AGENDA

- What is Security?
- What is cyber security?
- Threats & Risks
- Cyber Security Organizations
- Cyber Security Jobs
- Types of Attackers
- Common Attacks
- Methods of Attack
- Defenses against threats

COURSE OBJECTIVES

- We will **NOT** teach you how to be a Hacker.
- We will teach you a “**Knowledge**”.
- This knowledge will help you to **protect your systems**.
- Don’t Try to Attack , **without permission**.
- Try only on sites that **gives Permission**.

What is Security?

“The state of being secure, to be free from danger”

Security is Layers

Layers of Security:

- **Physical Security:** Protect the **Physical items**, object or areas from unauthorized access. Such as : Servers – Routers

- **Personal Security:** Protection to **personal** who authorized to access organization and its operation.
  Such as : System Admins , Security engineers

- **Network Security**: protection of **networking** components, connection and content

- **Communications Security:** Protection of communication media, networking components and content.
  Such as : Data Transmission

- **Information Security:** Protection of information and its Critical elements.

INFORMATION SECURITY?

- Means a *protection of information* and its critical elements, including systems and hardware that use, store, and transmit that information.

- What is the differences between :
  - Data
  - Information
  - Knowledge

WHAT IS CYBER SECURITY?

- are **security standards** which enable **organizations to practice safe security techniques to minimize the number of successful cyber security attacks.**
- refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the *Internet* by cyber criminals.

Cyber Security is **important for network, data and application security.**

CYBER SECURITY

- **Cyber**
  - Operating System
  - Network
  - Application
  - Data
- **Security**
  - Protect against attacks or danger

WHY DO WE NEED SECURITY?

- **Protect vital information** while still allowing access to those who need it
  - Trade secrets, medical records, etc.
- **Provide authentication and access control for resources**
  - Ex: shared printers/Files/Applications
- **Guarantee availability** of resources
  - Ex: Online services (99.999% reliability)
- **Digitalization** : every thing will be automated

Why security is important?

- Computer networks have grown in both, size and importance in a very short time.
- The Internet is an integral part of our daily lives (24/7).
- If the security of the network is compromised, there could be serious consequences, such as loss of privacy, theft of information, and even legal liability.
- Impact on business and individuals.
  - Decrease in productivity and sales revenue
  - Bad impact on company reputation (yahoo)
  - Loss of time --→ Money

- Increase in **Cyber Crimes** (Identity theft, Terrorism, ..)

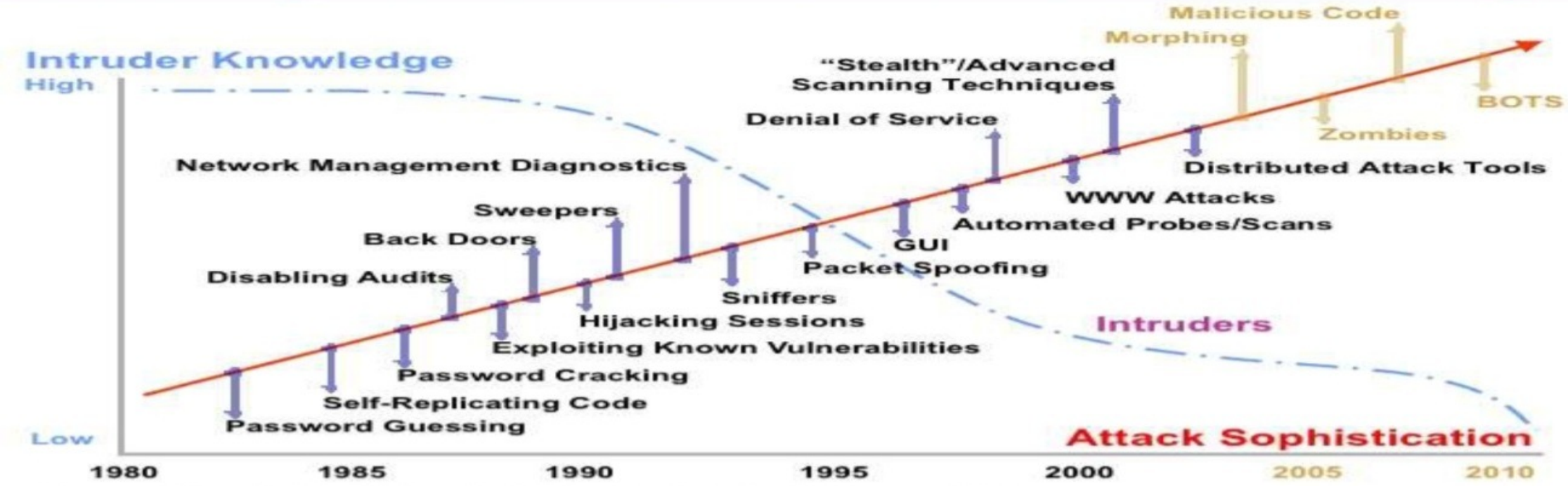
WHAT IS CYBER CRIME?

