **origin of a message or electronic document is correctly identified**, with an assurance that the identity is not false.

**Integrity:** Ensures that **only authorized parties are able to modify computer system assets and transmitted information**. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

**Non-repudiation**: Requires that neither the **sender nor the receiver of a message be able to deny the transmission.**

**Access control**: Requires that access to information resources may be controlled by or the target system.

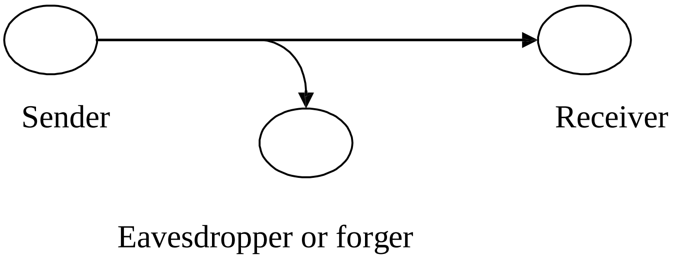
**Availability**: Requires that computer system assets be available to authorized parties when needed.

## SECURITY ATTACKS

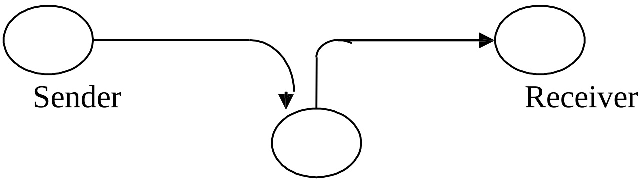
There are four general categories of attack, which are listed below.

**Interruption:** An asset of the system is **destroyed or becomes unavailable or unusable**. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

**Interception:** An **unauthorized party gains access to an asset**. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer. e.g., wiretapping to capture data in the network, illicit copying of files.

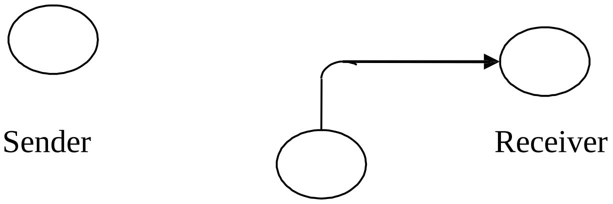


**Modification**: An **unauthorized party not only gains access to but also tampers with an asset**. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



Eavesdropper or forger

**Fabrication: An unauthorized party inserts counterfeit objects into the system**. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file



Eavesdropper or forger

## SECURITY MECHANISMS

**Security mechanisms** implement functions that help **prevent**, **detect**, and **respond** to recovery from security attacks. Examples include Encryption, Checksums, Key management, Authentication, Authorization, Accounting, Firewalls, VPNs, Intrusion Detection, Intrusion Response, Virus scanners, Policy managers, Trusted hardware etc.

## SECURITY GOALS

The objective of ICT security is to protect information from being stolen, compromised or attacked. At least one of three goals-can measure ICT security:

1. Protect the **confidentiality** of data.
2. Preserve the **integrity** of data.
3. Promote the **availability** of data for authorized users.

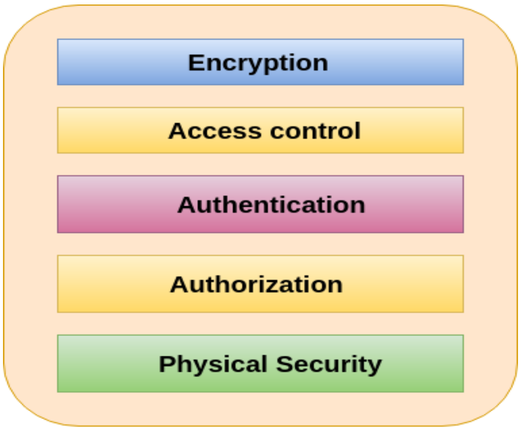
These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs. The CIA triad is a security model that is designed to guide policies for information security within the premises of an organization or company. This model is also referred to as the **AIC (Availability, Integrity, and Confidentiality)** triad to avoid the confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

The CIA criteria are one that most of the organizations and companies use when they have installed a new application, creates a database or when guaranteeing access to some data. For data to be completely secure, all of these security goals must come into effect. These are security policies that all work together, and therefore it can be wrong to overlook one policy.

