Photo Album

by SIDDHARTH


C|EH
Certified Ethical Hacker
Module 01
Introduction to Ethical Hacking

Module Objectives

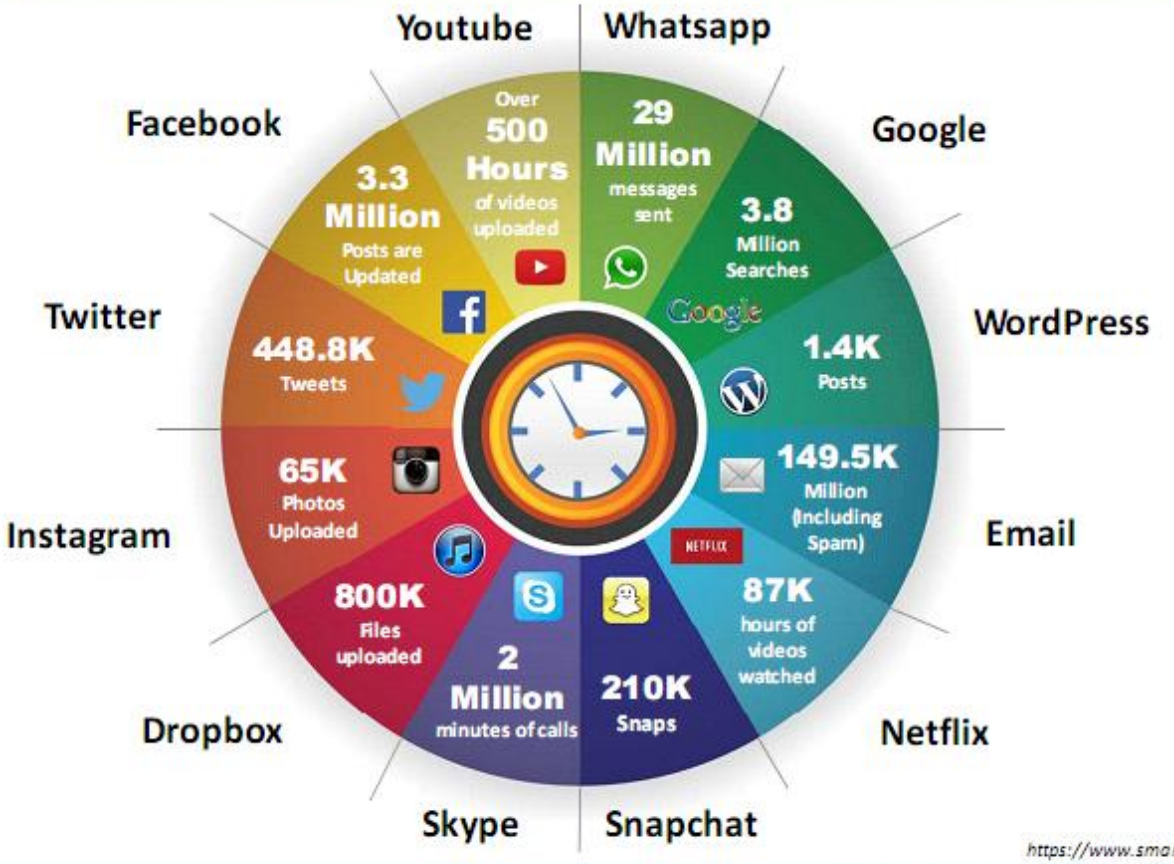
Module Objectives

- Overview of Current Security Trends
- Understanding the Elements of Information Security
- Understanding Information Security Threats and Attack Vectors
- Overview of Hacking Concepts, Types, and Phases
- Understanding Ethical Hacking Concepts and Scope
- Overview of Information Security Controls
- Overview of Penetration Testing
- Overview of Information Security Acts and Laws

Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Penetration Testing Concepts
7. Information Security Laws and Standards

Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds



https://www.smartinsights.com, https://www.go-globe.com

Essential Terminology

Hack Value

It is the notion among hackers that something is worth doing or is interesting

Zero-Day Attack

An attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability

Vulnerability

Existence of a weakness, design, or implementation error that can lead to an unexpected event compromising the security of the system

Daisy Chaining

It involves gaining access to one network and/or computer and then using the same information to gain access to multiple networks and computers that contain desirable information

Exploit

A breach of IT system security through vulnerabilities

Doxing

Publishing personally identifiable information about an individual collected from publicly available databases and social media

Payload

Payload is the part of an exploit code that performs the intended malicious action, such as destroying, creating backdoors, and hijacking computer

Bot

A "bot" is a software application that can be controlled remotely to execute or automate predefined tasks

Elements of Information Security

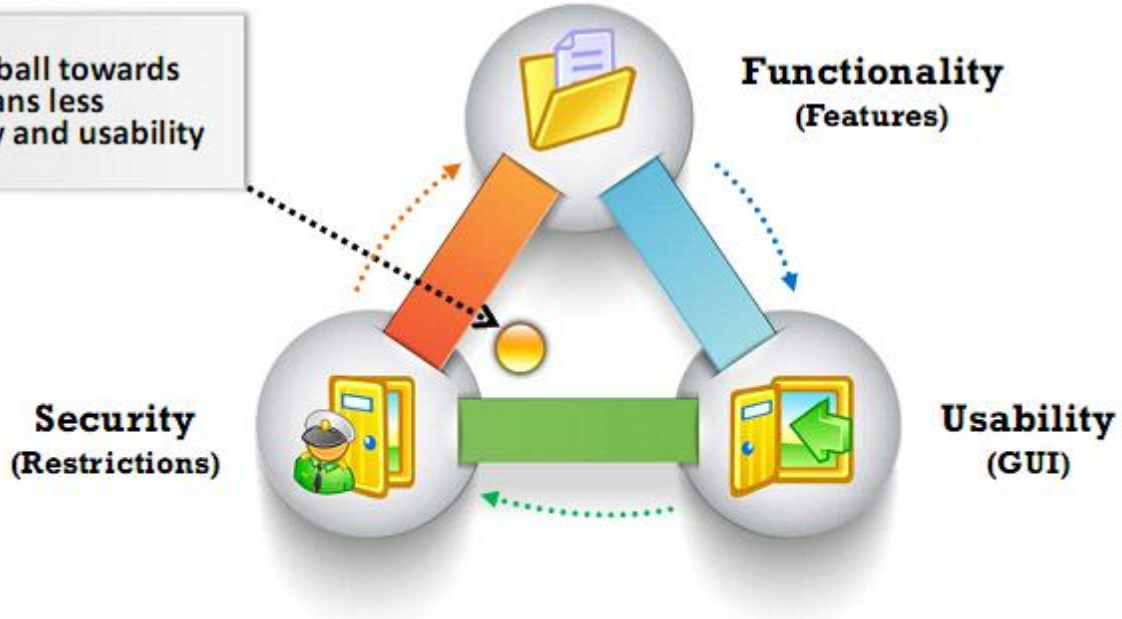
Information security is a state of well-being of information and infrastructure in which the possibility of **theft**, **tampering**, and **disruption of information and services** is kept low or tolerable

Confidentiality	Assurance that the information is accessible only to those **authorized to have access**
Integrity	The **trustworthiness of data or resources** in terms of preventing improper and unauthorized changes
Availability	Assurance that the systems responsible for delivering, storing, and processing information are accessible when **required by the authorized users**
Authenticity	Authenticity refers to the characteristic of a communication, document or any data that ensures the **quality of being genuine**
Non-Repudiation	**Guarantee** that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

The Security, Functionality, and Usability Triangle

Level of security in any system can be defined by the strength of three components:

Moving the ball towards security means less functionality and usability



Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Penetration Testing Concepts
7. Information Security Laws and Standards

Motives, Goals, and Objectives of Information Security Attacks

Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates out of the notion that the target system stores or processes something valuable and this leads to threat of an attack on the system
- Attackers try various tools and attack techniques to exploit vulnerabilities in a computer system or security policy and controls to achieve their motives

Motives Behind Information Security Attacks

- Disrupting business continuity
- Information theft and manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Financial loss to the target
- Propagating religious or political beliefs
- Achieving state's military objectives
- Damaging reputation of the target
- Taking revenge
- Demanding ransom