- The former descriptions were "computer crime", "computer-related crime" or "crime by computer".
- **Cyber Crimes includes**
  - Illegal access
  - Illegal Interception
  - System Interference
  - Data Interference
  - Misuse of devices

HISTORY OF CYBER ATTACKS

- The first recorded cyber crime was recorded in the year 1820.
- The first spam email took place in 1978 when it was sent over the Arpanet.
- The first Virus was installed on an Apple Computer in 1982

Attack Sophistication vs. Intruder Technical Knowledge



Sources: *Carnegie Mellon University, 2002 and Idaho National Laboratory, 2005*

THREATS & RISKS

- People use networks to exchange sensitive information with each other.
- People purchase products and do Internet. their banking over the internet

  - We rely on networks to be secure and to protect our identities and our private information
- Network Security is **a shared responsibility** that **each person must accept** when they connect to the network.

Risk = Vulnerability X Threats

WHO IS NOT ALLOWED TO BE VULNERABLE?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Multinational corporations

ANYONE ON THE NETWORK

SECURITY GOALS IN DIFFERENT ENVIRONMENTS

- Banking
- Electronic trading
- Pharmaceuticals
- All networks

SECURITY GOALS IN DIFFERENT ENVIRONMENTS

- **Banking**
  - Protect against accidental modification of transactions
  - Protect account numbers from disclosure
  - Ensure customers privacy
- **Electronic trading**
  - Assure source and integrity of transactions
  - Protect corporate privacy
  - Provide legally binding electronic signatures on transactions

SECURITY GOALS IN DIFFERENT ENVIRONMENTS

- **Pharmaceuticals**
  - **Protect corporate / individual privacy**
  - **Confidentiality is most critical**