**Confidentiality**

Confidentiality is roughly equivalent to privacy and avoids the unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content. It prevents essential information from reaching the wrong people while making sure that the right people can get it. Data encryption is a good example to ensure confidentiality.

Tools for Confidentiality



Confidentiality Tools

1 Encryption

Encryption is a method of transforming information to make it unreadable for unauthorized users by using an algorithm. The transformation of data uses a secret key (an encryption key) so that the transformed data can only be read by using another secret key (decryption key). It protects sensitive data such as credit card numbers by encoding and transforming data into unreadable cipher text. This encrypted data can only be read by decrypting it. Asymmetric-key and symmetric-key are the two primary types of encryption.

## 2 Access control

Access control defines rules and policies for limiting access to a system or to physical or virtual resources. It is a process by which users are granted access and certain privileges to systems, resources or information. In access control systems, users need to present credentials before they can be granted access such as a person's name or a computer's serial number. In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security.

## 3 Authentication

An authentication is a process that ensures and confirms a user's identity or role that someone has. It can be done in a number of different ways, but it is usually based on a combination of-

- something the person has (like a smart card or a radio key for storing secret keys),
- something the person knows (like a password),
- Something the person is (like a human with a fingerprint).

Authentication is the necessity of every organizations because it enables organizations to keep their networks secure by permitting only authenticated users to access its protected resources. These resources may include computer systems, networks, databases, websites and other network-based applications or services.

## 4 Authorization

Authorization is a security mechanism, which gives permission to do or have something. It is used to determine a person or system is allowed access to resources, based on an access control policy, including computer programs, files, services, data and application features. It is normally preceded by authentication for user identity verification. System administrators are typically assigned permission levels covering all system and user resources. During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

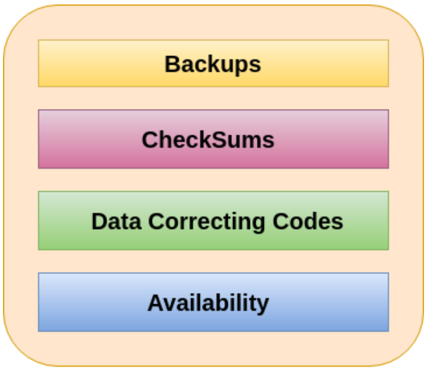
5 Physical Security

Physical security describes measures designed to deny the unauthorized access of IT assets like facilities, equipment, personnel, resources and other properties from damage. It protects these assets from physical threats including theft, vandalism, fire and natural disasters.

## Integrity

Integrity refers to the methods for ensuring that data is real, accurate and safeguarded from unauthorized user modification. It is the property that information has not be altered in an unauthorized way, and that source of the information is genuine.

## Tools for Integrity



Integrity Tools

1 Backups

Backup is the periodic archiving of data. It is a process of making copies of data or data files to use in the event when the original data or data files are lost or destroyed. It is also used to make copies for historical purposes, such as for longitudinal studies, statistics or for historical records or to meet the requirements of a data retention policy. Many applications especially in a Windows environment produce backup files using the .BAK file extension.

2 Checksums

A checksum is a numerical value used to verify the integrity of a file or a data transfer. In other words, it is the computation of a function that maps the contents of a file to a numerical value. They are typically used to compare two sets of data to make sure that they are the same. A checksum function depends on the entire contents of a file. It is designed in a way that even a small change to the input file (such as flipping a single bit) likely to results in different output value.

3 Data Correcting Codes

It is a method for storing data in such a way that small changes can be easily detected and automatically corrected.

**Availability**

Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Tools for Availability

- Physical Protections
- Computational Redundancies

1 Physical Protections

Physical safeguard means to keep information available even in the event of physical challenges. It ensure sensitive information and critical information technology are housed in secure areas.

2 Computational redundancies

It is applied as fault tolerant against accidental faults. It protects computers and storage devices that serve as fallbacks in the case of failures.

# IDENTIFY SECURITY THREATS

## DEFINITION OF SECURITY THREATS

A **threat**, in the context of **computer security**, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

## CATEGORIES OF SECURITY THREATS

An **internal threat** is a threat originating inside a company, government agency, or institution, and typically an exploit by a disgruntled employee denied promotion or informed of employment termination. An attacker who has sought temporary employment with a target and uses social engineering skills to get on the inside also can launch such exploits.