Top Information Security Attack Vectors

Cloud Computing Threats	• Cloud computing is an **on-demand delivery of IT capabilities** where sensitive data of organizations and their clients is stored • Flaw in one client's application cloud allow attackers to access other client's data
Advanced Persistent Threats (APT)	APT is an attack that is focused on **stealing information from the victim machine** without the user being aware of it
Viruses and Worms	Viruses and worms are the most prevalent networking threat that are **capable of infecting a network within seconds**
Ransomware	Ransomware **restricts access** to the computer system's files and folders and **demands an online ransom payment** to the malware creator(s) in order to remove the restrictions
Mobile Threats	Focus of attackers has shifted to **mobile devices** due to increased adoption of mobile devices for business and personal purposes and comparatively **lesser security controls**

Top Information Security Attack Vectors (Cont'd)

Botnet	A botnet is a huge network of the compromised systems used by an intruder to perform various network attacks
Insider Attack	It is an attack performed on a corporate network or on a single computer by an entrusted person (insider) who has authorized access to the network
Phishing	Phishing is the practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempts to acquire a user's personal or account information
Web Application Threats	Attackers target web applications to steal credentials, set up phishing site, or acquire private information to threaten the performance of the website and hamper its security
IoT Threats	• IoT devices include many software applications that are used to access the device remotely • Flaws in the IoT devices allows attackers access into the device remotely and perform various attacks

Information Security Threat Categories

Network Threats

- Information gathering
- Sniffing and eavesdropping
- Spoofing
- Session hijacking and Man-in-the-Middle attack
- DNS and ARP poisoning
- Password-based attacks
- Denial-of-Service attack
- Compromised-key attack
- Firewall and IDS attacks

Host Threats

- Malware attacks
- Footprinting
- Profiling
- Password attacks
- Denial-of-Service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Backdoor attacks
- Physical security threats

Application Threats

- Improper data/input validation
- Authentication and authorization attacks
- Security misconfiguration
- Information disclosure
- Hidden-field manipulation
- Broken session management
- Buffer overflow issues
- Cryptography attacks
- SQL injection
- Phishing
- Improper error handling and exception management

Types of Attacks on a System

Operating System Attacks

- Attackers search for vulnerabilities in an operating system's design, installation or configuration and exploit them to **gain access to a system**
- **OS Vulnerabilities**: Buffer overflow vulnerabilities, bugs in operating system, unpatched operating system, etc.

Misconfiguration Attacks

- Misconfiguration vulnerabilities affect web servers, application platforms, databases, networks, or frameworks that may result in **illegal access** or possible owning of the system

Application-Level Attacks

- Attackers **exploit the vulnerabilities in applications** running on organizations' information system to gain unauthorized access and steal or manipulate data
- **Application Level Attacks**: Buffer overflow, cross-site scripting, SQL injection, man-in-the-middle, session hijacking, denial-of-service, etc.

Shrink-Wrap Code Attacks

- Attackers **exploit default configuration and settings** of the off-the-shelf libraries and code

Information Warfare

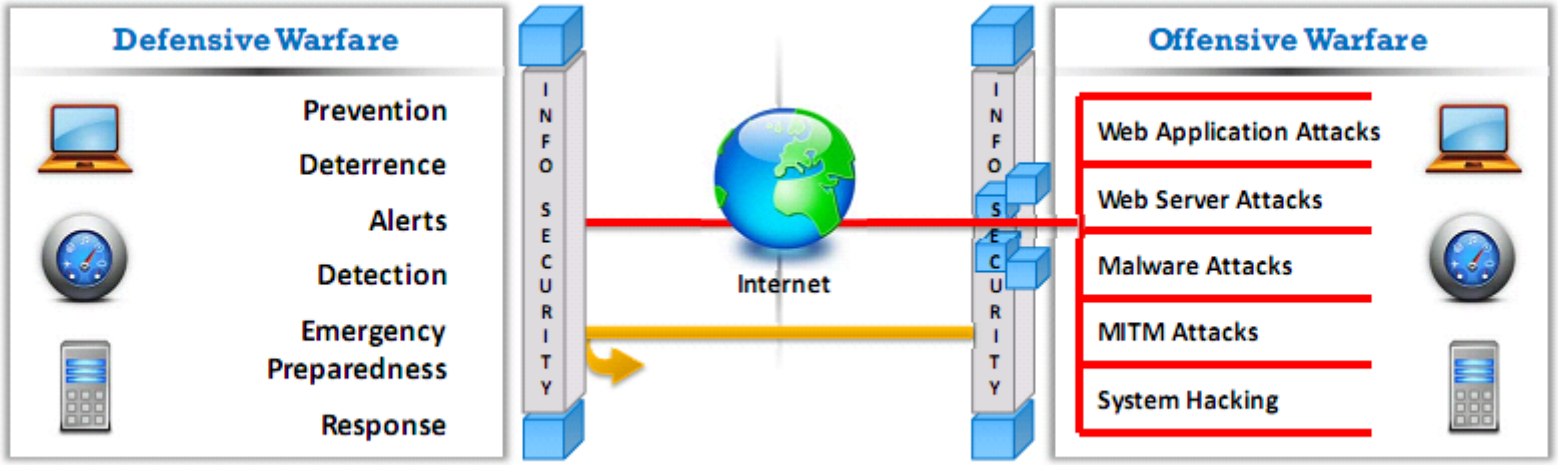
- The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) to take competitive advantages over an opponent

Defensive Information Warfare

It refers to all strategies and actions to defend against attacks on ICT assets

Offensive Information Warfare

It refers to information warfare that involves attacks against ICT assets of an opponent



Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Penetration Testing Concepts
7. Information Security Laws and Standards

What is Hacking?

- Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to the system resources

- It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose

- Hacking can be used to steal, pilfer, and redistribute intellectual property leading to **business loss**

Who is a Hacker?

01

Intelligent individuals with **excellent computer skills**, with the ability to create and explore into the computer's software and hardware

02

For some hackers, **hacking is a hobby** to see how many computers or networks they can compromise

03

Their intention can either be to gain knowledge or to **poke around to do illegal things**

Some do hacking with **malicious intent** behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.

Hacker Classes

01

Black Hats

Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers

02

White Hats

Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts. They have permission from the system owner

03

Gray Hats

Individuals who work both offensively and defensively at various times

04

Suicide Hackers

Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

05

Script Kiddies

An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers

06

Cyber Terrorists

Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks

07

State Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments

08

Hacktivist

Individuals who promote a political agenda by hacking, especially by defacing or disabling websites

Hacking Phases: Reconnaissance

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack
- Could be the future point of return, noted for ease of entry for an attack when more about the **target is known on a broad scale**
- Reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems

Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information **without directly interacting with the target**
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves **interacting with the target directly by any means**
- For example, telephone calls to the help desk or technical department

Hacking Phases: Scanning

Pre-Attack Phase	Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information on the basis of information gathered during reconnaissance
Port Scanner	Scanning can include use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, etc.
Extract Information	Attackers extract information such as **live machines**, port, port status, OS details, device type, **system uptime**, etc. to launch attack

Hacking Phases: Gaining Access

1. Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the computer or network

2. The attacker can gain access at the **operating system level**, **application level**, or **network level**

3. The attacker can **escalate privileges** to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised

4. Examples include **password cracking**, buffer overflows, denial of service, **session hijacking**, etc.

Hacking Phases: Maintaining Access

1. Maintaining access refers to the phase when the attacker tries to retain his or her **ownership of the system**
2. Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **Backdoors**, **RootKits**, or **Trojans**
3. Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**
4. Attackers use the compromised system to **launch further attacks**

Hacking Phases: Clearing Tracks

1

Covering tracks refers to the activities carried out by an attacker to **hide malicious acts**

2

The attacker's intentions include: **Continuing access** to the victim's system, remaining **unnoticed and uncaught**, deleting evidence that might lead to his prosecution

3

The attacker overwrites the server, system, and application logs to **avoid suspicion**

Attackers always cover their tracks to hide their identity

Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Penetration Testing Concepts
7. Information Security Laws and Standards

What is Ethical Hacking?

- Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** so as to ensure system security

- It focuses on simulating techniques used by attackers to **verify the existence of exploitable vulnerabilities** in the system security

- Ethical hackers performs security assessment of their organization **with the permission of concerned authorities**

Why Ethical Hacking is Necessary

To beat a hacker, you need to think like one!

Ethical hacking is necessary as it **allows counter attacks from malicious hackers** by anticipating methods used by them to break into a system

Reasons why Organizations Recruit Ethical Hackers

- To **prevent hackers** from gaining access to organization's information systems
- To **uncover vulnerabilities** in systems and explore their potential as a risk
- To analyze and **strengthen an organization's security posture** including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to **avoid security breaches**
- To help **safeguard customer's data** available in business transactions
- To **enhance security awareness** at all levels in a business

Why Ethical Hacking is Necessary (Cont'd)

Ethical Hackers Try to Answer the Following Questions

1. What can the intruder see on the **target system**? (Reconnaissance and Scanning phases)
2. What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)
3. Does anyone at the target **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)
4. If all the **components of information system** are adequately protected, updated, and patched
5. How much effort, time, and money is required to obtain **adequate protection**?
6. Are the **information security measures** in compliance with industry and legal standards?