- **All Networks**
  - **Prevent outside penetrations**

CHALLENGES OF SECURING INFORMATION

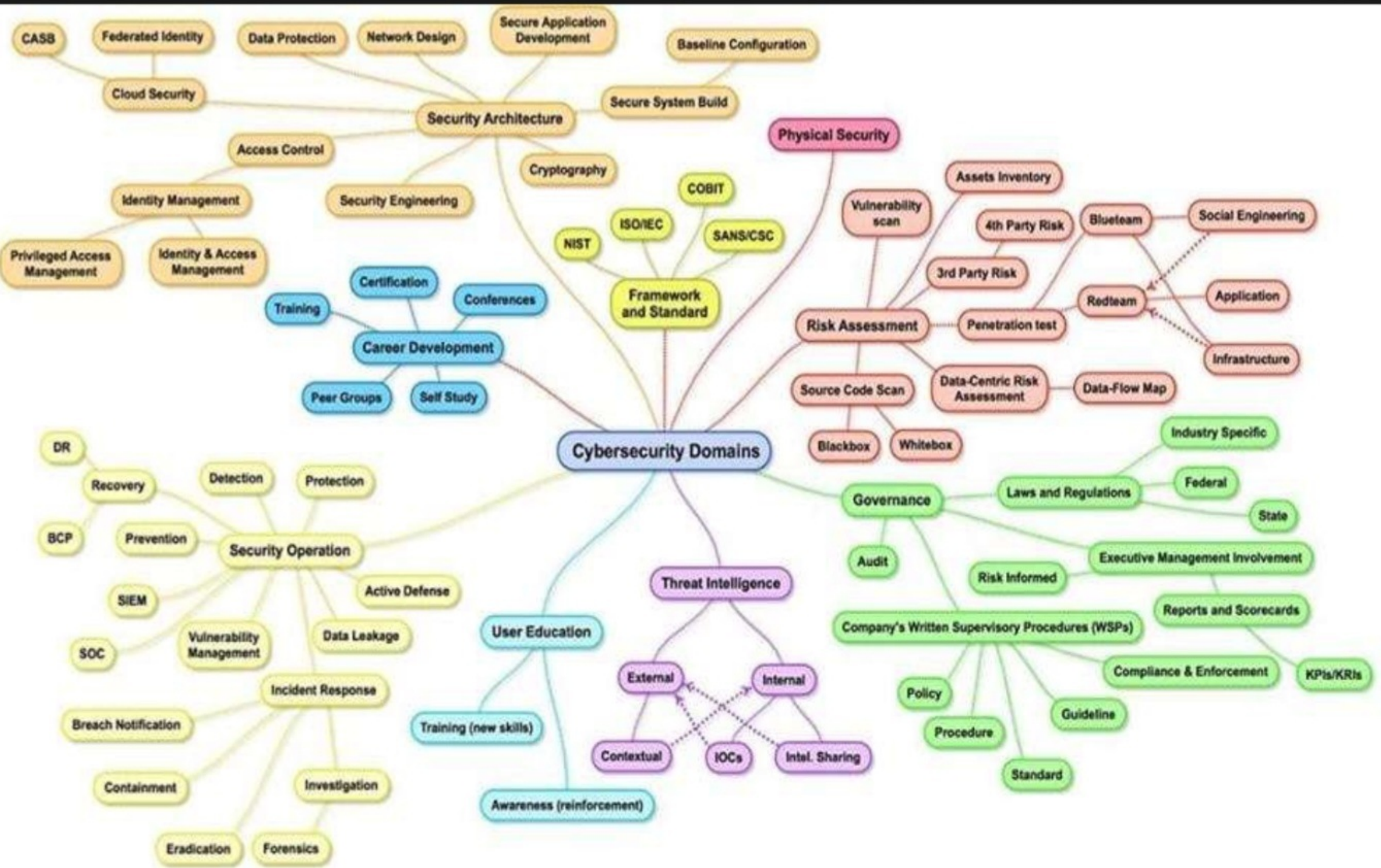
- There is **NO simple solution** to securing information
- Security 99.9 % Not found Why ?
  - This can be seen through the different types of attacks that users face today.
  - New technologies / applications
  - New Vulnerabilities
  - the difficulties in defending against these attacks

CYBER SECURITY JOBS

MAJOR CYBER SECURITY SPECIALTIES

- System Security
- Network Security
- Application Security
- Penetration Testing
- Threat / Bug Hunting
- Malware analysis
- Digital Forensic

CYBER SECURITY DOMAINS



JOB TYPES

- **Red Team (Pentest)**
  - Vulnerability Assessment.
  - Network Pentesting.
  - Web Pentesting.
  - Mobile Pentesting.
  - Wireless Pentesting.
  - Advanced Exploitation

- **Blue Team (SOC)**
  - Secure Network Design.
  - OS Hardening.
  - Network Hardening.
  - Monitoring.
  - Intrusion Detection.
  - Incident Response.
  - Digital Forensics.
  - Malware Analysis.
  - Threat Intelligence.
  - Threat Hunting.

WHAT IS PENETRATION TESTING ?