**External threat**, originate outside a company, government agency, or institution. In contrast, an internal threat is one originating inside the organization typically by an employee or "insider."

## IMPORTANCE OF COMPUTER SECURITY TO AN ORGANIZATION

**To protect company's assets:** This can be considered as the primary goal of securing the computers and computer networks. The assets mean the information that is stored in the computer networks, which are as crucial and valuable as the tangible assets of the company. The computer and network security is concerned with the integrity, protection and safe access of the confidential information. It also involves the accessibility of information in a meaningful manner.

**To comply with regulatory requirements and ethical responsibilities:** It is the responsibility of every organization to develop procedures and policies addressing the security requirements of every organization. These policies work for the safety and security of any organization and are compulsory for any organization working on computers. Protection of company's assets would mean that it is protected from liability addressing to the ethical responsibilities of an organization.

**For competitive advantage:** Developing an effective security system for networks will give the organization a competitive edge. In the arena of Internet financial services and ecommerce, network security assumes prime importance. The customers would avail the services of Internet banking only if the networks are secured.

Read: Importance of ICT security to an organization: https://www.avalan.com/blog/bid/385189/Importance-Of-Network-Security-For-Business-Organization

## IDENTIFICATION OF COMMON THREATS

It is important to identify and appropriately manage common threats to an organization.

**Fraud and theft** have a lot in common. Both are criminal acts, and both are forcibly taking something from others without asking permission. Both are all about stealing and both are bad things. Read: Difference between fraud and theft: http://www.differencebetween.net/miscellaneous/difference-between-fraud-and-theft/#ixzz5qRVXtQ00

**Employee sabotage**: Employees are most familiar with their employer's computers and applications, this include knowing what actions might cause the most damage, mischief, or sabotage.

**The loss of supporting infrastructure** includes power failures (outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes.

The term **malicious hackers**, sometimes called crackers, refer to those who break into computers without authorization. They can include both outsiders and insiders. Much of the rise of hacker activity is often attributed to increases in connectivity in both government and industry.

**Malicious code** refers to viruses, worms, Trojan horses, logic bombs, and other "uninvited" software. Sometimes mistakenly associated only with personal computers, malicious code can attack other platforms.

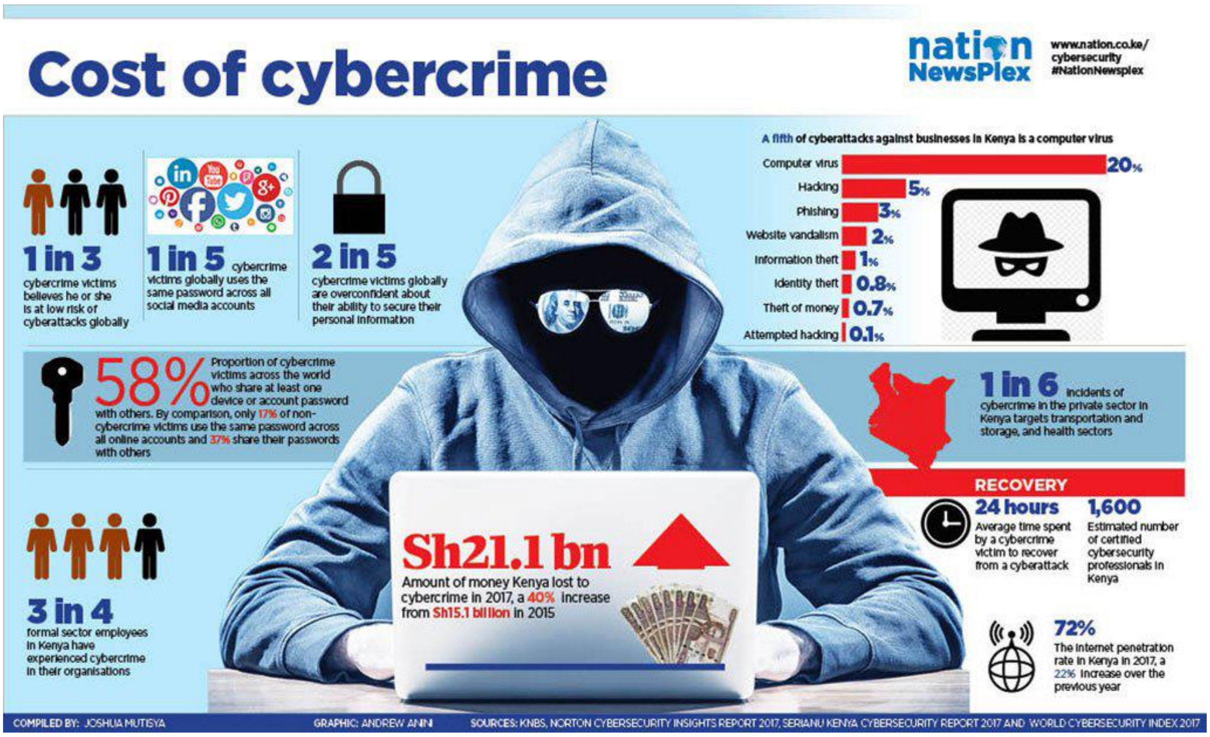
**Industrial espionage** is the act of gathering proprietary data from private companies or the government for the purpose of aiding another company(ies). Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries.