Scope and Limitations of Ethical Hacking

Scope

- Ethical hacking is a crucial component of **risk assessment**, **auditing**, **counter fraud**, and information systems security **best practices**
- It is used to **identify risks** and highlight the **remedial actions**, and also reduces information and communications technology (ICT) costs by resolving those vulnerabilities

Limitations

- However, unless the businesses first know what it is that they are looking for and why they are **hiring an outside vendor to hack systems** in the first place, chances are there would not be much to gain from the experience
- An ethical hacker thus can only help the organization to better **understand their security system**, but it is up to the organization to **place the right guards** on the network

Skills of an Ethical Hacker

1 Technical Skills

- Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh
- Has in-depth **knowledge of networking** concepts, technologies and related hardware and software
- Should be a **computer expert** adept at technical domains
- Has **knowledge of security areas** and related issues
- Has "**high technical**" **knowledge** to launch the sophisticated attacks

2 Non-Technical Skills

Some of the non-technical characteristics of an ethical hacker include:

- **Ability to learn** and adapt new technologies quickly
- **Strong work ethics**, and good problem solving and communication skills
- Committed to **organization's security policies**
- Awareness of **local standards and laws**

Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Penetration Testing Concepts
7. Information Security Laws and Standards

Information Assurance (IA)

- IA refers to the assurance that the **integrity**, **availability**, **confidentiality**, and **authenticity** of information and information systems is protected during usage, processing, storage, and transmission of information
- Some of the processes that help in achieving information assurance include:

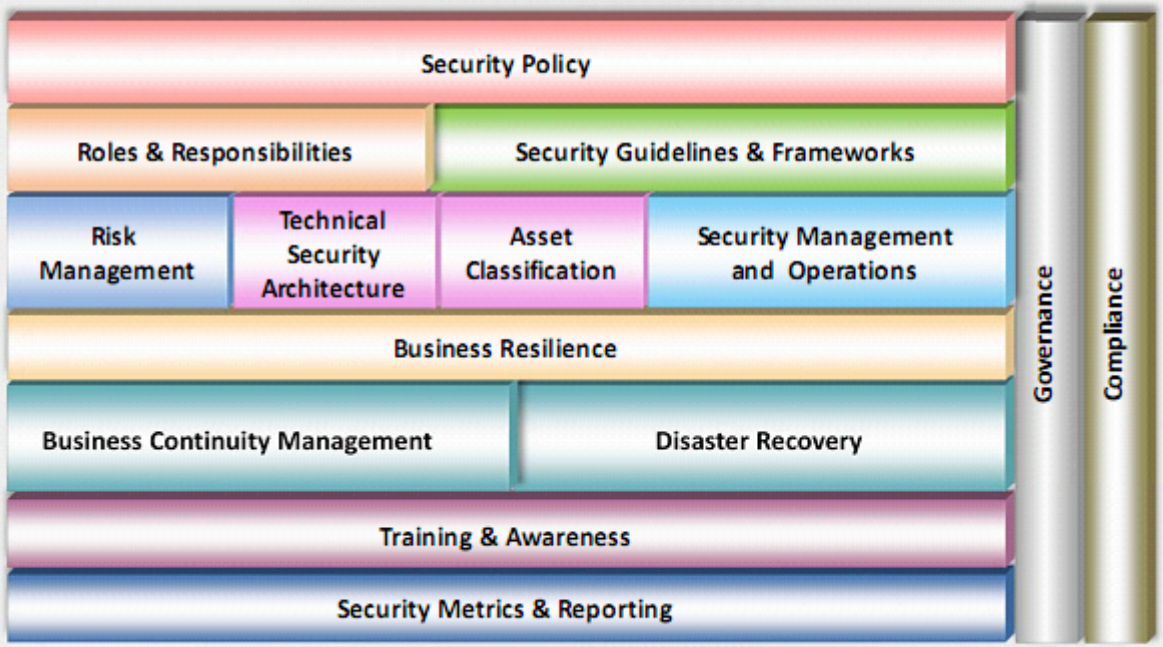
1. Developing local policy, process, and guidance
2. Designing network and user authentication strategy
3. Identifying network vulnerabilities and threats
4. Identifying problems and resource requirements
5. Creating plan for identified resource requirements
6. Applying appropriate information assurance controls
7. Performing certification and accreditation
8. Providing information assurance training

Information Security Management Program

- Programs that are designed to **enable a business to operate in a state of reduced risk**
- It encompasses all **organizational** and **operational processes**, and participants relevant to information security

Information Security Management Framework

It is a combination of **well-defined** policies, processes, procedures, standards, and guidelines to establish the required **level of information security**



Enterprise Information Security Architecture (EISA)

- EISA is a set of requirements, processes, principles, and models that **determines the structure and behavior of an organization's information systems**

EISA Goals

1. **Helps in monitoring and detecting network behaviors** in real time acting upon internal and externals security risks
2. Helps an organization to **detect and recover from security breaches**
3. Helps in prioritizing resources of an organization and **pays attention to various threats**
4. **Benefits organization in cost prospective** when incorporated in security provisions such as incident response, disaster recovery, event correlation, etc.
5. Helps in analyzing the procedure needed for the IT department to function properly and **identify assets**
6. **Helps to perform risk assessment** of an organization IT assets with the cooperation of IT staff

Network Security Zoning

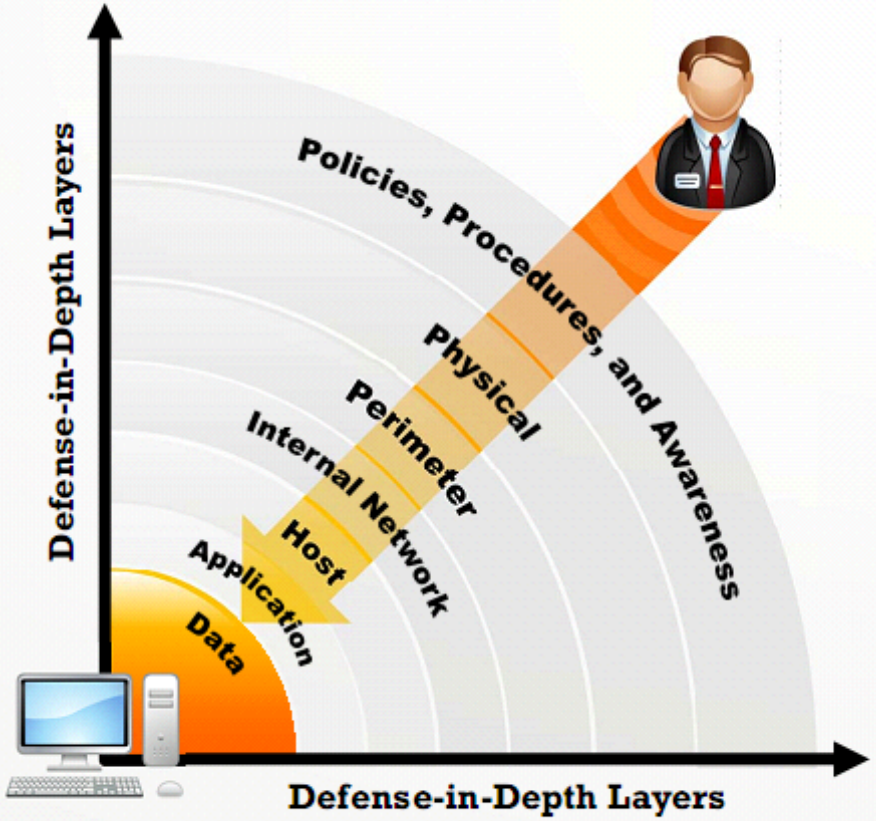
- Network security zoning mechanism allows an organization **to manage a secure network environment** by selecting the appropriate security levels for different **zones of Internet** and **Intranet networks**
- It helps in effectively monitoring and controlling **inbound and outbound traffic**

Examples of Network Security Zones

Internet Zone	Uncontrolled zone, as it is **outside the boundaries** of an organization
Internet DMZ	Controlled zone, as it **provides a barrier** between internal networks and Internet
Production Network Zone	Restricted zone, as it strictly **controls direct access** from uncontrolled networks
Intranet Zone	Controlled zone with **no heavy restrictions**
Management Network Zone	Secured zone with **strict policies**

