Risk Analysis & Threat

Topics Covered In This Presentation

TOPIC
○ Key Principles of Computer Security ○ Risk Analysis & it’s Process ○ Organizational Security Policies
○ Internal vs. External Threat ○ User Authentication - Biometrics ○ Data protection
○ Passwords ○ Computer Forensics ○ Incident Response Plan ○ Access Control

Key Principles of Computer Security

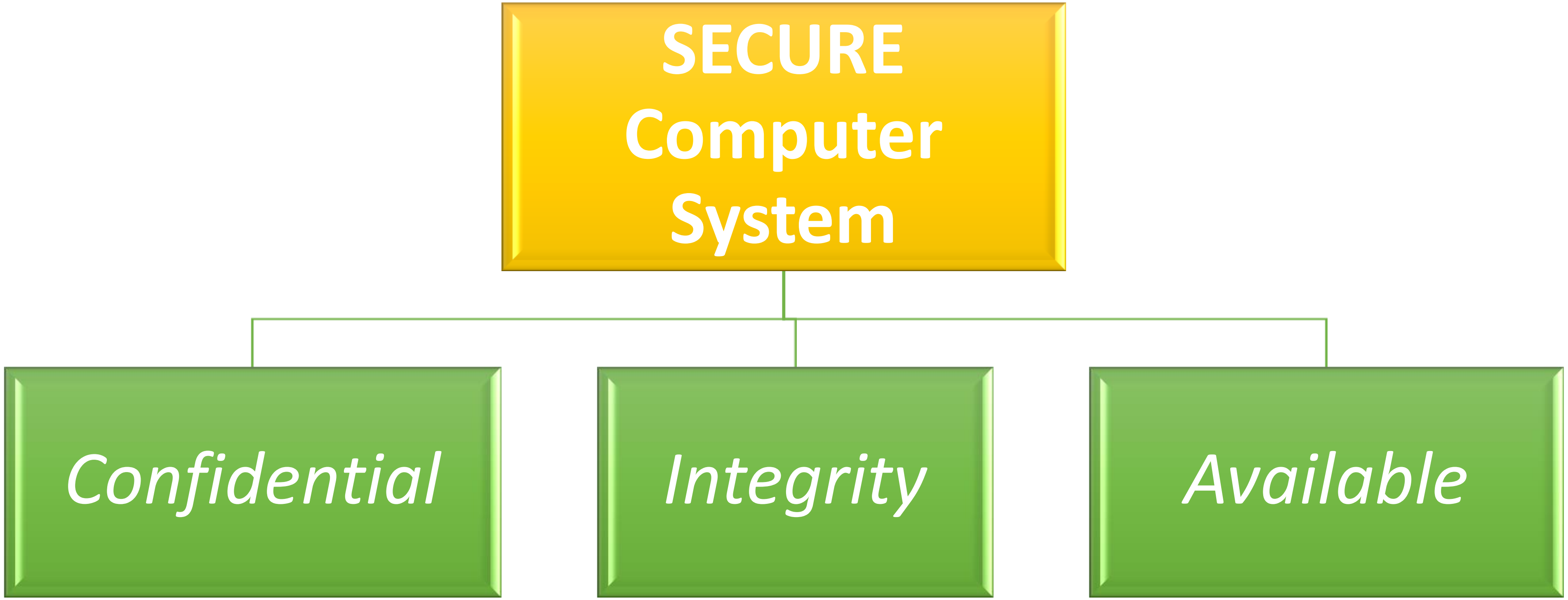
Why should there be computer security ?

Computer & related systems have both theoretical and real weaknesses. It is impossible to have a computer system that does not have any vulnerabilities.

The purpose of computer security is to devise ways to prevent the weaknesses from being exploited.

Security Goals

A secure computer system must have the following 3 important features.



SECURE Computer System

Confidential

Integrity

Available

Confidentiality

- Also called secrecy or privacy.
- Computer related assets should be accessed only by authorized parties.
- Access = to view, to print, to simply know an asset exists.

Integrity

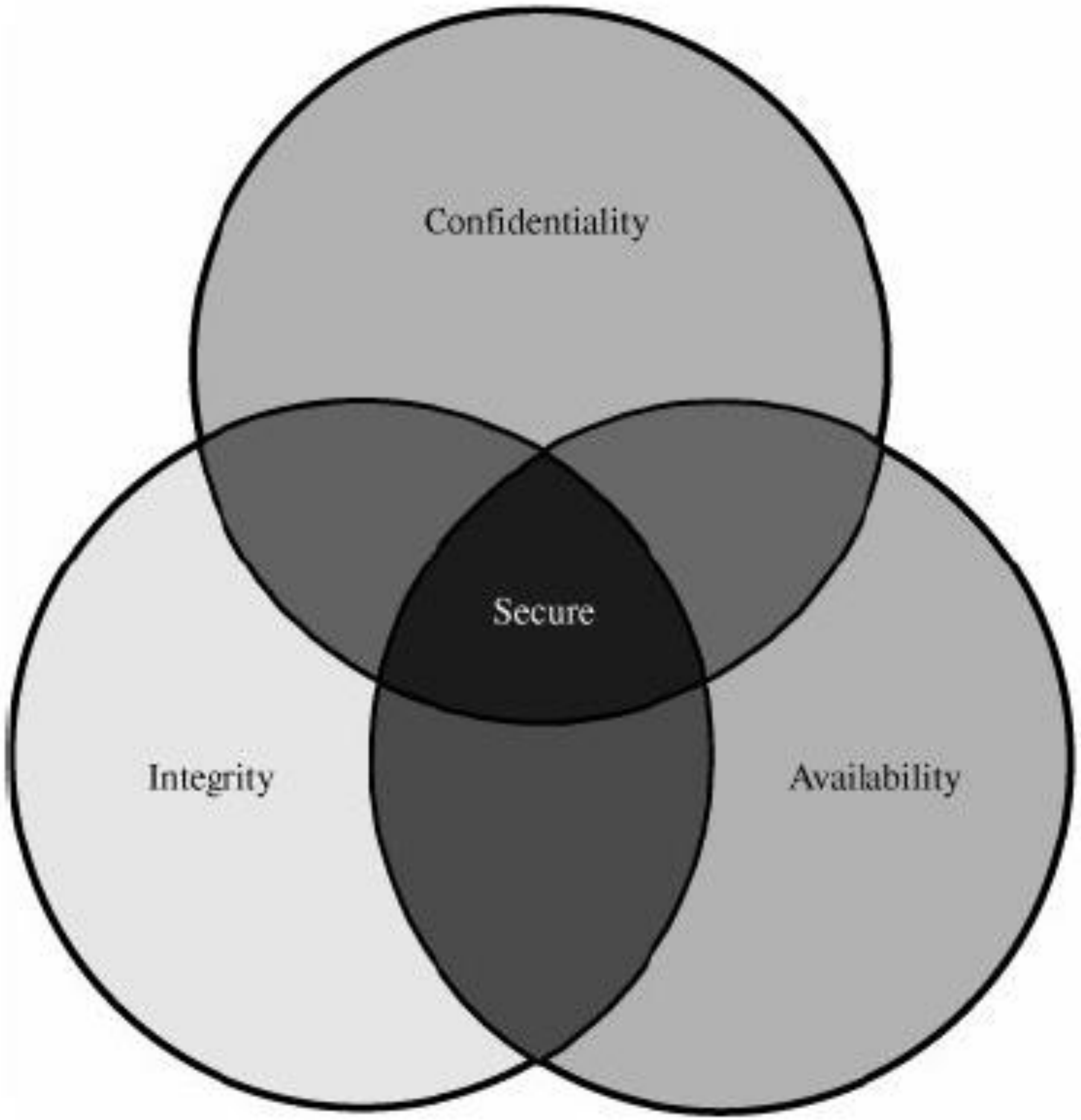
- Computer assets can be modified only be authorized parties and online authorized ways.
- Modification = writing, changing, deleting, creating

Accessibility

- Computer assets are accessible to authorized parties at appropriate times.
- If some person or system has legitimate access to an asset of the computer system, that access should not be prevented.
- Example of lack of accessibility – ***denial of service***.