- **Pentesting, known as "penetration testing",**
  - security assessment, simulated attacks on an application (web, mobile, …etc) or network to check its **security posture**.
- **Team Responsibilities**
  - A highly skilled team
  - looking for vulnerabilities.
  - Looking for unauthorized gaining access to the system's features and data
  - **Simulated** cyberattack but **have authorization** to do that

WHAT IS SECURITY OPERATIONS CENTER (SOC)?

- **Security Operations Center (SOC)**
  - Centralized unit that deals with security issues on an organizational and technical level.
- **Team Responsibilities**
  - A highly skilled team
  - Defined definitions, policies, processes and utilizing technologies
  - Manage threats and Reduce security risk and respond to cyber emergencies
  - Monitor, Analyse, Correlate & Escalate Intrusion Events
  - Conduct Incident Management and Forensic Investigation
  - Maintain Security Community Relationships and assist in Crisis Operations
  - Protects mission-critical data and assets.
  - Helps provide continuity and efficient recovery

WORKING FIELDS IN EGYPT

WORKING FIELDS (COMPANIES TYPES) IN EGYPT

- **Vendors**
  IBM ,TrendMicro , Cisco

- **Integrators**
  - Zinad, Security meter ,Secure Misr, Fixed solutions , ITS ,Salic, Equinox

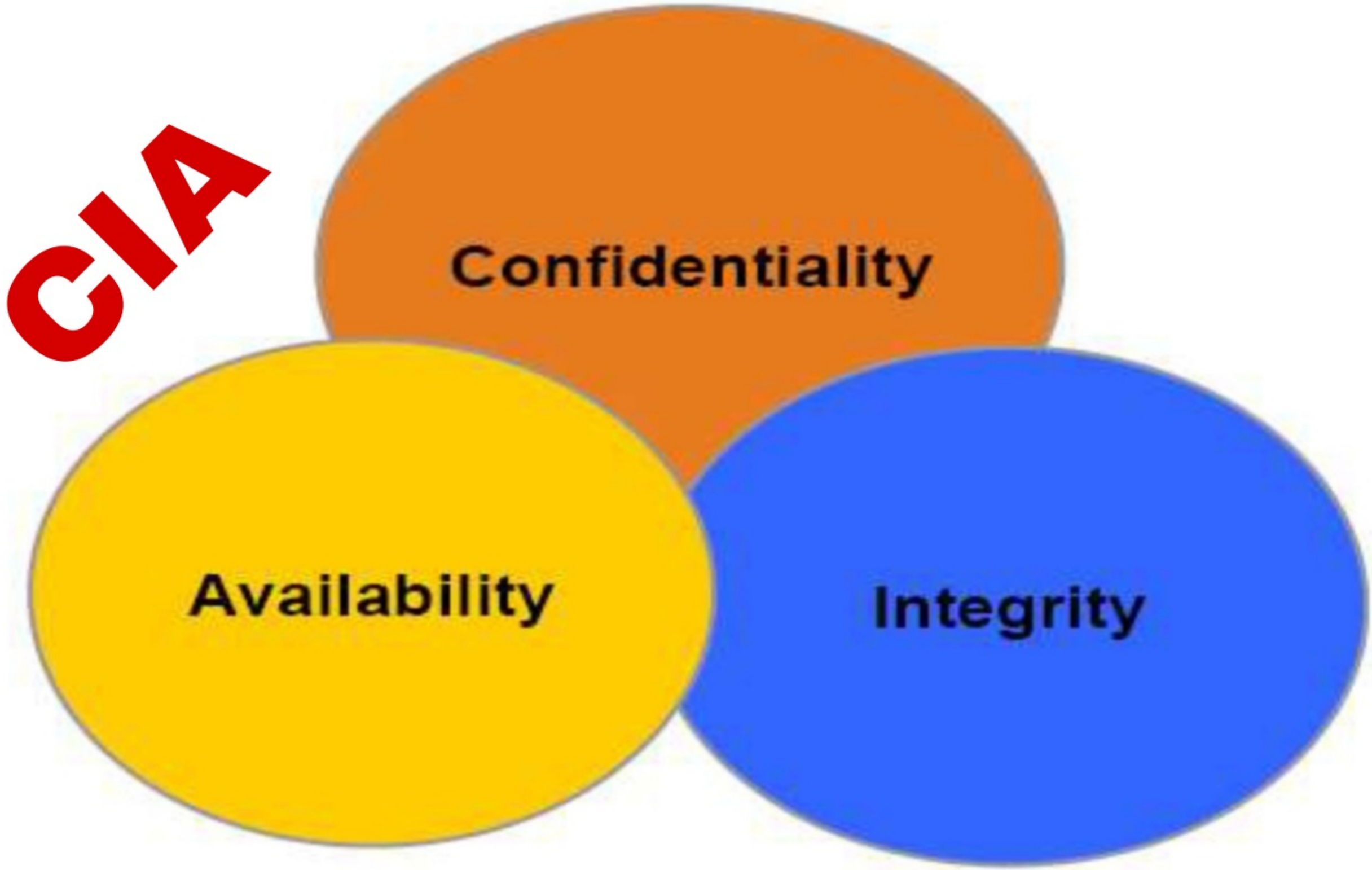
- **Customer's**
  - Banks {Qnb ,Alex ,CIB ..etc}
  - Telecom {Orange ,Vodafone ,Etisalat , We}
  - Gov {Cert , Central Bank,..}