Defense-in-Depth

- Defense-in-depth is a security strategy in which **several protection layers** are placed throughout an information system
- It helps to **prevent direct attacks** against an information system and data because a break in one layer only leads the attacker to the next layer



Information Security Policies

- Security policies are the foundation of the **security infrastructure**
- Information security policy defines the basic security requirements and rules to be implemented in order to **protect** and **secure organization's information systems**

Goals of Security Policies

1. Maintain an outline for the management and administration of network security
2. Protect an organization's computing resources
3. Eliminate legal liabilities arising from employees or third parties
4. Prevent waste of company's computing resources
5. Prevent unauthorized modifications of the data
6. Reduce risks caused by illegal use of the system resource
7. Differentiate the user's access rights
8. Protect confidential, proprietary information from theft, misuse, unauthorized disclosure

Types of Security Policies

Promiscuous Policy	▪ **No restrictions** on usage of system resources
Permissive Policy	▪ Policy begins wide open and only known **dangerous services/attacks or behaviors** are blocked ▪ It should be updated regularly to be effective
Prudent Policy	▪ It provides **maximum security** while allowing known but necessary dangers ▪ It **blocks all services** and only safe/ necessary services are enabled individually; everything is logged
Paranoid Policy	▪ It **forbids everything**, no Internet connection, or severely limited Internet usage

Examples of Security Policies

Access Control Policy

It defines the resources being protected and the rules that control access to them

User-Account Policy

It defines the account creation process, authority, and rights and responsibilities of user accounts

Remote-Access Policy

It defines who can have remote access, and defines access medium and remote access security controls

Information-Protection Policy

It defines the sensitivity levels of information, who may have access, how it is stored and transmitted, and how should it be deleted from storage media

Firewall-Management Policy

It defines access, management, and monitoring of firewalls in the organization

Special-Access Policy

This policy defines the terms and conditions of granting special access to system resources

Network-Connection Policy

It defines who can install new resources on the network, approve the installation of new devices, document network changes, etc.

Email Security Policy

It is created to govern the proper usage of corporate email

Passwords Policy

It provides guidelines for using strong password protection on organization's resources

Acceptable-Use Policy

It defines the acceptable use of system resources

Privacy Policies at Workplace

- Employers will have **access to employees' personal information** that may be confidential and they wish to keep private

Basic Rules for Privacy Policies at Workplace

Intimate employees about what you collect, why and what you will do with it

Keep employees' **personal information** accurate, complete, and up-to-date

Limit the collection of information and collect it by fair and lawful means

Provide employees **access to their personal information**

Inform employees about the **potential collection**, use, and disclosure of personal information

Keep employees' **personal information** secure

Note: Employees' privacy rule at workplace may differ from country to country

Steps to Create and Implement Security Policies

1. Perform **risk assessment** to identify risks to the organization's assets
2. Learn from **standard guidelines** and other organizations
3. Include **senior management** and all other staff in policy development
4. **Set clear penalties** and enforce them
5. Make **final version** available to all staff in the organization
6. Ensure every member of your staff **read, sign, and understand the policy**
7. Deploy tools to **enforce policies**
8. **Train your employees** and educate them about the policy
9. Regularly **review and update**

Security policy development team in an organization generally consists of Information Security Team (IST), Technical Writer(s), Technical Personnel, Legal Counsel, Human Resources, Audit and Compliance Team, and User Groups

HR/Legal Implications of Security Policy Enforcement

HR Implications of Security Policy Enforcement

- HR department is responsible to **make employees aware of security policies** and train them in best practices defined in the policy
- HR department works with management to **monitor policy implementation** and address any policy violation issue

Legal Implications of Security Policy Enforcement

- Enterprise information policies should be **developed in consultation with legal experts** and must comply to relevant local laws
- Enforcement of a security policy that may **violate users rights** in contravention to local laws may result in lawsuits against the organization

Physical Security

- Physical security is the **first layer of protection** in any organization
- It involves **protection of organizational assets** from environmental and man made threats

Why Physical Security?

- To prevent any **unauthorized access** to the systems resources
- To prevent **tampering/stealing of data** from the computer systems
- To safeguard against **espionage**, sabotage, damage, or theft
- To protect personnel and prevent **social engineering attacks**

Physical Security Threats

- Environmental threats
  - Floods and earthquakes
  - Fire
  - Dust
- Man made threats
  - Terrorism
  - Wars
  - Explosion
  - Dumpster diving and theft
  - Vandalism

Types of Physical Security Control

Preventive Controls	Prevent **security violations** and enforce various access control mechanisms Examples include door lock, security guard, etc.
Detective Controls	Detect security violations and **record any intrusion attempts** Examples include motion detector, alarm systems and sensors, video surveillance, etc.
Deterrent Controls	Used to discourage attackers and **send warning messages** to the attackers to discourage an intrusion attempt Examples include various types of warning signs
Recovery Controls	Used to recover from security violation and **restore information and systems** to a persistent state Examples include disaster recovery, business continuity plans, backup systems, etc.
Compensating Controls	Used as an alternative control when the **intended controls failed** or cannot be used Examples include hot site, backup power system, etc.

Physical Security Controls

Premises and company surroundings	Fences, gates, walls, guards, alarms, CCTV cameras, intruder systems, panic buttons, burglar alarms, windows and door bars, deadlocks, etc.
Reception area	Lock the important files and documents Lock equipment when not in use
Server and workstation area	Lock the systems when not in use, disable or avoid having removable media and DVD-ROM drives, CCTV cameras, workstation layout design
Other equipment such as fax, modem, and removable media	Lock fax machines when not in use, file the faxes obtained properly, disable auto answer mode for modems, do not place removal media at public places, and physically destroy the corrupted removal media
Access control	Separate work areas, implement biometric access controls (fingerprinting, retinal scanning, iris scanning, vein structure recognition, face recognition, voice recognition), entry cards, man traps, faculty sign-in procedures, identification badges, etc.
Computer equipment maintenance	Appoint a person to look after the computer equipment maintenance
Wiretapping	Inspect all the wires carrying data routinely, protect the wires using shielded cables, never leave any wire exposed
Environmental control	Humidity and air conditioning, HVAC, fire suppression, EMI shielding, and hot and cold aisles

What is Risk?

- Risk refers to a degree of **uncertainty** or expectation that an adverse event may cause damage to the system
- Risks are categorized into different levels according to their estimated impact on the system
- A risk matrix is used to scale risk by considering the **probability**, **likelihood**, and **consequence/impact** of the risk

Risk Levels

Risk Level	Action
Extreme / High	➢ Immediate measures should be performed to combat risk ➢ Identify and impose controls to reduce risk to a reasonably low level
Medium	➢ Immediate action is not required but it should implement quickly ➢ Implement controls as soon as possible to reduce risk to a reasonably low level
Low	➢ Take preventive steps to mitigate the effects of risk

Risk Matrix

Probability		Consequences				
		Insignificant	Minor	Moderate	Major	Severe
81-100%	Likelihood: Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 – 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 – 20%	Very Low Probability	Low	Low	Medium	Medium	High

Risk Management

- Risk management is the process of **reducing and maintaining risk at an acceptable level** by means of a well-defined and actively employed security program

Risk Management Phases

Risk Identification	**Identifies the sources**, causes, consequences, etc. of the internal and external risks affecting the security of the organization
Risk Assessment	**Assesses the organization's risk** and provides an estimate on the likelihood and impact of the risk
Risk Treatment	**Selects and implements appropriate controls** on the identified risks
Risk Tracking	**Ensures appropriate controls are implemented** to handle risks and identifies the chance of a new risk occurring
Risk Review	**Evaluates the performance** of the implemented risk management strategies

Key Roles and Responsibilities in Risk Management

Senior Management	The support and **involvement of senior management** is required for effective risk management
Chief Information Officer (CIO)	Responsible for IT planning, budgeting, and performance based on a risk management program
System and Information Owners	Responsible for the **appropriate security control** use to maintain confidentiality, integrity and availability for an information system
Business and Functional Managers	Responsible for **making trade-off decisions** in the risk management process
IT security program managers and computer security officers (ISSO)	Responsible for an organization's **information security programs**
IT Security Practitioners	Responsible for implementing **security controls**
Security Awareness Trainers	Responsible for **developing and providing appropriate training** on the risk management process