There should be right balance between these 3 goals.

They should not conflict each other.



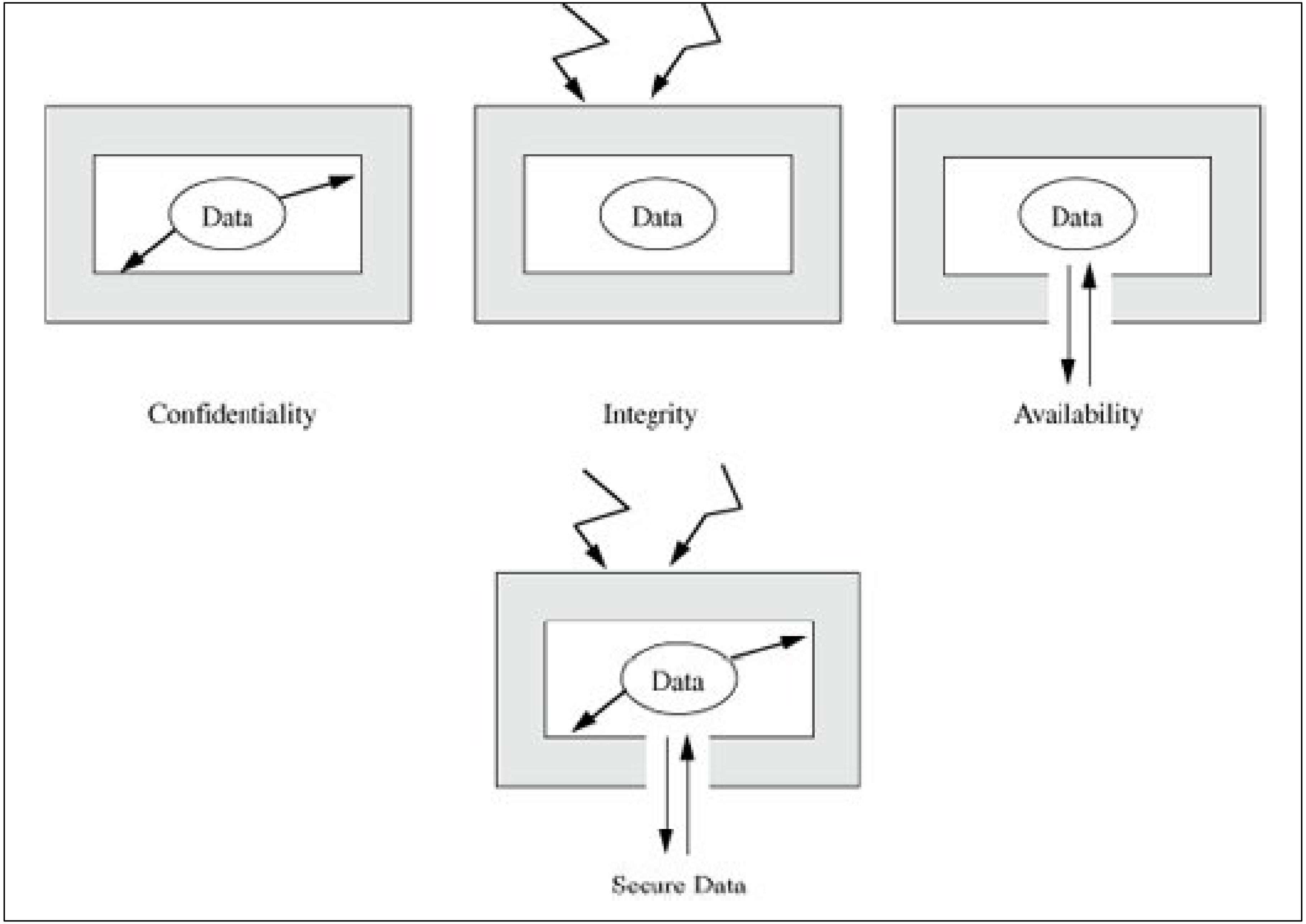


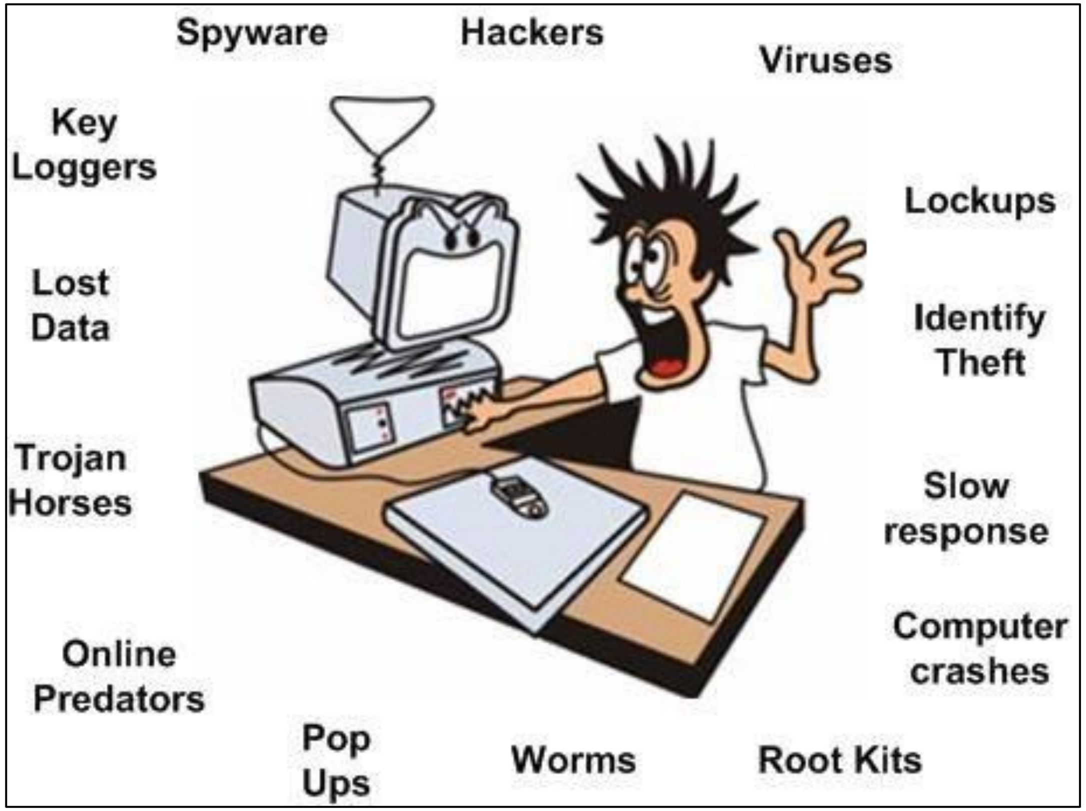
Figure showing a secure computer system.

Risk Analysis

What is a Risk ?