**Threats to personal privacy:** The accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies, combined with the ability of computers to monitor, process, and aggregate large amounts of information about individuals have created a threat to individual privacy.

**Natural calamities**, such as earthquakes, floods and hurricanes, can damage computer. Fires, extreme temperatures and lightning strikes can cause major physical damage and lead to loss of data.

**Cybercrime**, or computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

### Cybercrime in Kenya



Cost of cybercrime

nation NewsPlex www.nation.co.ke/cybersecurity #NationNewsplex

1 in 3 cybercrime victims believes he or she is at low risk of cyberattacks globally

1 in 5 cybercrime victims globally uses the same password across all social media accounts

2 in 5 cybercrime victims globally are overconfident about their ability to secure their personal information

58% Proportion of cybercrime victims across the world who share at least one device or account password with others. By comparison, only 17% of non-cybercrime victims use the same password across all online accounts and 37% share their passwords with others

3 in 4 formal sector employees in Kenya have experienced cybercrime in their organisations

Sh21.1 bn Amount of money Kenya lost to cybercrime in 2017, a 40% increase from Sh15.1 billion in 2015

A fifth of cyberattacks against businesses in Kenya is a computer virus

| | |
|---|---|
| Computer virus | 20% |
| Hacking | 5% |
| Phishing | 3% |
| Website vandalism | 2% |
| Information theft | 1% |
| Identity theft | 0.8% |
| Theft of money | 0.7% |
| Attempted hacking | 0.1% |

1 in 6 incidents of cybercrime in the private sector in Kenya targets transportation and storage, and health sectors

RECOVERY

24 hours Average time spent by a cybercrime victim to recover from a cyberattack

1,600 Estimated number of certified cybersecurity professionals in Kenya

72% The internet penetration rate in Kenya in 2017, a 22% increase over the previous year

COMPILED BY: JOSHUA MUTISYA GRAPHIC: ANDREW ANIN SOURCES: KNBS, NORTON CYBERSECURITY INSIGHTS REPORT 2017, SERIANU KENYA CYBERSECURITY REPORT 2017 AND WORLD CYBERSECURITY INDEX 2017

### Case studies - Cyber Crime around the world

### Wanna Cry virus hits the NHS, 2017

The most widespread cyber-attack ever, hackers managed to gain access to the NHS' computer system in mid-2017, causes chaos among the UK's medical system. The same hacking tools were used to attack worldwide freight company FedEx and infected computers in 150 countries. Ransomware affectionately named "WannaCry" was delivered via email in the form of an attachment. Once a user clicked on the attachment, the virus was spread through their computer, locking up all of their files and demanding money before they could be accessed again. As many as 300,000 computers were infected with the virus. It was only stopped when a 22-year-old security researcher from Devon managed to find the kill switch, after the NHS had been down for a number of days.