Threat Modeling

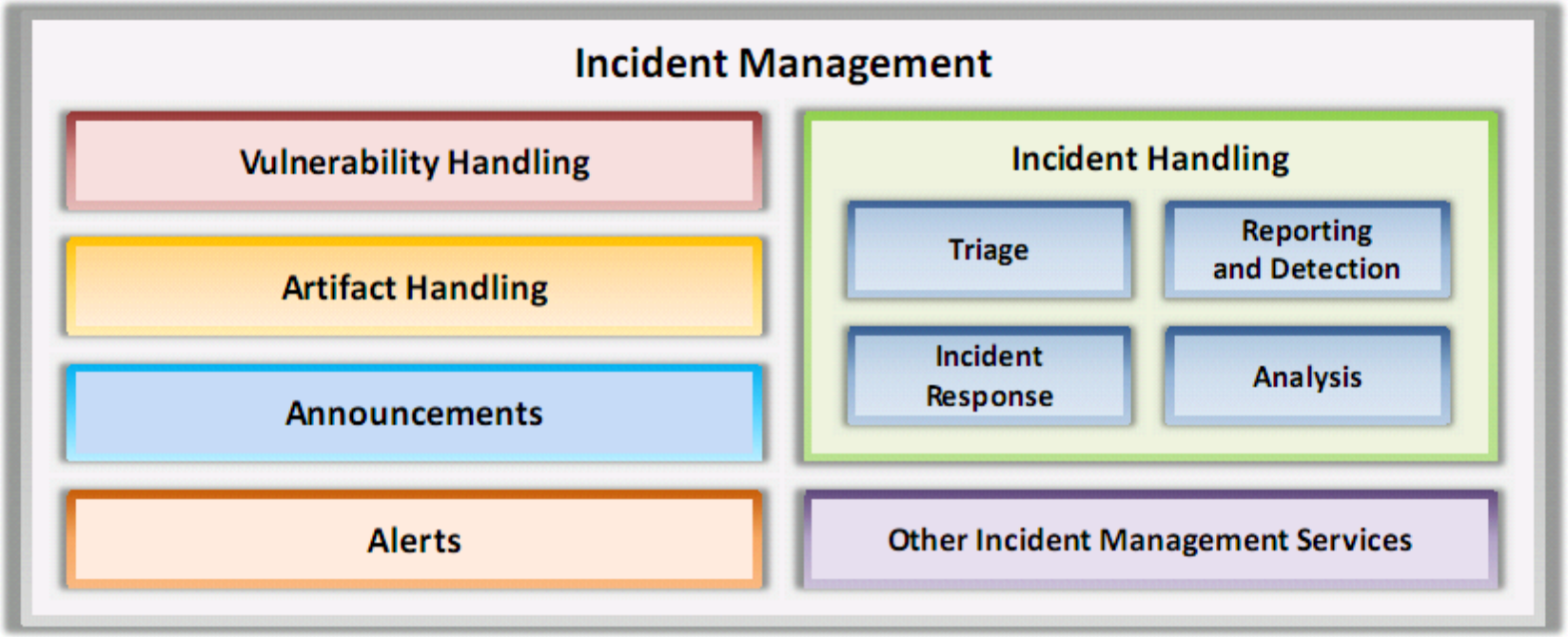
Threat modeling is a **risk assessment approach** for analyzing security of an application by capturing, organizing, and analyzing all the information that affects the security of an application

Threat Modeling Process

01	Identify Security Objectives	Helps to determine how much **effort needs to be put** on subsequent steps
02	Application Overview	Identify the **components**, **data flows**, and trust boundaries
03	Decompose Application	Helps you to find more relevant and more **detailed threats**
04	Identify Threats	Identify threats relevant to your **control** scenario and context using the information obtained in steps 2 and 3
05	Identify Vulnerabilities	**Identify weaknesses** related to the threats found using **vulnerability categories**

Incident Management

- Incident management is a set of defined processes to **identify**, **analyze**, **prioritize**, and **resolve security incidents** to restore normal service operations as quickly as possible and prevent future recurrence of the incident



Incident Management Process

1. Preparation for Incident Handling and Response
2. Detection and Analysis
3. Classification and Prioritization
4. Notification
5. Containment
6. Forensic Investigation
7. Eradication and Recovery
8. Post-incident Activities

Responsibilities of an Incident Response Team

1. Managing security issues by taking a **proactive approach** towards the customers' security vulnerabilities and **by responding effectively** to potential information security incidents
2. **Developing or reviewing** the processes and procedures that must be followed in response to an incident
3. Managing the response to an incident and ensuring that **all procedures are followed** correctly in order **to minimize** and **control the damage**
4. **Identifying** and **analyzing** what has happened during an incident, including the impact and threat
5. Providing a **single point of contact** for reporting security incidents and issues
6. Reviewing **changes in legal and regulatory requirements** to ensure that all processes and procedures are valid
7. **Reviewing existing controls** and recommending steps and technologies to **prevent future security incidents**
8. Establishing **relationship with local law enforcement agency, government agencies**, key partners, and suppliers

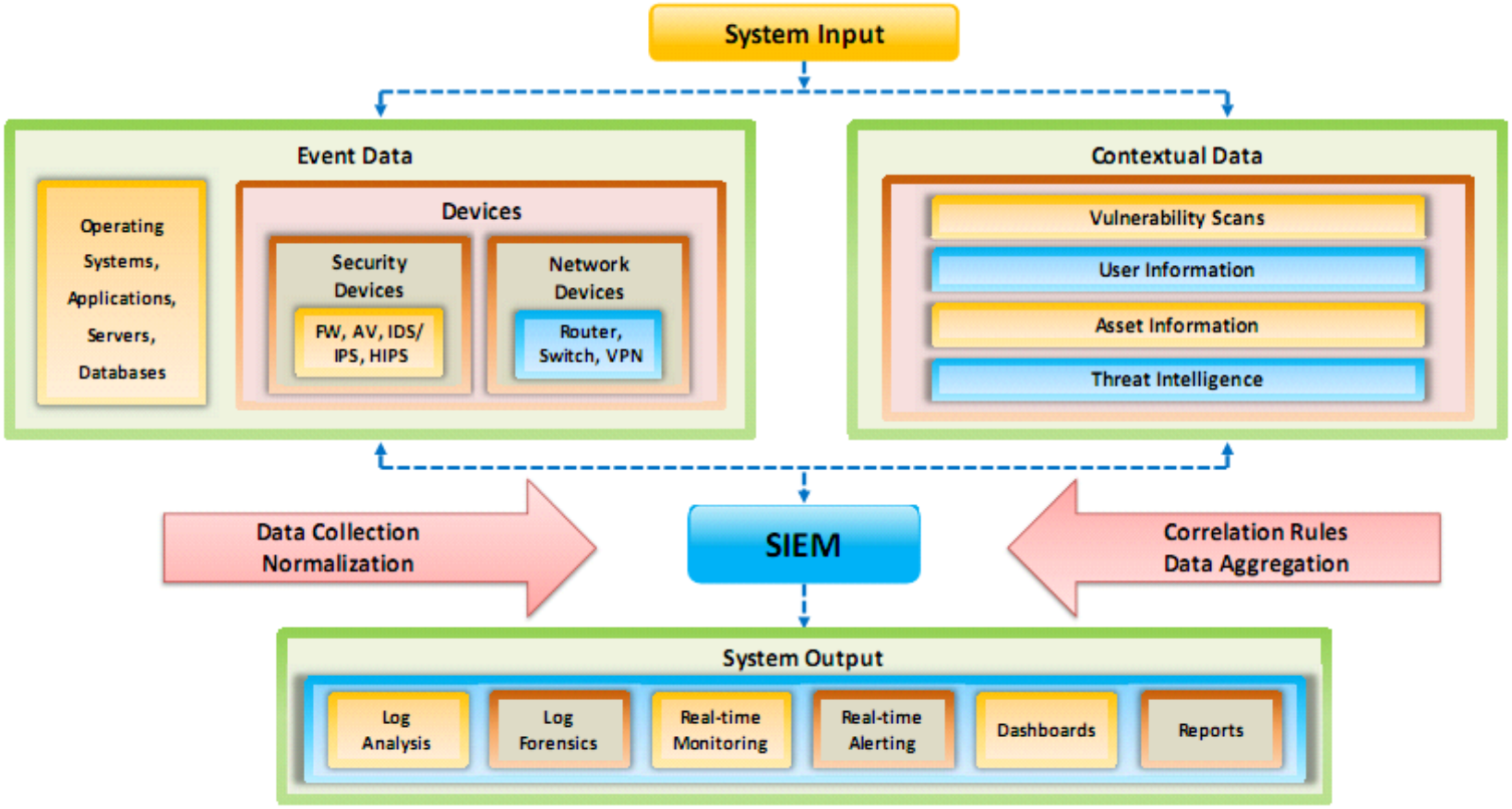
Security Incident and Event Management (SIEM)