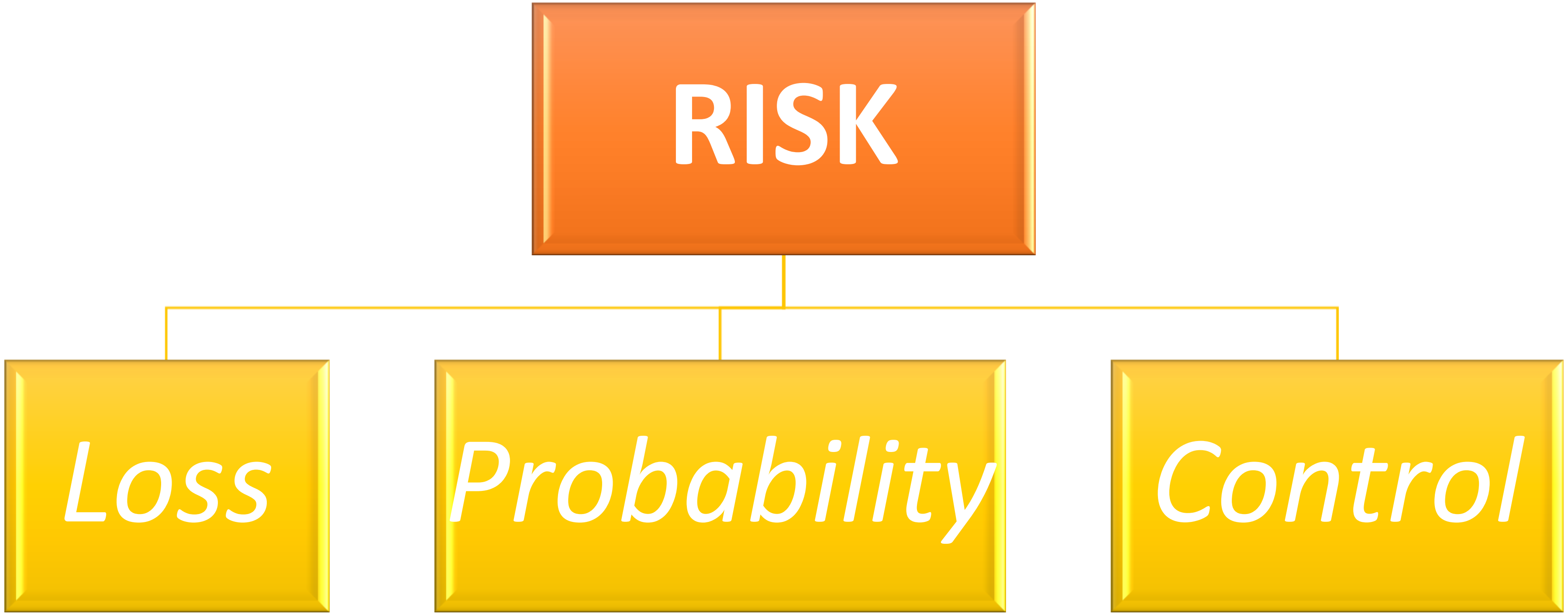
A **risk** is a potential problem that the system or its users may experience.

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.



Characteristics of Risk

Following three are the characteristics of a risk



RISK

Loss

Probability

Control

***A loss associated with an event*.**

- The event must generate a negative effect: compromised security, lost time, diminished quality, lost money, lost control, lost understanding, and so on.
- This loss is called the **risk impact**.

The likelihood that the event will occur.

- The probability of occurrence associated with each risk is measured from 0 (impossible) to 1 (certain).
- When the risk probability is 1, we say we have a **problem.**

The degree to which we can change the outcome.

- We must determine what, if anything, we can do to avoid the impact or at least reduce its effects.
- **Risk control** involves a set of actions to reduce or eliminate the risk.

Risk Exposure

- Risk exposure is a value to quantify the effects of a risk. This value helps us to predict the outcomes of a risk if it may happen.

Risk exposure = Risk impact x Risk probability

- Risk impact = $ (cost of fixing the problem)
- Risk probability = out of 100 (vary over time)
- Example –

Risk exposure = $ 10,000 x 0.3 = $3000

Here, the risk exposure is $3000.

Strategies to deal with Risk

Following are the three ways to deal with a risk.

RISK

Avoid it

Transfer it

Assume it

AVOID THE RISK

- Change the requirements for security or other system characteristics.
- Here, we are fixing the vulnerability so that a potential problem no longer occurs.

TRANSFER THE RISK

- Allocate the risk to other systems, people, organizations, or assets.
- This may lessen the risk impact as the other system, people etc may be more efficient in controlling the risk.
- Another alternative is to buy insurance to cover any financial loss should the risk become a reality.

ASSUME THE RISK

- We accept the risk.
- We Control it with available resources.
- We prepare to deal with the loss if it occurs.

RISK LEVERAGE

$$\frac{Risk\ exposure\ before\ reduction\ \ - risk\ exposure\ after\ reduction}{cost\ of\ risk\ reduction}$$

Higher the leverage value, more cost efficient is the proposed action for reducing the risk.

If there are 2 methods to deal with a risk. Their respective risk leverage is calculated.

Here, it is clear that method 1 should be preferred as it costs less to reduce the risk by the same extent.

Method 1

$$= \frac{\$3000-\$1000}{\$100}$$

= 20

Method 2

$$= \frac{\$3000-\$1000}{\$200}$$

= 10

What is a Risk Analysis?

Risk analysis is the process of examining a system and its operational context to determine possible exposure and the potential harm they can cause.

Risk analysis can be broadly defined to include *risk assessment*, *risk characterization*, *risk communication*, *risk management*, and *policy relating to risk*, in the context of risks of concern.

STEPS OF RISK ANALYSIS

1. Identify assets.
2. Determine vulnerabilities.
3. Estimate likelihood of exploitation.
4. Compute expected annual loss.
5. Survey applicable controls and their costs.
6. Project annual savings of control.

Identify Assets

- ***hardware***: processors, boards, keyboards, monitors, terminals, communications media etc.
- ***software***: source programs, object programs, purchased programs etc.
- ***data***: data used during execution, stored data on various media, printed data, archival data, update logs etc.
- ***people**:* skills needed to run the computing system or specific programs.
- ***documentation***: on programs, hardware, systems, administrative procedures, and the entire system
- ***supplies***: paper, forms, laser cartridges, magnetic media, and printer fluid.

No two organizations will have the same assets to protect, and something that is valuable in one organization may not be as valuable to another.

Determine Vulnerabilities

- The next step in risk analysis is to determine the vulnerabilities of these assets.
- This step requires imagination; we want to *predict what damage might occur* to the assets and from what sources.
- We can enhance our imaginative skills by developing a clear idea of the nature of vulnerabilities.
- This nature derives from the need to ensure the three basic goals of computer security: *confidentiality, integrity, and availability.*

Estimate likelihood of exploitation

- *Likelihood of occurrence* relates to the stringency of the existing controls and the likelihood that someone or something will evade the existing controls.

- Several approaches to computing the probability that an event will occur: *classical, frequency, and subjective*.

- *Each approach has its advantages and disadvantages*, and we must choose the approach that best suits the situation.

Compute expected annual loss

- Next, we must *determine the likely loss* if the exploitation does indeed occur.
- This value is *difficult to determine*.
- Some costs, such as the cost to replace a hardware item, are easy to obtain.
- However, we must take care to include *hidden costs* in our calculations.
- There are costs in restoring a system to its previous state, reinstalling software, or deriving a piece of information.
- These costs are substantially *harder to measure*.

Survey applicable controls and their costs

- We want to match each vulnerability with *at least one appropriate security technique*.

- Once we do that, we can use our expected loss estimates to help us decide which controls, alone or in concert, are the most cost effective for a given situation.

Project annual savings of control

- risk analysis is used to *evaluate the true cost*s of proposed controls.

- The effectiveness of *different controls can be compared* on paper before actual investments are made.

- Risk analysis can thus be *used repeatedly*, to select an optimum set of controls.

Organizational Security Policies

What is a Security Policy ?

A security policy is a high level management document to inform all users of the goals of and constraints on using a system.

- It helps *recognize sensitive information assets.*
- It *clarifies security responsibilities*.
- It *promotes awareness* for existing employees.
- It *guides* new employees.

AUDIENCE

- A security policy *addresses several different audiences* with different expectations. That is, each group users, owners, and beneficiaries uses the security policy in important but different ways.

CONTENTS

- The policy should *describe the nature of each audience* and their security goals.
- Several other sections are required, including the *purpose of the computing system*, the *resources needing protection*, and the *nature of the protection to be supplied*.

CHARACTERISTICS OF A GOOD SECURITY POLICY

- If a security policy is written poorly, it cannot guide the developers and users in providing appropriate security mechanisms to protect important assets. *Certain characteristics make a security policy a good one*.