### JP and Morgan Chase & Co target of giant hacking conglomerate, 2015

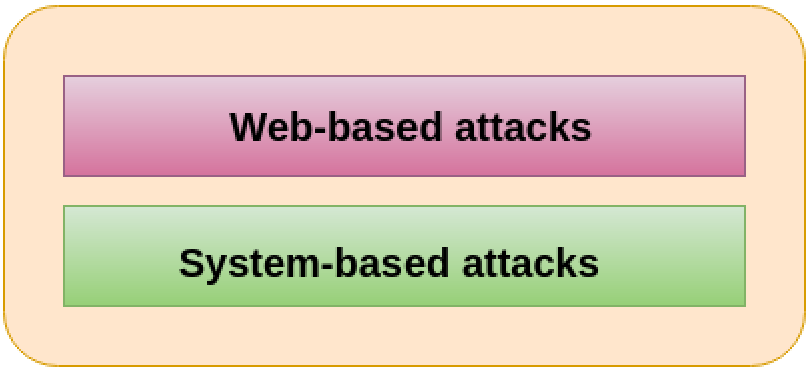
Late in 2015, three men were charged with stealing data from millions of people around the world, as part of a hacking conglomerate that spanned the best part of a decade. The group stole information from more than 83 million customers from JP Morgan alone, and are thought to have made hundred of millions of dollars in illegal profits. Along with personal data, the hacking group also stole information related to company performance and news, which allowed them to manipulate stock prices and make enormous financial gain.

### Sony Pictures crippled by GOP hackers, 2014

In late 2014, major entertainment company Sony Pictures were hit with a crippling virus. Cybercrime group Guardians of Peace (GOP) were behind the apparent blackmail attempt, which saw around 100 terabytes of sensitive data stolen from the company. One billion user accounts stolen from Yahoo, 2013 In one of the largest cases of data theft in history, Yahoo had information from more than one billion user accounts stolen in 2013. Personal information including names, phone numbers, passwords and email addresses were taken from the Internet giant.

### Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.



Classification of Cyber attacks

**Web-based attacks**

These are the attacks, which occur on a website or web applications. Some of the important web-based attacks are as follows-

**1. Injection attacks**

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

**Example-** SQL Injection, code Injection, log Injection, XML Injection etc.

**2. DNS Spoofing**

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

**3. Session Hijacking**

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

**4. Phishing**

Phishing is a type of attack, which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

### 5. Brute force

It is a type of attack, which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

### 6. Denial of Service

It is an attack, which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

> **Volume-based attacks-** Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
>
> **Protocol attacks-** It consumes actual server resources, and is measured in a packet.
>
> **Application layer attacks-** Its goal is to crash the web server and is measured in request per second.

### 7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

### 8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

### 9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

### 10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

### System-based attacks

These are the attacks, which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

#### 1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

#### 2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

#### 3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

#### 4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

#### 5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

**CAT ONE**

i. What is the difference between fraud and theft?

ii. Differentiate internal and external threats?

iii. What is hacking?

iv. What is malicious?

v. Differentiate hacking and cybercrime?

vi. Case situation: One of your friend's social media accounts has been hacked. What will you do to help him?

vii. Review various risks associated with computer security and make a detail report on how to address them.

viii. What are the training contents you will consider for helping community understand the security treats related to cyber security?

ix. Case situation: You are working as a consultant to a Financial Auditing firm. They want you to evaluate their employee contract and ensure that there are strict rules against cybercrime. What will be your suggestions? They also want you to improvise their security. They are a financial audit firm and they need to ensure security of all their client data.

x. Which of the following are forms of malicious attack?

   a. Theft of information
   b. Modification of data
   c. Wiping of information
   d. All of the mentioned

xi. What are common security threats?

   a. File Shredding
   b. File sharing and permission
   c. File corrupting
   d. File integrity

xii. What is not a good practice for user administration?

   a. Isolating a system after a compromise
   b. Perform random auditing procedures
   c. Granting privileges on a per host basis
   d. Using telnet and FTP for remote access

xiii. Why would a hacker use a proxy server?

a. To create a stronger connection with the target.
b. To create a ghost server on the network.
c. To obtain a remote access connection.
d. To hide malicious activity on the network.

xiv. Conduct secondary analysis and share in-group discussion regarding challenges of data hacking on social media site. (To be discussed in class)

## CONSTRAINTS TO COMPUTER SECURITY

**i.** **User responsibility:** Use computer and information systems in an ethical and legal manner. Agree not to duplicate or use copyrighted or proprietary software without proper authorization.

ii. **The challenge of integration** between physical and cyber security creates a number of challenges. First, no single system exists to confirm a person's identity because each functional security department controls its own identity database. Second, the lack of integration increases the potential for theft.