- SIEM performs **real-time SOC** (Security Operations Center) functions like identifying, monitoring, recording, auditing, and analyzing security incidents
- It provides security by **tracking suspicious end-user behavior** activities within a real-time IT environment
- It provides security management services combining **Security Information Management** (SIM), and **Security Event Management** (SEM)
  - SIM supports permanent storage, analysis and reporting of log data
  - SEM deals with real-time monitoring, correlation of events, notifications, and console views
- SIEM protects organization's IT assets from **data breaches** occurred due to internal and external threats

SIEM Functions

- Log Collection
- Log Analysis
- Event Correlation
- Log Forensics
- IT Compliance and Reporting
- Application Log Monitoring
- Object Access Auditing
- Data Aggregation
- Real-time Alerting
- User Activity Monitoring
- Dashboards
- File Integrity Monitoring
- System and Device Log Monitoring
- Log Retention

SIEM Architecture



User Behavior Analytics (UBA)

- UBA is the process of **tracking user behavior** to detect malicious attacks, potential threats, and financial frauds
- It provides **advanced threat detection** in an organization to monitor specific behavioral characteristics of the employees
- UBA technologies are designed to **identify variations** in **traffic patterns** caused by user behaviors which can be either disgruntled employees or malicious attackers

Why User Behavior Analytics is Effective?

- Analyzes different patterns of human behavior and large volumes of user's data
- Monitors geolocation for each login attempt
- Detects malicious behavior and reduces risk
- Monitors privileged accounts and gives real time alerts for suspicious behavior
- Provides insights to security teams
- Produces results soon after deployment

Network Security Controls

Network security controls are used to **ensure the confidentiality**, **integrity**, and **availability** of the network services

1. Access Control
2. Identification
3. Authentication
4. Authorization
5. Cryptography
6. Accounting
7. Security Policy

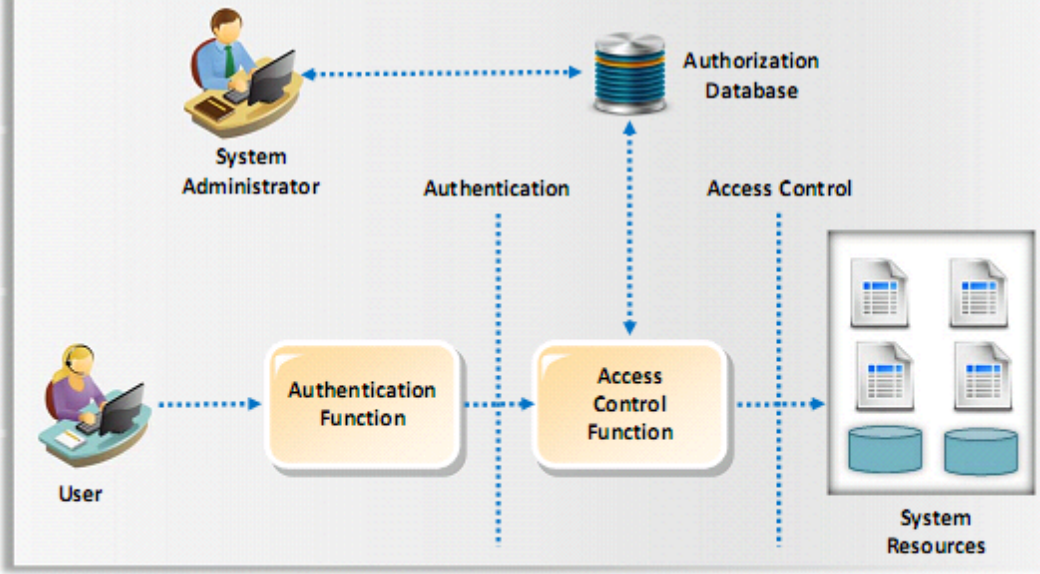
Access Control

- Access control is the **selective restriction** of access to a place or other system/network resource
- It **protects information assets** by determining who can and cannot access them
- It **involves user identification**, authentication, authorization, and accountability

Access Control Terminology

Subject	It refers to a **particular user or process** which wants to access the resource
Object	It refers to a specific resource that the user wants to access such as a file or any **hardware device**
Reference Monitor	It checks the **access control rule** for specific restrictions
Operation	It represents the **action taken** by the object on the subject

Access Control Principles



Types of Access Control

Discretionary Access Control (DAC)

- It permits the user, who is granted access to information, to decide how **to protect the information**, and the **level of sharing** desired
- Access to files is **restricted to users** and **groups** based upon their identity and the groups to which the users belong

Mandatory Access Control (MAC)

- It does not permit the end user **to decide who can access the information**
- It does not permit the user to **pass privileges** to other users, as the access could then be circumvented

Role-based Access

- Users can be assigned **access to systems**, **files**, and **fields on a one-by-one basis** whereby access is granted to the user for a particular file or system
- It can simplify the **assignment of privileges** and ensure that individuals have all the privileges necessary to perform their duties

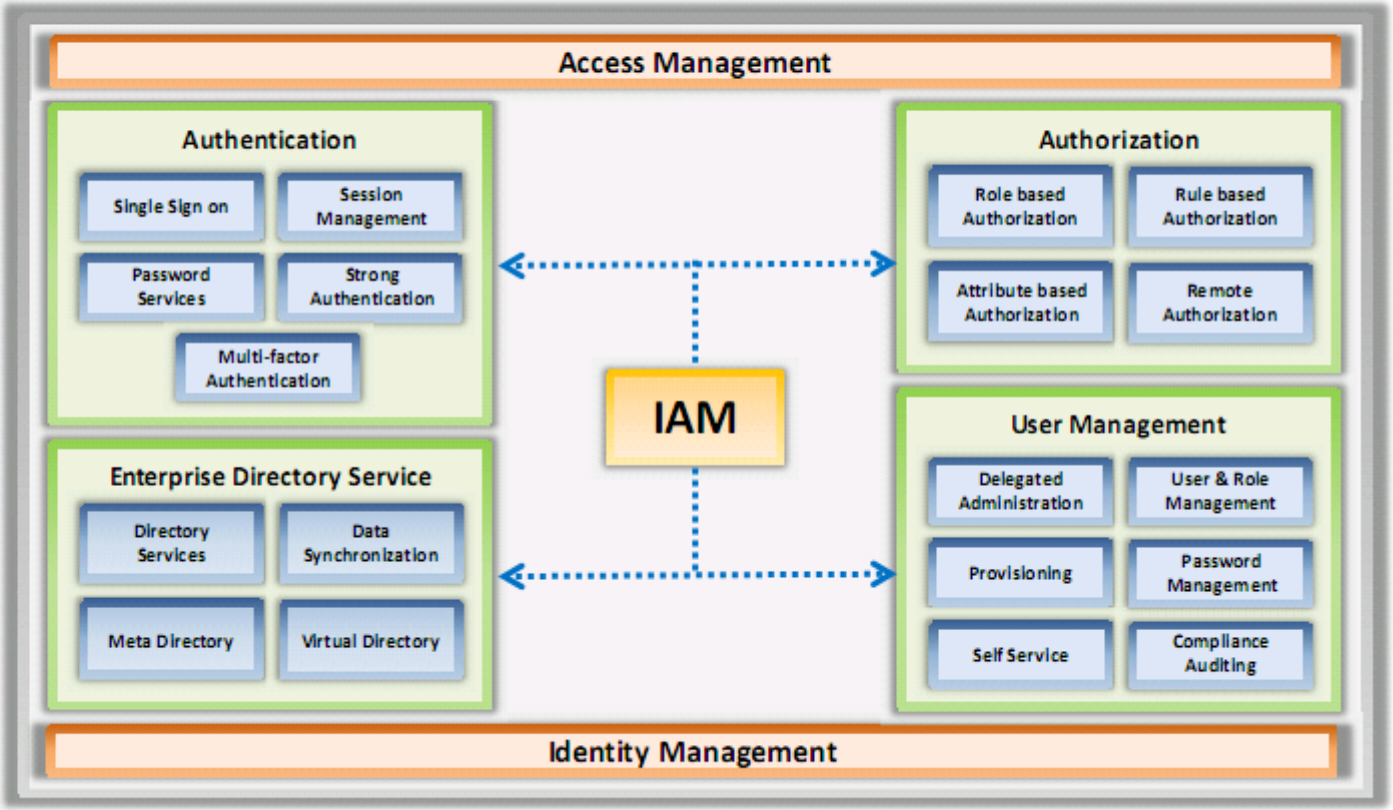
User Identification, Authentication, Authorization, and Accounting

Identification	Describes a method to ensure that an **individual holds a valid identity** (Ex: username, account no, etc.)
Authentication	It involves validating the **identity of an individual** (Ex: Password, PIN, etc.)
Authorization	It involves **controlling the access** of information for an individual (Ex: A user can only read the file but not write to or delete it)
Accounting	It is a method of keeping **track** of **user actions** on the network. It keeps track of who, when, how the users access the network. It helps in identifying authorized and unauthorized actions

Identity and Access Management (IAM)

- Identity and Access Management (IAM) is a framework that consists of users, procedures, and software products to **manage user digital identities** and access to resources of an organization
- It ensures that *"the right users obtain access to the right information at the right time"*
- The services provided by IAM are classified into four distinct components:
  - Authentication
  - Authorization
  - User Management
  - Enterprise Directory Services (Central User Repository)

IAM Framework



Data Leakage

- Data leakage refers to unauthorized access or disclosure of **sensitive or confidential data**
- Data leakage may happen electronically through an email or malicious link or via some physical method such as device theft, hacker break-ins, etc.