1. A security policy must be **comprehensive.**
2. A security policy must **grow** and **adapt** well.
3. The policy must be **realistic**.
4. The policy should be **clear** and **direct**.

INTERNET SECURITY POLICY

- Users are *individually responsible* for understanding and respecting the security policies of the systems (computers and networks) they are using. Users are individually accountable for their own behavior.
- Users have a responsibility to *employ available security mechanisms* and procedures for protecting their own data.
- Computer and network service providers are responsible for maintaining the security of the systems they operate.
- Vendors and system developers are responsible for providing systems which are sound and which embody adequate security controls.
- Users, service providers, and hardware and software vendors are *responsible for cooperating* to provide security.
- *Technical improvements* in Internet security protocols should be sought on a continuing basis.

Internal Vs. External Threat

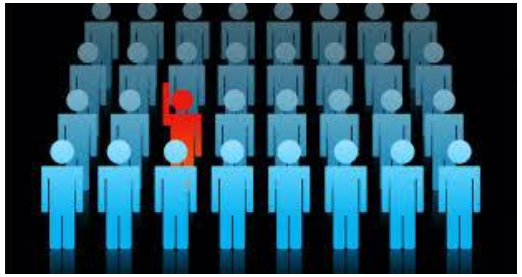
WHAT DOES A THREAT MEAN ?

- The word 'threat' in information security means anyone or anything that poses danger to the information, the computing resources, users, or data. The threat can be from 'insiders' who are within the organization, or from outsiders who are outside the organization.
- Security threats can be categorized in many ways. One of the important ways they are categorized is on the basis of the “origin of threat,” namely external threats and internal threats

ORIGIN OF THREAT

- External threats originate from outside the organization, primarily from the environment in which the organization operates. These threats may be primarily physical threats, socio-economic threats specific to the country like a country's current social and economic situation, network security threats, communication threats, human threats like threats from hackers, software threats, and legal threats.
- Internal threats originate from within the organization. The primary contributors to internal threats are employees, contractors, or suppliers to whom work is outsourced. The major threats are frauds, misuse of information, and/or destruction of information.

REASONS FOR INTERNAL THREAT



Weak Security Policies, including:

- Unclassified or improperly classified information, leading to the divulgence or unintended sharing of confidential information with others, particularly outsiders.
- Inappropriately defined or implemented authentication or authorization, leading to unauthorized or inappropriate access.
- Undefined or inappropriate access to customer resources or contractors/suppliers, leading to fraud, misuse of information, or theft.
- Unclearly defined roles and responsibilities, leading to no lack of ownership and misuse of such situations.

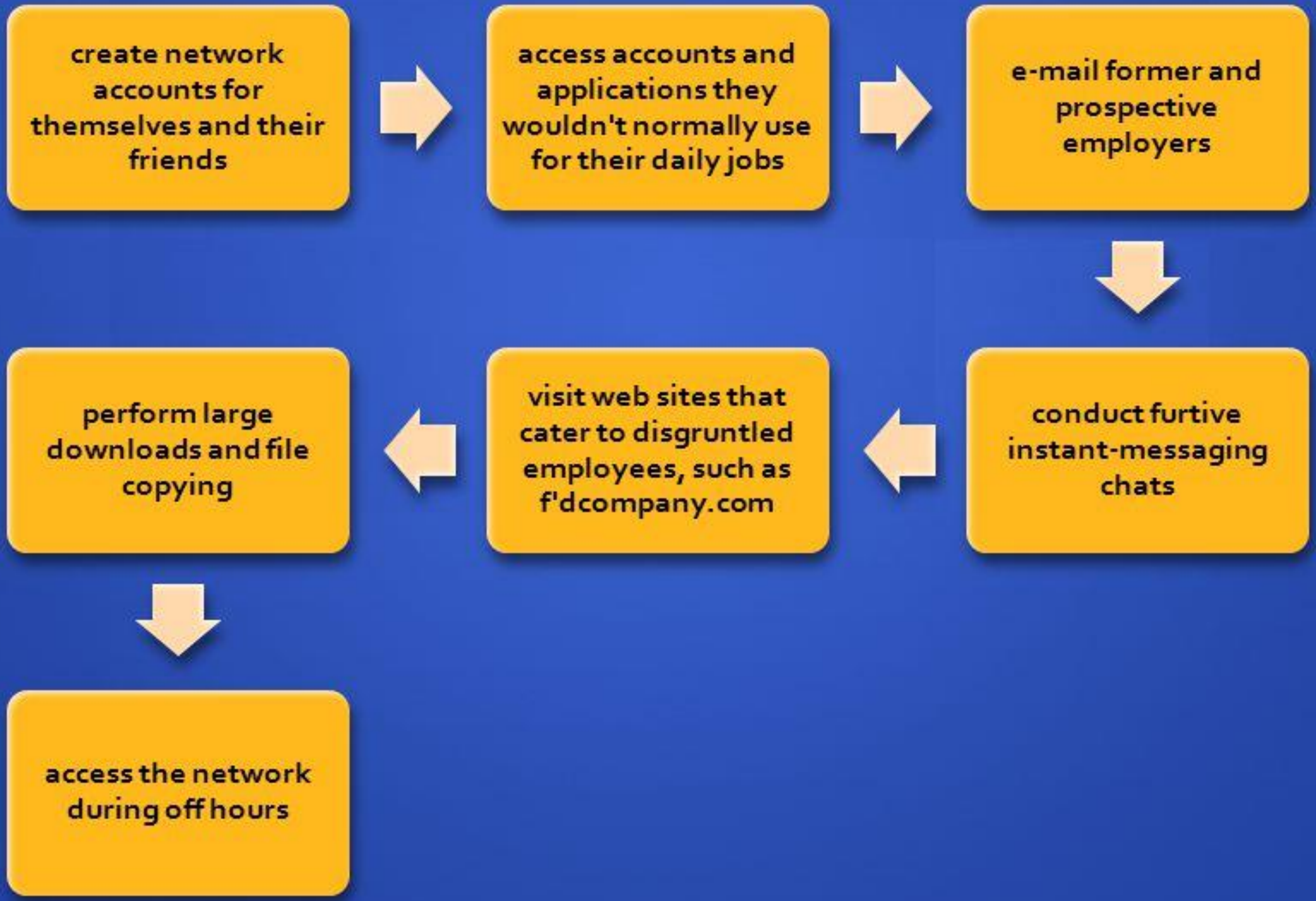
Weak Security Administration, including:

- Weak user passwords allowed in the system and applications, leading to unauthorized access and information misuse.
- Inappropriately configured systems and applications, leading to errors, wrong processing, or corruption of data.
- Non-restricted administrative access on the local machines and/or network, leading to misuse of the system or infection of the systems.
- Non-restricted access to external media such as USB or personal devices, leading to theft of data or infection of the systems.
- Unrestricted access to contractors and suppliers leading to theft or misuse of information including through dumpster diving or shoulder surfing.
- Unrestricted website surfing, leading to infections of viruses, phishing, or other malware.
- Unrestricted software downloads leading to infection, copyright violations, or software piracy.

Lack of user security awareness, including:

- Identity theft and unauthorized access due to weak password complexity.
- Not following company policies, such as appropriate use of assets, clean desk policy, or clear screen policy, leading to virus attacks or confidential information leakage.
- Divulging user IDs and/or passwords to others, leading to confidential information leakage..
- Inappropriate configuration or relaxation of security configurations, leading to exploitation of the systems.
- Entering incorrect information by oversight and not checking it again or processing the wrong information.
- Ignoring security errors and still continuing with transactions, leading to the organization being defrauded.