**iii.** **Cost**

**iv.** **Inadequate Assessment**

## Challenges of ICT security:

i. Your security frequently depends on others i.e. **Tragedy of commons.**

ii. **A good solution must:** Handle the problem to a great extent, Handle future variations of the problem too, Be inexpensive, Have economic incentive, Require a few deployment points, Require non-specific deployment points.

iii. **Fighting a live enemy**: Security is an adversarial field, No problem is likely to be completely solved, New advances lead to improvement of attack techniques, and Researchers must play a double game.

iv. **Attack patterns change**

v. **Often there is scarce attack data**

vi. T**esting security systems requires reproducing or simulating legitimate and traffic:** No agreement about realistic traffic patterns.

vii. **No agreement about metrics**

viii. **There is no standardized evaluation procedure**

**ix. Some security problems require a lot of resources to be reproduced realistically**

**Why we are not secure:**

i. Buggy code
ii. Protocol design failures
iii. Weak crypto
iv. Social engineering/human factor
v. Insider threats
vi. Poor configuration
vii. Incorrect policy specification
viii. Stolen keys or identities
ix. Misplaced incentives (DoS, spoofing, tragedy of commons)

## ESTABLISH AND INSTALL SECURITY MEASURES

**Risk** is the possibility of something adverse happening. **Risk management** is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Though perhaps not always aware of it, individuals manage risks every day. Actions as routine as buckling a car safety belt, carrying an umbrella when rain is forecast, or writing down a list of things to do rather than trusting to memory fall into the purview of risk management. People recognize various threats to their best interests and take precautions to guard against them or to minimize their effects. **Risk assessment and risk analysis** are concerned with placing an economic value on assets to best determine appropriate countermeasures that protect them from losses.

### Benefits of Risk Management

*As discussed in class.*

### Risk Management Procedures

i. **Risk assessment** is the process of analyzing and interpreting risk. **Risk assessment often produces an important side benefit** of in depth knowledge about system and an organization as risk analyst tries to figure out how system and functions are interrelated. It is comprised of three basic activities:

   **Determining the assessment's scope and methodology:** The first step in assessing risk is to identify the system under consideration, the part of the system that will be analysed, and the analytical method including its level of detail and formality. The assessment may be focused on certain areas where either the degree of risk is unknown or is known to be high. Different parts of a system may be analysed in greater or lesser detail. Defining the scope and boundary can help ensure a cost-effective assessment.

   **Collecting and analyzing data**: Risk has many different components: assets, threats, vulnerabilities, safeguards, consequences, and likelihood. This examination normally includes gathering data about the threatened area and synthesizing and analyzing the information to make it useful.

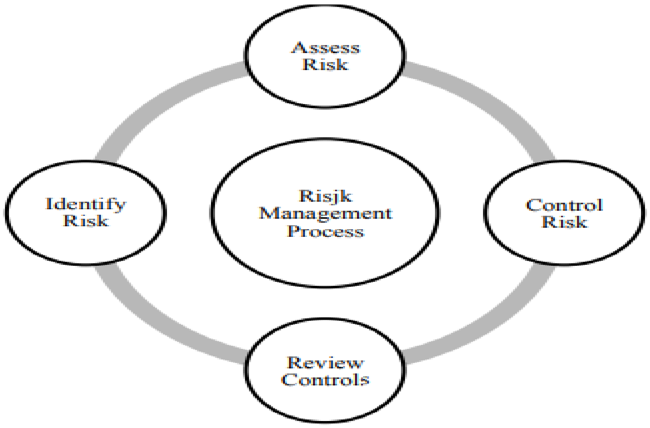
   **Interpreting the risk analysis results:** The risk assessment is used to support two related functions: the acceptance of risk and the selection of cost-effective controls. To accomplish these functions, the risk assessment must produce a meaningful output that reflects what is truly important to the organization.

ii. **Risk mitigation** involves the selection and implementation of security controls to reduce risk to a level acceptable to management, within applicable constraints. Although there is flexibility in how risk assessment is conducted, the sequence of identifying boundaries, analyzing input, and producing an output is quite natural. The process of risk mitigation has greater flexibility, and the sequence will differ more, depending on organizational culture and the purpose of the risk management activity.