CYBER SECURITY COMPANIES IN EGYPT

- Demand for cyber security companies in Egypt is high.
  - The growth of the internet era has ultimately increased the requirement for cybersecurity
- **Trend of cybersecurity** has led to creations of many **startup companies** with useful insights.
  - These cyber security service providers in Egypt are meant to save companies from any kind of theft.
- The **digitalization** led to **high** demand for these company

SECURITY TERMINOLOGIES

SECURITY GOALS (OBJECTIVES)



SECURITY GOALS TECHNICALLY DEFINED

- **Confidentiality**
  - Data transmitted or stored should only be revealed to an intended audience (Authorized persons) How ?
  - Done by encryption
- **Integrity**
  - Ensuring consistency of data (detect any modification) How ?
  - Done by Hashing
- **Availability**
  - Ensuring that legitimate users are not denied access to information and resources How ?
  - Done by Replications and Redundancy

FOCUS OF SECURTY IS RISK

- Risk is a **measure** of the cost of realized vulnerability
- It's **impossible** to totally eliminate risk
- Risk is the probability of a threat crossing or touching a vulnerability

Risk = Threat x Vulnerabilities

The risk is high when

The value of a vulnerable asset is high

The probability of successful attack (Threat) is high

Vulnerability is the degree of weakness which is inherent in every network and device.

THREATS

- A person, thing, event or idea which poses danger to an asset in terms of that asset's confidentiality, integrity, availability or legitimate use.

- **Accidental** (How to avoid ?)
  - Natural disasters
  - Revolutions
  - Force majeure
- **Intentional** (How to avoid ?)
  - Passive (No change)
  - Active (Change)