Internal Threat
Patterns of Behavior



create network accounts for themselves and their friends

access accounts and applications they wouldn't normally use for their daily jobs

e-mail former and prospective employers

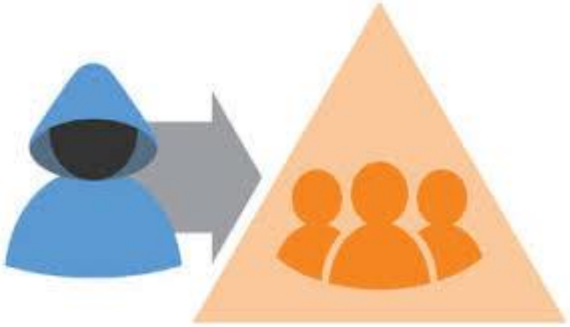
conduct furtive instant-messaging chats

visit web sites that cater to disgruntled employees, such as f'dcompany.com

perform large downloads and file copying

access the network during off hours

REASONS FOR EXTERNAL THREAT



➢ **Non Deliberate**

- The main threats of this type are ‘disasters’.
- These may be natural:
- Floods, Extreme weather conditions, earthquakes, volcanoes etc.
- Human, mechanical, Plane crashes, power cuts, fires, building collapse etc.
- Both have potential to wipe out an organization's Information systems.

➢ **Deliberate**

- Threats of this type can take many forms, including:
- Criminals wishing to defraud the organization by accessing and amending financial data;
- Viruses with potential to corrupt data
- Industrial espionage, i.e. rival organizations accessing confidential information in order to gain competitive advantage
- Actual theft of hardware/software
- Terrorist attack

Data Protection

- There are many things we do online from entertaining ourselves all the way completing upto business transactions. While internet allows many people to do a lot from a single location, we must understand the importance of protecting our information and data online to keep life running as smoothly as possible.
- In the modern era of information security violation and attacks increased on each day. For data security we need to implement more strict policies in a way our business operations not blocked and execute smoothly.
- **Security Measures**:

1. Prevent the physical access to the servers where data reside.
2. Implement operating system operations in more secure way.
3. Implement security models that enforce security measures.
4. DBA should implement the security polices to protect the data.

WHAT IS DATA PROTECTION?

- Data protection refers to the degree to which data is fully protected from tampering or unauthorized acts. It comprises of information system and information security concepts.
- Information system (IS) comprises of components working together to produce and generate accurate information.
- Information / data is one of the most valuable asset for any organization. Its security consist of procedures and measures taken to protect information systems components.
- Data Integrity refers to the overall completeness, accuracy and consistency of data. Integrity has two types physical and logical.
- Physical integrity: Physical integrity deals with challenges associated with correctly storing and fetching the data itself.

  Challenges: electromechanical faults, physical design flaws, natural disasters etc.
- Logical Integrity: Concerned with referential integrity and entity integrity in a relational database

  Challenges: software bugs, design flaws, and human errors

SECURITY METHODS

DATA COMPONENT PROTECTED	SECURITY METHOD
PEOPLE	● Physical limit to access hardware and documents. ● Through the process of identification and authentication make sure right user is going to access the information ● Conduct training courses on the Importance of security and how to guard assets ● Establishment of security policies and procedures.
APPLICATION	● Authentication of users who access the application. ● Apply business rules. ● A Single sign on

DATA COMPONENT PROTECTED	SECURITY METHOD
NETWORK	● Network firewall to block the intruders. ● VPN ● Network Authentication
OPERATING SYSTEM	● Authentication ● Password policy ● User accounts
DBMS	● Authentication ● Audit mechanism ● Database resource limits ● Password policy ● Data encryption
DATA FILES	● Files / Folder permissions ● Access monitoring
DATA	● Data Validation ● Data constraints ● Data Encryption ● Data Access

User Authentication

USER AUTHENTICATION

- An operating system bases much of its protection on knowing who a user of the system. Over time, organizations and systems have developed means of authentication, using documents, voice recognition, fingerprint and retina matching, and other trusted means of identification.

- In computing, the choices are more limited and the possibilities less secure. Anyone can attempt to log in to a computing system. Thus, most computing authentication systems must be based on some knowledge shared only by the computing system and the user.

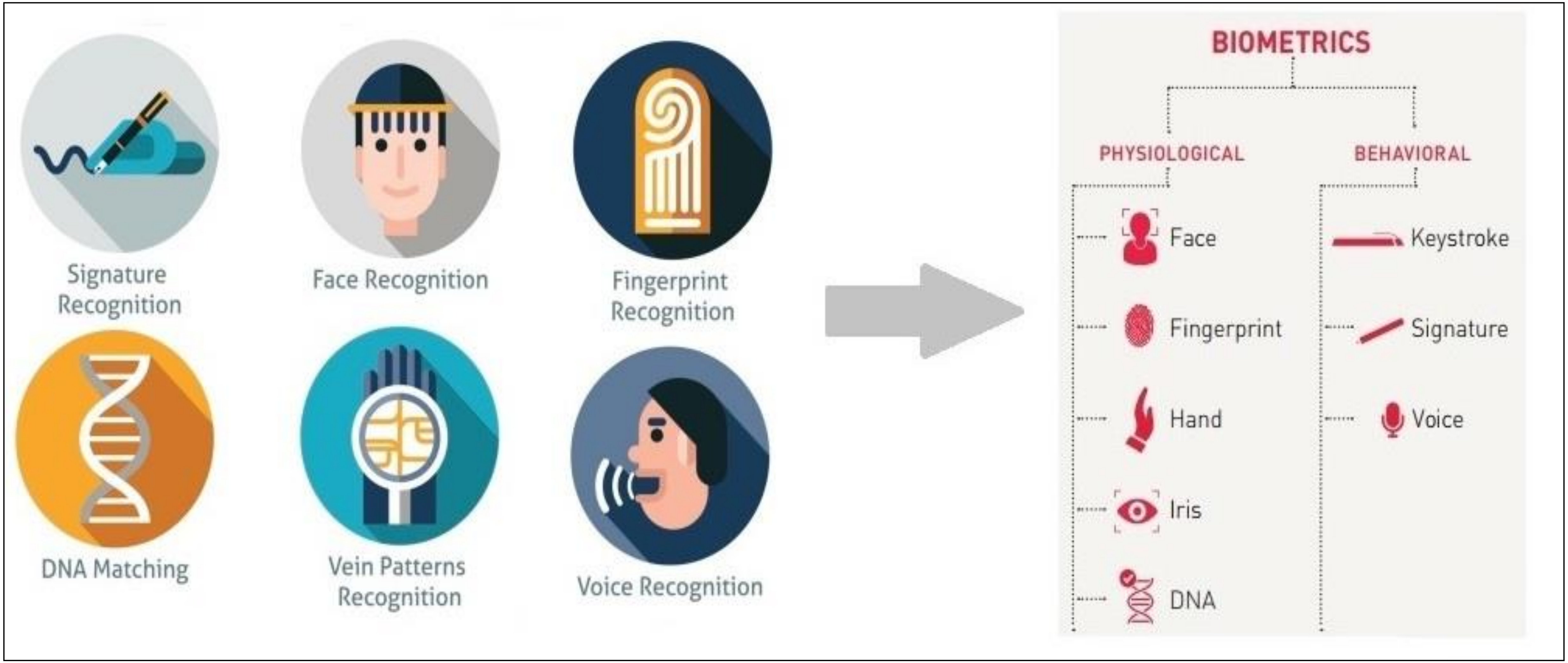
- Authentication mechanisms use any of three qualities to confirm a user's identity:
- **Something the user *knows*.** Passwords, PIN numbers, passphrases, a secret handshake, and mother's maiden name are examples of what a user may know.
- **Something the user *has*.** Identity badges, physical keys, a driver's license, or a uniform are common examples of things people have that make them recognizable.
- **Something the user *is*.** These authenticators, called **biometrics,** are based on a physical characteristic of the user, such as a fingerprint, the pattern of a person's voice, or a face(picture). These authentication methods are old (we recognize friends in person by their faces or on a telephone by their voices) but are just starting to be used in computer authentications.
- The most common authentication mechanism for user to operating system is a **password**, a "word“ known to computer and user. Although password protection seems to offer a relatively secure system, human practice sometimes degrades its quality.
- In addition to the name and password, we can use other information available to authenticate users.