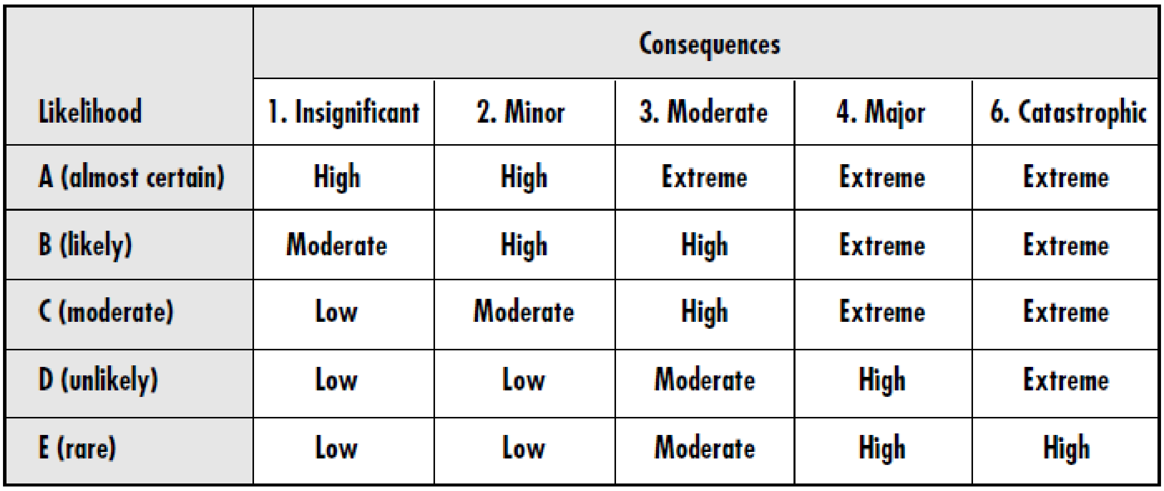
iii. **Uncertainty analysis:** Risk management often must rely on speculation, best guesses, incomplete data, and many unproven assumptions. The uncertainty analysis attempts to document this so that the risk management results can be used knowledgeably. There are two primary sources of uncertainty in the risk management process: (1) a lack of confidence or precision in the risk management model or methodology and (2) a lack of sufficient information to determine the exact value of the elements of the risk model, such as threat frequency, safeguard effectiveness, or consequences.

iv. **Interdependencies:** Risk management touches on every control. It is, however, most closely related to life cycle management and the security planning process. The requirement to perform risk management is often discussed in organizational policy and is an issue for organizational oversight.

v. **Cost considerations:** The goals of risk management should be kept in mind as a methodology is selected or developed. The methodology should concentrate on areas where identification of risk and the selection of cost-effective safeguards are needed. The cost of different methodologies can be significant. A "back-of-the-envelope" analysis or high-medium-low ranking can often provide all the information needed. However, especially for the selection of expensive safeguards or the analysis of systems with unknown consequences, more in-depth analysis may be warranted.



*Risk Management Process*



| | Consequences | | | | |
|---|---|---|---|---|---|
| Likelihood | 1. Insignificant | 2. Minor | 3. Moderate | 4. Major | 6. Catastrophic |
| A (almost certain) | High | High | Extreme | Extreme | Extreme |
| B (likely) | Moderate | High | High | Extreme | Extreme |
| C (moderate) | Low | Moderate | High | Extreme | Extreme |
| D (unlikely) | Low | Low | Moderate | High | Extreme |
| E (rare) | Low | Low | Moderate | High | High |

*Categorizing ICT threats according to risk impact.*

## TYPES OF SECURITY MEASURES

A **security measure** serves a purpose by **preventing a compromise**, **detecting that a compromise or compromise attempt** is underway, or **responding to a compromise** while it is happening or after it has been discovered, i.e. security controls are either **preventive**, **detective** or **responsive**. They include but not limited to:

i. **Firewalls:** Its main purpose is to control access to or from a protected network i.e. a site. It implements a network policy by forcing connections to pass through the firewall, where they can be examined and evaluated. Types of firewalls:

   a. **Packet filtering gateways:** use routers with packet filtering rules to grant or deny access based on source address, destination address and port.

   b. **Application gateways:** uses server programs called proxies that ran on the firewall. These proxies take external requests, examine them, and forward legitimate requests to the internal host that provides the appropriate service.

ii. **Intrusion detection system:** is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. IDS are classified into 5 types:

a. **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying cracking the firewall.