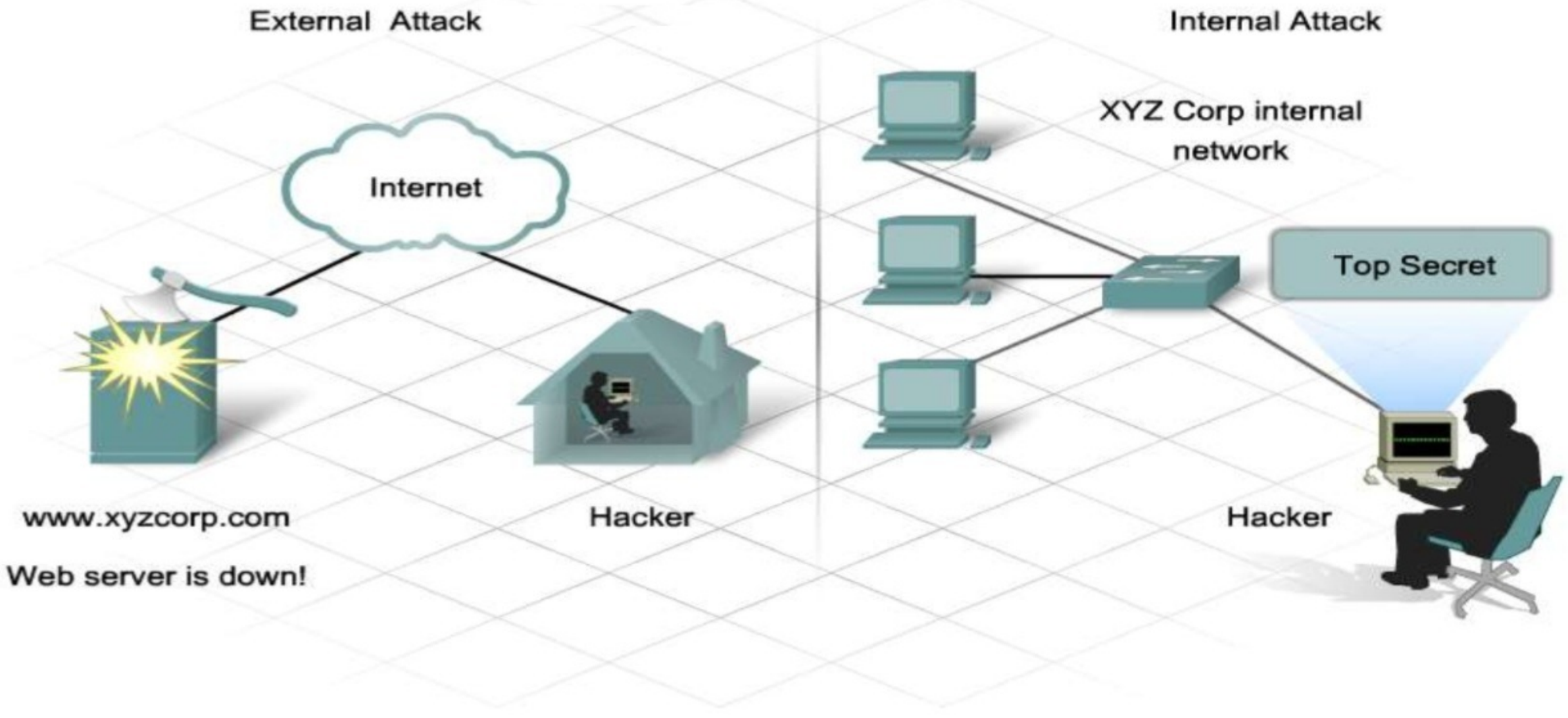
Assets : **Everything that have value** for an organization **or impact its** business continuity. This includes personals, hardware, software, physical devices and documents.

EXAMPLES OF RISKS

- Information Theft
  - Breaking into a computer to **obtain confidential information**. Information can be used or sold for various purposes. Exams
- Data Loss and Manipulation
  - Breaking onto a computer to **destroy or alter data records**.(Results)
- Identity Theft
  - **Personal Information is stolen** for the purpose of taking over **someone's identity**. Using this information anyone can obtain legal documents, apply for credits and make unauthorized online activities. Facebook Pages
- Disruption of Service
  - Preventing legitimate users from **accessing services** to which they should be entitled (Home internet access).

SOURCES OF NETWORK INTRUSION

- External
- Internal



SOCIAL ENGINEERING

- Social engineering is a term that refers to the ability of something or someone to influence the behavior of a group of people.

Hi this is Amy from the help desk. We need to upgrade the software on your computer after work hours. What is your user ID and password? You can change the password tomorrow when you log in.

Social Engineer

Ok, my user ID and password are...

Unsuspecting Employee at Xyz Corporation.

PHISHING

- Phishing is a form of social engineering where the phisher pretends to represent a legitimate outside organization.