Biometrics

WHAT DOES BIOMETRICS MEAN?

- **Biometrics** are biological authenticators, based on some physical characteristic of the human body.

- The list of biometric authentication technologies is still growing. Now there are devices to recognize the following biometrics: fingerprints, hand geometry (shape and size of fingers), retina and iris (parts of the eye), voice, handwriting, blood vessels in the finger, and face. Authentication with biometrics has advantages over passwords because a biometric cannot be lost, stolen, forgotten, lent, or forged and is always available, always at hand, so to speak.


Signature Recognition
Face Recognition
Fingerprint Recognition
DNA Matching
Vein Patterns Recognition
Voice Recognition
BIOMETRICS
PHYSIOLOGICAL
BEHAVIORAL
Face
Fingerprint
Hand
Iris
DNA
Keystroke
Signature
Voice

- Biometrics are very reliable for authentication but much less reliable for authentication.
- First, a user registers with the reader, during which time a characteristic of the user (for example, the geometry of the hand) is captured and reduced to a template or pattern. During registration, the user may be asked to present the hand several times so that the registration software can adjust for variations, such as how the hand is positioned.
- Second, the user later seeks authentication from the system, during which time the system remeasures the hand and compares the new measurements with the stored template. If the new measurement is close enough to the template, the system accepts the authentication; otherwise, the system rejects it. Every template is thus a pattern of some number of measurements.

Problems with Biometrics

- Biometrics are relatively new, and some people find their use **intrusive**. People have real concerns about peering into a laser beam or sticking a finger into a slot are examples of people resisting biometrics.
- Biometric recognition devices are **costly**, although as the devices become more popular, their costs go down.
- All biometric readers use sampling and establish a threshold for when a match is close enough to accept. The device has to sample the biometric, measure often hundreds of key points, and compare that set of measurements with a template. There is normal variability if, for example, your face is tilted, you press one side of a finger more than another, or your voice is affected by an infection. **Variation reduces accuracy.**
- Biometrics can become a single point of **failure**. Forgetting a password is a user's fault; failing biometric authentication is not.
- Although equipment is improving, there are still false readings. We label a "false positive" or "false accept" a reading that is accepted when it should be rejected (that is, the authenticator does not match) and a "false negative" or "false reject" one that rejects when it should accept. Often, reducing a false positive rate increases false negatives, and vice versa.
- The speed at which a recognition must be done limits accuracy. The user understandably wants to get past the gate and becomes frustrated and irritated if authentication takes too long.
- Although we like to think of biometrics as unique parts of an individual, forgeries are possible.

Disadvantages of Biometrics

- Costly

- Facial imaging can also hinder accurate identifications.

- Missing body part problem

- False acceptances and rejections.

- The scanning of eye is fearful.

- Ethical issues
  - Personal data used for something other than its advertised purpose.
- Privacy issues
  - Who can access data
  - Misuse of personal data

Advantages Of Biometric System

- directly authenticates the person
- difficult to steal; thereby making biometrics authentication very strong.
- portable, and is unlikely to be lost.
- user cannot share or forget his retina or fingerprint, while a password and username are easily forgotten.
- User friendliness
- Comfort
- Accuracy

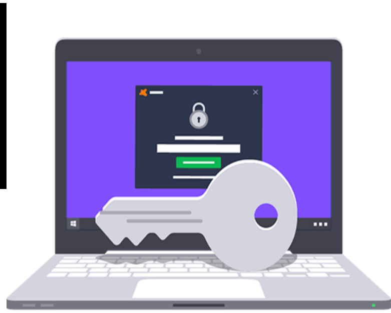
Passwords

WHAT IS A PASSWORD?

The most common authentication mechanism for user and operating system is a **password,** a “word” known to computer and user.

Passwords are mutually agreed-upon code words b/w user and system.Its either assigned by a user or a system chooses it

DIFFICULTIES IN USE OF PASSWORDS

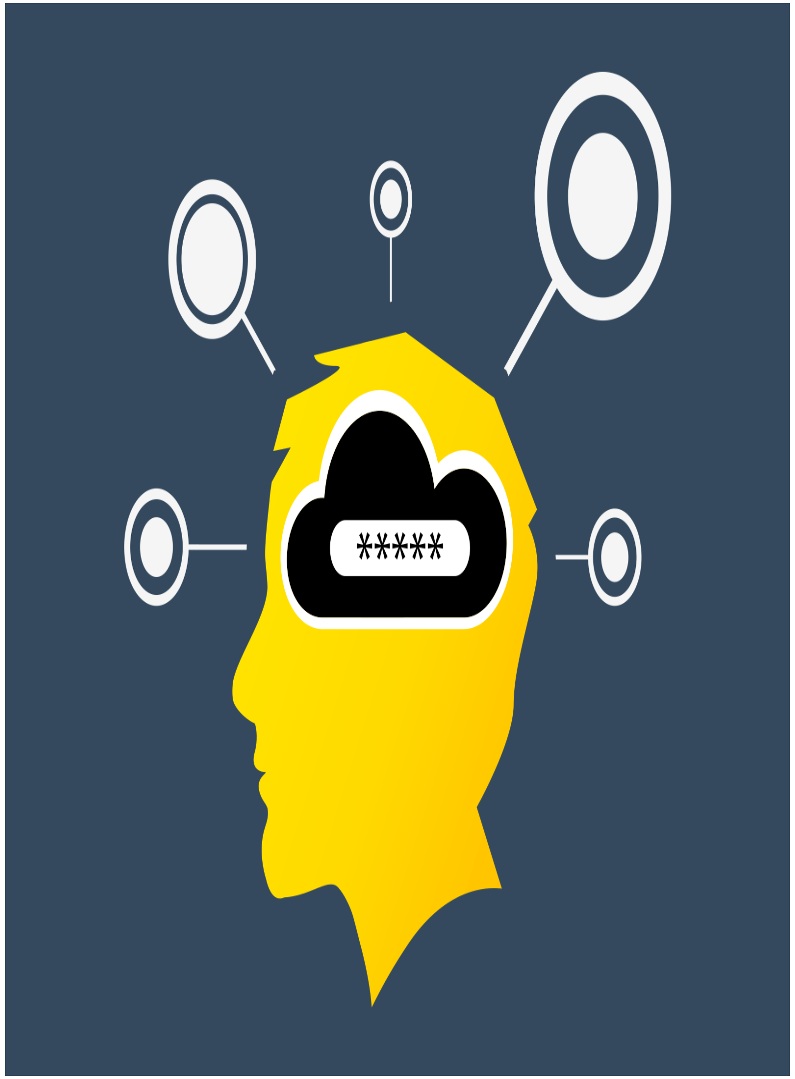


- **LOSS**-It is very difficult to replace a lost or forgotten password
- **USE**- Supplying a password for each access to a file can be inconvenient and time consuming
- **Disclosure-** If a password is disclosed to an unauthorized individual, the file becomes immediately accessible. New password are assigned to user because old password will fail.
- **Revocation-** To revoke one user's access right to a file, someone must change the password,thereby causing the same problems as disclosure.

ATTACK ON A PASSWORD

Some ways one might be able to determine a user's password, in decreasing order of difficulty.

1. **Try all possible passwords.**
2. **Try frequently used passwords.**
3. **Try passwords likely for the user.**
4. **Search for the system list of passwords.**
5. **Ask the user.**



SELECTION CRITERIA FOR PASS WORDS

- ***Use characters other than just A-Z***:
  If passwords are chosen from the **letters A-Z, there are only 26 possibilities** for each character. **Adding digits expands the number of possibilities to 36.Using both uppercase and lowercase letters plus digits expand it to 62** . Although this change seems small, the effect is large when someone is testing a full space of all possible combinations of characters

4ET%1ge6 ✓
1234 ✗

- **Choose long passwords-** The combinatorial explosion of passwords begins at length **4** or **5. Choosing longer passwords makes it less likely that a password will be uncovered.** Remember that a brute force penetration can stop as soon as the password is found. Some penetrators will try the easy cases known words and short passwords and move on to another target if those attacks fail.