Major Risks to Organizations

- Loss of customer loyalty
- Potential litigations
- Heavy fines
- Decline in share value
- Loss of brand name
- Loss of reputation
- Reduction of sales and revenue
- Unfavorable media attention
- Unfavorable competitor advantage
- Insolvency/liquidation
- Loss of new and existing customers
- Monetary loss
- Prone to cyber criminal attacks
- Loss of productivity
- Discloses trade secrets
- Pre-release of latest technology developed by company
- Loss of proprietary and customer information
- Ready to release projects gets pirated

Data Leakage Threats

Insider Threats

- Disgruntled or negligent employees may leak sensitive data knowingly or unknowingly to the outside world incurring huge financial losses and business interruptions
- Employees may use various techniques such as eavesdropping, shoulder surfing, dumpster diving, etc. to gain unauthorized access to information in violation of corporate policies

Reasons for Insider Threats

- Inadequate security awareness and training
- Lack of proper management controls for monitoring employee activities
- Use of insecure mode of data transfers

External Threats

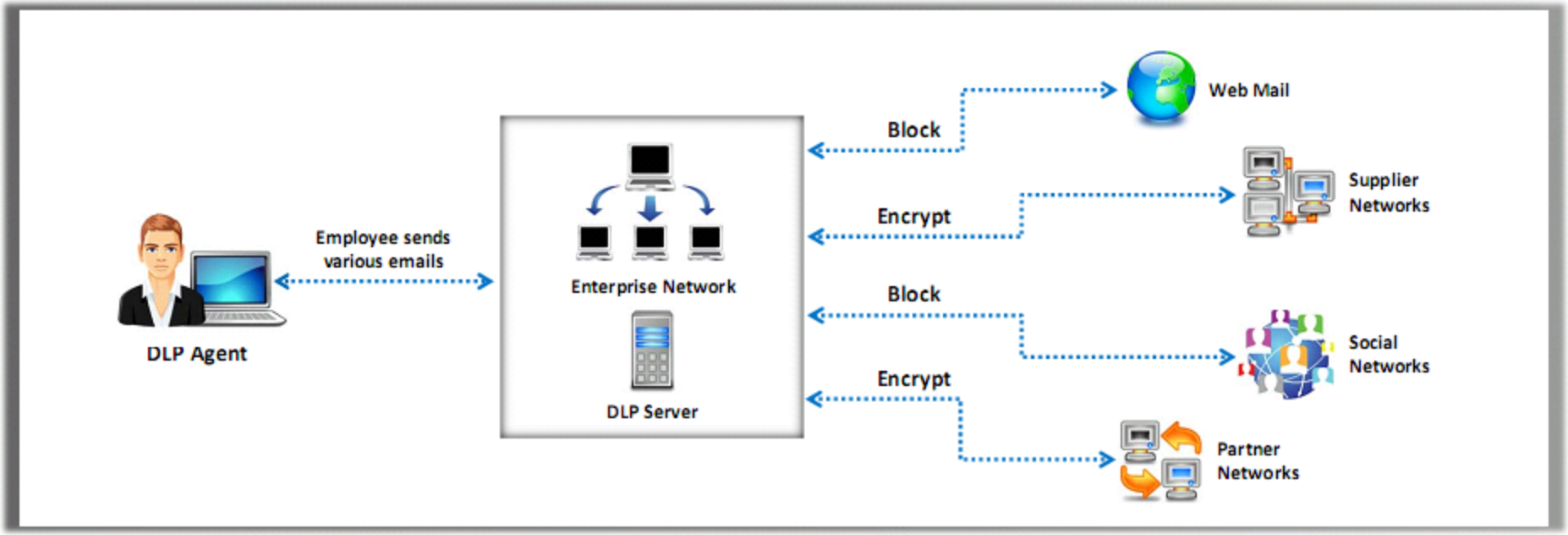
- Attackers take advantage of insider's vulnerabilities to perform various attacks by stealing credentials of a legitimate employee
- This gives the attacker unlimited access to the target network

Examples of External Threats

- Hacking/Code Injection Attacks
- Malware
- Phishing
- Corporate Espionage/Competitors
- Business Partners/Contractors

What is Data Loss Prevention (DLP)?

Data Loss Prevention (DLP) refers to the **identification and monitoring of sensitive data** to ensure that end users do not send sensitive information outside the corporate network



Data Backup

- Data is the **heart** of any organization; data loss can be very costly as it may have financial impact to any organization

- Backup is the process of making a **duplicate copy** of critical data that can be used to restore and recover purposes when a primary copy is lost or corrupted either accidentally or on purpose

- Data backup plays a **crucial role** in maintaining business continuity by helping organizations recover from IT disasters such as hardware failures, application failures, security breaches, human error or deliberate sabotage, etc.

Backup Strategy/Plan

- Identifying critical **business data**
- Selecting the **backup media**
- Selecting a **backup technology**
- Selecting the appropriate **RAID levels**
- Selecting an **appropriate backup** method
- Choosing the **backup location**
- Selecting the **backup types**
- Choosing the **right backup** solution
- Conducting a recovery **drill test**

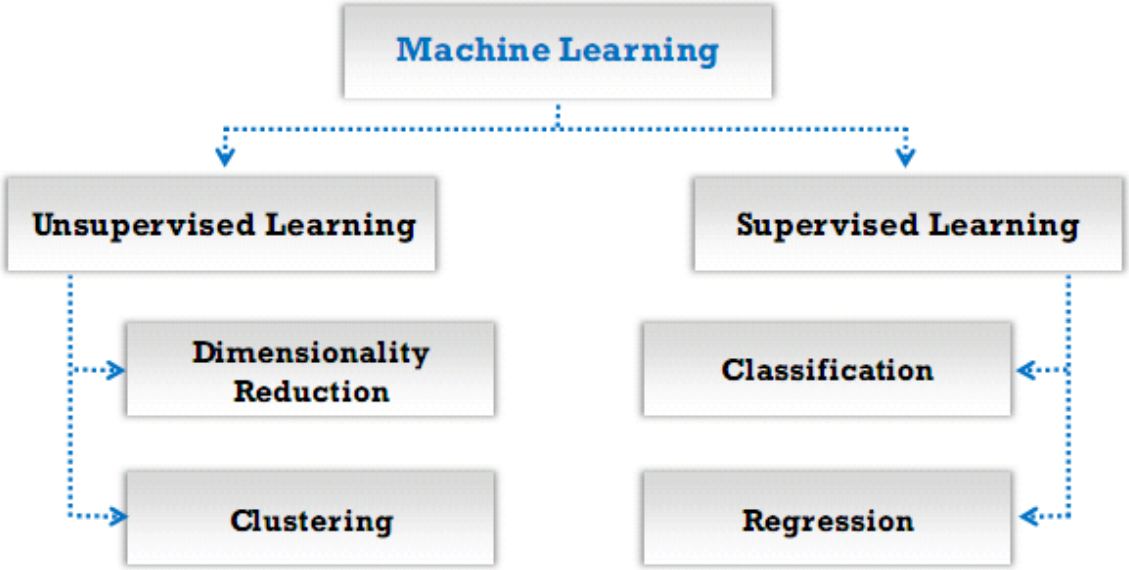
Data Recovery

- Data recovery is a process for the recovery of data that may have been accidentally/intentionally **deleted** or **corrupted**
- Deleted items include files, folders and partitions from electronic storage media (hard drives, removable media, optical devices, etc.)
- A majority of data that is lost is **recoverable**. There are situations where damage to the data is permanent and irreversible and cannot be recovered
- When attempting to recover data from a target, use different data recovery tools