b. **Host intrusion detection systems (HIDS)** run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

c. **Protocol-based intrusion detection system (PIDS)** comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

d. **Application Protocol-based Intrusion Detection System (APIDS)** is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

e. **Hybrid intrusion detection system** is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

**Detection Methods of IDS:**

a. **Signature-based IDS** detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

b. **Anomaly-based IDS** was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

**Comparison of IDS with Firewalls:**

IDS and firewall both are related to the network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it do not signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

iii. **User accounts control** refers to the management of user accounts, particularly those with special access privileges, to protect against misuse and unauthorized access. Accounts should be assigned only to authorised individuals and provide the minimum level of access to applications, computers and networks.

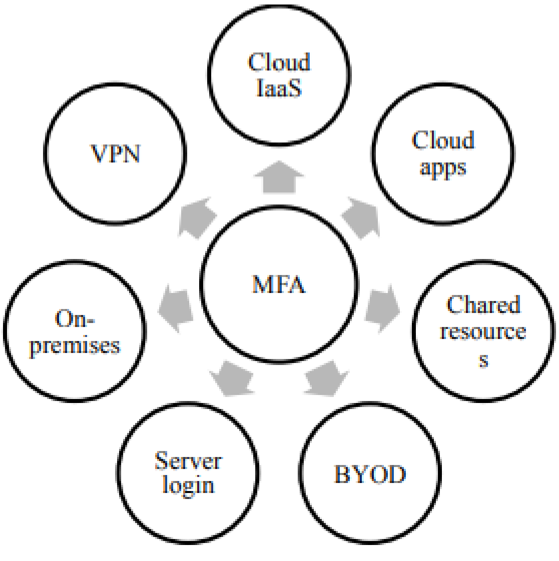
iv. **ICT Security policies** refers to a document that has a set of rules enacted by an organization to ensure that all users or networks of the IT structure within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority. **Policy:** a statement of what is, and is not allowed. **Mechanism:** a procedure, tool, or method of enforcing a policy.

v. **Antivirus,** also known as **anti-malware** is a computer program used to prevent, detect, and remove malware. Once installed, most antivirus software run automatically in the background to provide real-time protection against virus attacks.

vi. **Encryption** is the practice of hiding messages so that they cannot be read by anyone other than the intended recipient. Encryption schemes are largely classified as asymmetric and symmetric i.e. private key and public key encryption respectively.

vii. **Secure Socket Layer protocol (SSL)** is a standard protocol used for the secure transmission of documents over a network. Developed by Netscape, SSL technology creates a secure link between a Web server and browser to ensure private and integral data transmission. SSL uses Transport Control Protocol (TCP) for communication.

viii. **Multi-factor authentication** is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence. Two-factor authentication is a type, or subset, of multi-factor authentication.



*Multi-factor authentication (MFA)*

Watch: Introduction to multi-factor authentication: https://youtu.be/tFv101qURKE

ix. **Malware detection** focuses on detecting intrusions by monitoring the activity of systems and classifying it as normal or anomalous. Malware infection symptoms include strange emails, files that will not open, programs acting weird and pop-up.

Watch: Prevention and detection of malware: https://youtu.be/Ces7UeMQ7ic

x. **Site monitoring** is the process of testing and verifying that end-users can interact with a website or web application as expected. Website monitoring is often used by businesses to ensure website uptime, performance, and functionality is as expected.
Read: https://www.keycdn.com/blog/website-monitoring-tools
Watch: Introduction to site monitoring: https://youtu.be/Ufw6iuwm1rU

xi. **Daily or weekly backups:** Some common backup frequencies you'll see offered include continuous, once per minute, every x minutes (e.g. every 15 minutes), hourly, daily, weekly, monthly, and manually. Continuous backup means that the software is constantly backing up data.

## APPLICATION SECURITY MEASURES

**Application security** encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities. Application security issues include:

i. **Non-Malicious Programs Errors** i.e. buffer overflows, incomplete mediation, Time-of-check to Time-of-Use errors.
ii. **Malicious Code** i.e. Viruses and Worms.
iii. **Targeted Malicious Codes** i.e. Trapdoors, Salami Attack, Convert Channels.

### Controls against program threats:

i. Programming and process controls.
ii. OS controls.
iii. Administrative controls.