- **Avoid actual names or words:** Theoretically, there are 266 or about 300 million 6-letter "words", but there are only about 150,000 words in a good collegiate dictionary, ignoring length.

- **Choose an unlikely password*:-*** Password choice is a double bind. To remember the password easily, you want one that has special meaning to you. However, you don't want someone else to be able to guess this special meaning replacements of 0 (zero) for o or O (letter "oh") and 1 (one) for l (letter"ell") or $ for S (letter "ess").

- **Change the password regularly***:-* Even if there is no reason to suspect that the password has been compromised, change is advised. A penetrator may break a password system by obtaining an old list or working exhaustively on an encrypted list.

- **Don't write it down:-**This time-honored advice is relevant only if physical security is a serious risk.

- **Don't tell anyone else:-**The easiest attack is **social engineering, in which the attacker** contacts the system's administrator or a user to elicit the password in some way. For example,the attacker may phone a user, claim to be "system administration," and ask the user to verify the user's password.

One Time Password

WHAT IS OTP ?

- A **one-time password is one that changes every time it is used.**
- Instead of static phrase, the system assigns a static mathematical function to a user.
- The system provides an argument to the function, and the user c $f(E(x)) = E(D(E(x)) + 1)$ computes and returns the function value.
- Such systems are also called **challenge response systems** *because the system presents a challenge to the user and* judges the authenticity of the user by the user's response.
- Examples of **FUNCTIONS** used for OTPs are as follows :- $f(x) = x + 1$, $f(x) = r(x)$, $f(a1a2a3a4a5a6) = a3a1a1a4$, $f(E(x)) = E(D(E(x)) + 1)$.

Computer Forensics

COMPUTER FORENSICS

digital forensic science

storage

media

.

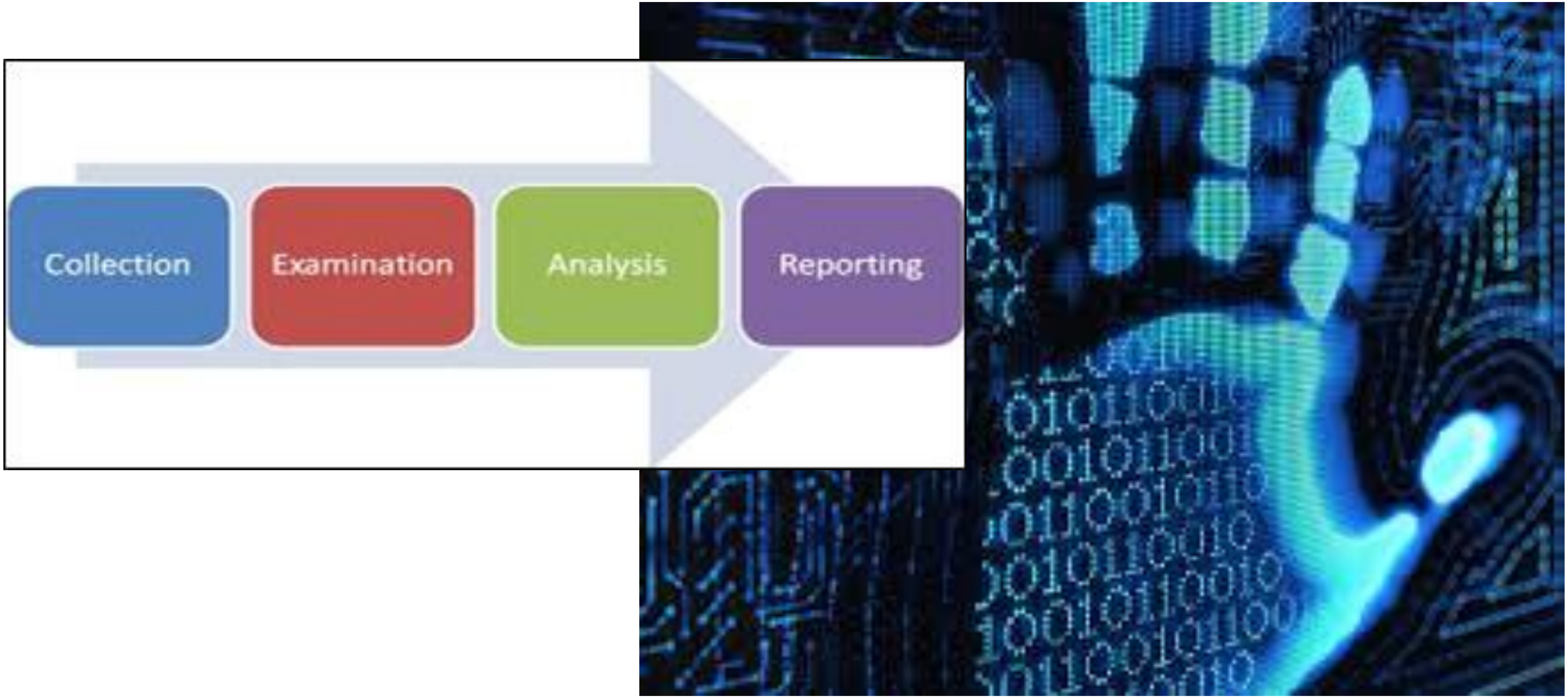
IMPORTANCE OF COMPUTER FORENSICS

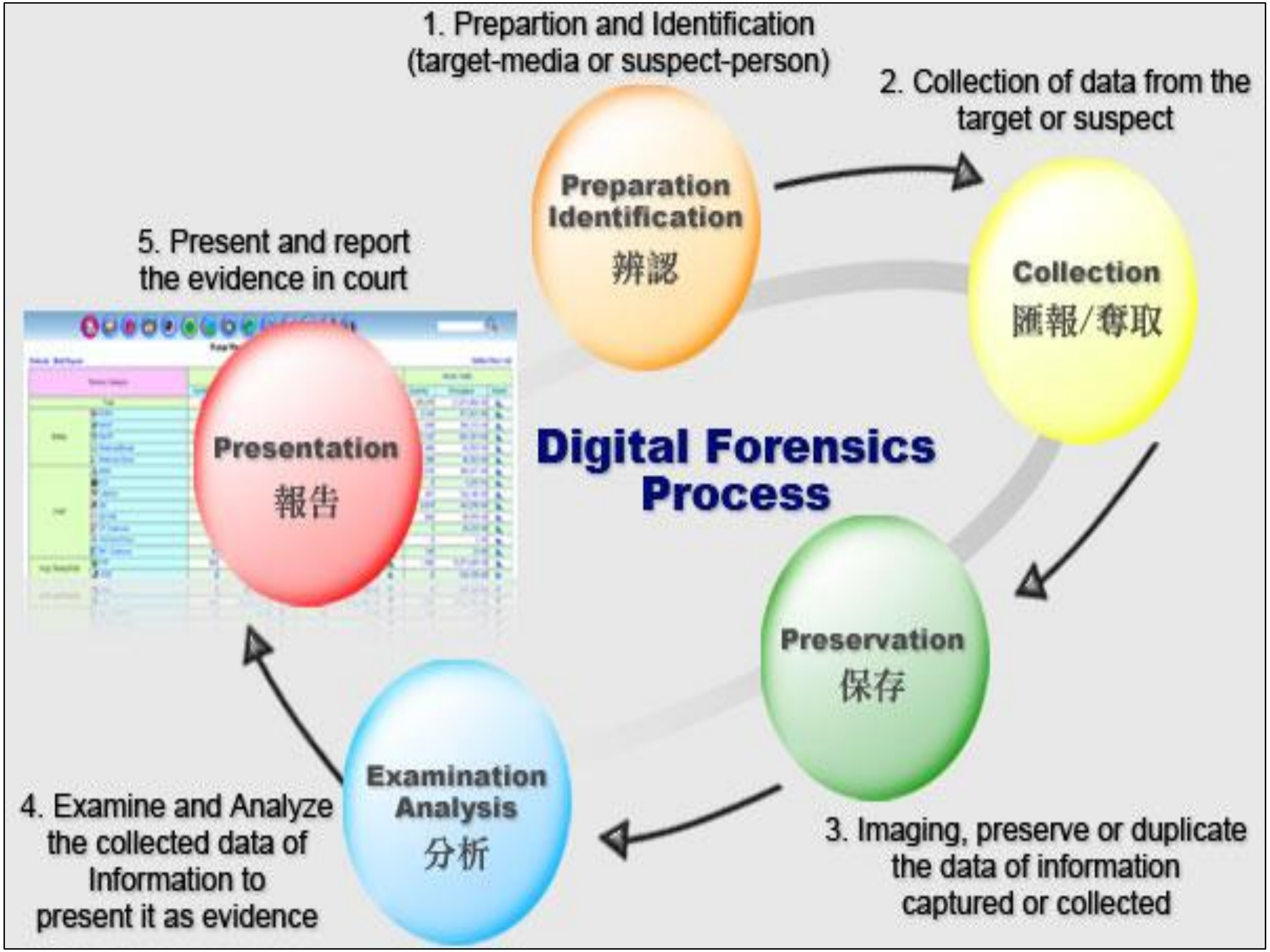
- Investigation of a wide variety of computer crimes.
- Used in civil proceedings.
- Involves techniques and principles to data recovery.
- Used in a number of high-profile cases.
- Is becoming widely accepted as reliable within U.S. and European court systems.

HISTORY

1980s personal computers became more accessible to consumers, leading to their increased use in criminal activity (for example, to help commit fraud). At the same time, several new "computer crimes" were recognized (such as cracking). The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court.

DIGITAL FORENSIC PROCESS





Digital Forensics Process

1. Prepartion and Identification (target-media or suspect-person)

Preparation Identification 辨認

2. Collection of data from the target or suspect

Collection 匯報/奪取

3. Imaging, preserve or duplicate the data of information captured or collected

Preservation 保存

4. Examine and Analyze the collected data of Information to present it as evidence

Examination Analysis 分析

5. Present and report the evidence in court

Presentation 報告

Incident Response Plan

WHAT IS AN INCIDENT RESPONSE PLAN ?

- An **incident response plan tells the staff how to deal with a security incident.**
- **GOAL**: Handling the current security incident, without regard for the business issues. The security incident may at the same time be a business
- It may not interrupt business severely but could be a
- An incident could be a single event, a series of events, or an ongoing problem

AN INCIDENT RESPONSE PLAN SHOULD

- **define** what constitutes an *incident*

- **identify** who is responsible for *taking charge of the situation*

- **describe** the plan of *action*

3 PHASES OF IRP

1.ADVANCE PLANNING

With an incident response plan in place, everybody is trained in advance to call the designated leader. There is an established list of people to call, in order, in case the first person is unavailable.

- The leader decides what to do next, and he or she begins by determining if this is a real incident or a false alarm
- Indeed, natural events sometimes look like incidents, and the facts of the situation should be established first.
- If the leader decides this may be a real incident, he or she invokes the response team.

2. RESPONSE TEAM:-

The response team is the set of people include:-

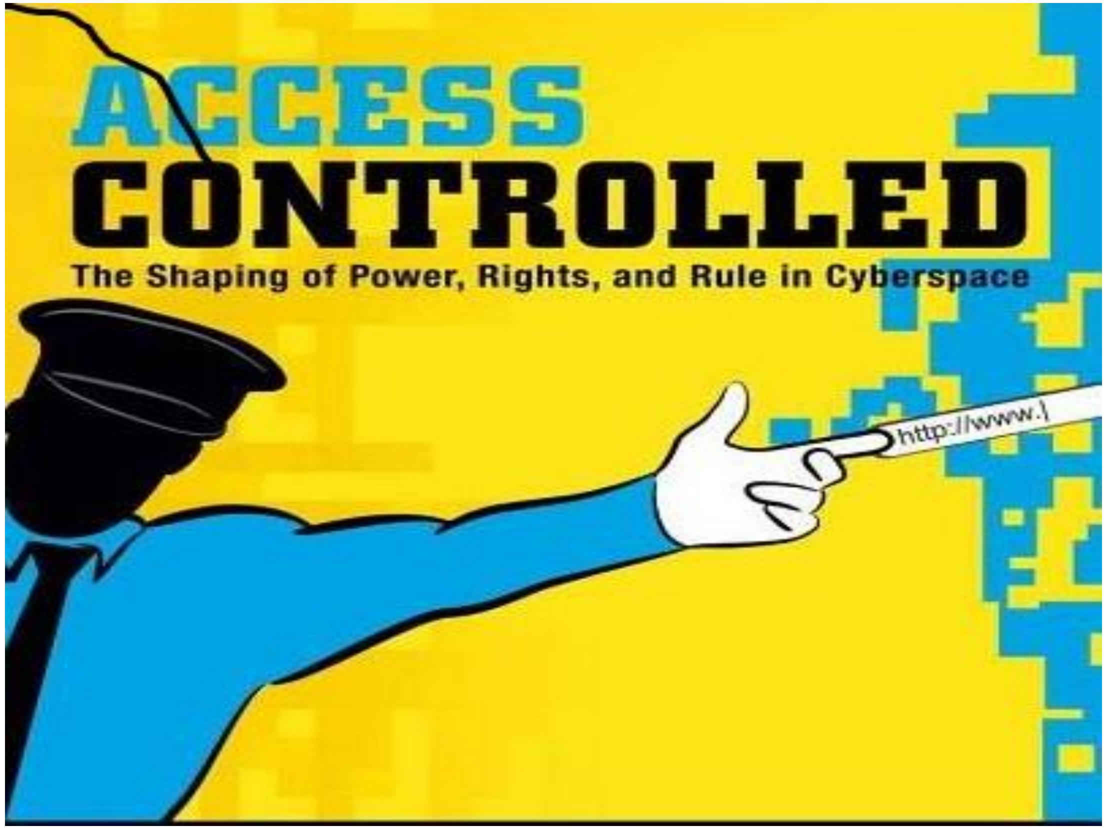
- DIRECTOR: Person in charge of the incident, who decides what actions to take and when to terminate the response. The director is typically a management employee.
- LEAD TECHNICIAN: person who directs and coordinates the response. The lead technician decides where to focus attention, analyzes situation data, documents the incident and how it was handled, and calls for other technical people to assist with the analysis.
- ADVISOR: legal, human resources, or public relations staff members as appropriate.

3.After the Incident Is Resolved

Eventually, the incident response team closes the case. At this point it will hold a review after the incident to consider two things:

- *Is any security control action to be taken? Did an intruder compromise a system because Did the incident response plan work? Did everyone know whom to notify?*
- *Did the team have needed resources? Was the response fast enough? What should be done differently next time?*

Access Control



ACCESS CONTROL

Access control is a security technique that can be used to regulate **who or what** can view or use **which** resources in a computing environment.

TYPES OF ACCESS CONTROL

1.PHYSICAL ACCESS CONTROL- Physical access control limits access to campuses, buildings, rooms and physical IT assets.

2. LOGICAL ACCESS CONTROL- Logical access limits connections to computer networks, system files and data.

Access Control

- Most common approach to protection
- Each file & directory has an **access control list**
  - Contains user + access rights
  - OS checks list before granting a user access to a file
- Problems:
  - Giving access to a file to everyone involves listing each individual user in the access control list
  - Building a list may be impossible if we do not know in advance the users of the system
  - The list is stored in the directory entry, making is unpredictable in size (and potentially very large)

CATEGORIES OF ACCESS CONTROL

- Mandatory access control
- Discretionary access control
- Role-based access control
- Rule-based access control

MAIN ROLE

Access control systems perform authorization, identification, authentication, access approval, and accountability of entities through login credentials including **passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.**

THANK YOU !