Role of AI/ML in Cyber Security

- Machine learning (ML) and artificial intelligence (AI) are now vastly used across various industries and applications due to the increase in the computing power, data collection and storage capabilities
- Machine Learning (ML) is unsupervised self-learning system that is used to define what the normal network looks like along with its devices and then use this to backtrack and report any deviations and anomalies in real time
- AI and ML in cyber security helps in identifying new exploits and weaknesses which can be easily analyzed to mitigate further attacks

- ML classification techniques-
  - Supervised learning makes use of algorithms that inputs a set of labeled training data, with aim of learning the differences between the labels
  - Unsupervised learning makes use of algorithms that input unlabeled training data, with the aim of deducing all categories by itself



Role of AI/ML in Cyber Security (Cont'd)

1. By 2018, 25% of security products used for detection will have some form of machine learning built into them
2. By 2020, 10% of penetration tests will be conducted by machine-learning-based smart machines, up from 0% in 2016
3. By 2020, 75% of security products will be embedded with Advanced Security Analytics

https://www.gartner.com

Role of AI/ML in Cyber Security (Cont'd)

According to CB Insights, alongside overall rising investment activity, a number of cybersecurity companies are emerging to offer novel solutions to cyber threats by leveraging the advantages of artificial intelligence (AI)

Cybersecurity is the fourth most active industry for deals to companies applying AI

Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Penetration Testing Concepts
7. Information Security Laws and Standards

Penetration Testing

- Penetration testing is a method of evaluating the security of an information system or network by **simulating an attack to find out vulnerabilities** that an attacker could exploit
- **Security measures** are actively analyzed for design weaknesses, technical flaws and vulnerabilities
- A penetration test will not only point out vulnerabilities, but will also **document** how the weaknesses can be exploited
- The results are delivered comprehensively in a **report**, to executive management and technical audiences

Why Penetration Testing?

Identify the threats facing an **organization's information assets**

Reduce an organization's expenditure on IT security and enhance **Return On Security Investment** (ROSI) by identifying and remediating vulnerabilities or weaknesses

Provide assurance with comprehensive **assessment of organization's security** including policy, procedure, design, and implementation

Gain and maintain certification to an **industry regulation** (BS7799, HIPAA etc.)

Adopt **best practices** in compliance to legal and industry regulations

For testing and validating the efficacy of **security protections and controls**

For changing or upgrading **existing infrastructure** of software, hardware, or network design

Focus on **high-severity vulnerabilities** and emphasize **application-level security issues** to development teams and management

Provide a comprehensive approach of **preparation steps** that can be taken to prevent upcoming exploitation

Evaluate the efficacy of **network security devices** such as firewalls, routers, and web servers

Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

Security Audit

- A security audit just checks whether the organization is following a set of standard **security policies and procedures**

Vulnerability Assessment

- A vulnerability assessment focuses on **discovering the vulnerabilities in the information system** but provides no indication if the vulnerabilities can be exploited or the amount of damage that may result from the successful exploitation of the vulnerability

Penetration Testing

- Penetration testing is a methodological approach to security assessment that **encompasses the security audit** and vulnerability assessment and demonstrates if the vulnerabilities in system can be successfully exploited by attackers

Blue Teaming/Red Teaming

Blue Teaming

- An approach where a set of **security responders** performs analysis of an information system to assess the adequacy and efficiency of its security controls
- Blue team has **access** to all the organizational resources and information
- Primary role is to detect and mitigate red team (attackers) activities, and to anticipate how **surprise attacks** might occur

Red Teaming

- An approach where a team of ethical hackers perform penetration test on an information system with **no or very limited access** to the organization's internal resources
- It may be conducted **with** or **without** warning
- It is proposed to **detect network** and **system vulnerabilities** and **check security** from an attacker's perspective approach to network, system, or information access

Types of Penetration Testing

Black-box

- **No prior knowledge** of the infrastructure to be tested
  - Blind Testing
  - Double Blind Testing

White-box

- **Complete knowledge** of the infrastructure that needs to be tested

Grey-box

- **Limited knowledge** of the infrastructure that needs to be tested

Phases of Penetration Testing

Pre-Attack Phase

- Planning and preparation
- Methodology designing
- Network information gathering

Attack Phase

- Penetrating perimeter
- Acquiring target
- Escalating privileges
- Execution, implantation, retracting

Post-Attack Phase

- Reporting
- Clean-up
- Artifact destruction

Security Testing Methodology

- A security testing or pen testing methodology refers to a methodological approach to **discover and verify vulnerabilities in the security mechanisms of an information system**; thus enabling administrators to apply appropriate security controls to protect critical data and business functions

Examples of Security Testing Methodologies

OWASP	The Open Web Application Security Project (OWASP) is an open-source application security project that **assist the organizations to purchase, develop and maintain software tools**, software applications, and knowledge-based documentation for Web application security
OSSTMM	Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for performing **high quality security tests** such as methodology tests: data controls, fraud and social engineering control levels, computer networks, wireless devices, mobile devices, physical security access controls and various security processes
ISSAF	Information Systems Security Assessment Framework (ISSAF) is an open source project aimed to provide a security assistance for professionals. The mission of ISSAF is to "**research**, **develop**, **publish**, and **promote** a complete and practical generally accepted information systems security assessment framework"
EC-Council LPT Methodology	LPT Methodology is a industry accepted comprehensive **information system security auditing framework**

Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Penetration Testing Concepts
7. Information Security Laws and Standards

Payment Card Industry Data Security Standard (PCI DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data
- High level overview of the PCI DSS requirements developed and maintained by Payment Card Industry (PCI) Security Standards Council

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	Implement Strong Access Control Measures
Protect Cardholder Data	Regularly Monitor and Test Networks
Maintain a Vulnerability Management Program	Maintain an Information Security Policy

https://www.pcisecuritystandards.org

Failure to meet the PCI DSS requirements may result in fines or termination of payment card processing privileges

ISO/IEC 27001:2013

- ISO/IEC 27001:2013 specifies the requirements for **establishing**, **implementing**, **maintaining** and continually improving an **information security management system** within the context of the organization
- It is intended to be suitable for several different types of use, including the following:

1. Use within organizations to formulate **security requirements** and **objectives**
2. Use within organizations as a way to ensure that security risks are **cost effectively managed**
3. Use within organizations to **ensure compliance with laws and regulations**
4. Definition of new **information security management processes**
5. Identification and clarification of existing **information security management processes**
6. Use by the management of organizations to determine the **status of information security management activities**
7. Implementation of **business-enabling information security**
8. Use by organizations to provide relevant information about **information security** to customers

https://www.iso.org

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Sets Standards	Requires every provider who does business electronically to **use the same health care transactions**, **code sets**, and **identifiers**
Privacy Rule	Provides **federal protections for personal health information** held by covered entities and gives patients an array of rights with respect to that information
Security Rule	Specifies a series of administrative, physical and technical safeguards for covered entities to use to assure the **confidentiality**, **integrity**, and **availability of electronic protected health information**
National Identifier Requirements	Requires that health care providers, health plans and employers have standard national numbers that identify them on **standard transactions**
Enforcement Rule	Provides standards for enforcing all the **Administration Simplification Rules**

https://www.hhs.gov

Sarbanes Oxley Act (SOX)

- Enacted in 2002, the Sarbanes-Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures
- Key requirements and provisions of SOX are organized into **11 titles**:

Title I	**Public Company Accounting Oversight Board (PCAOB)** establishes to provide independent oversight of public accounting firms providing audit services ("auditors")
Title II	**Auditor Independence** establishes standards for external auditor independence, to limit conflicts of interest and addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements
Title III	**Corporate Responsibility** mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports
Title IV	**Enhanced Financial Disclosures** describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and stock transactions of corporate officers
Title V	**Analyst Conflicts of Interest** consists of measures designed to help restore investor confidence in the reporting of securities analysts
Title VI	**Commission Resources and Authority** defines practices to restore investor confidence in securities analysts

Sarbanes Oxley Act (SOX) (Cont'd)

Title VII	**Studies and Reports** include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing and others to manipulate earnings and obfuscate true financial conditions
Title VIII	**Corporate and Criminal Fraud Accountability** describes specific criminal penalties for fraud by manipulation, destruction or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers
Title IX	**White Collar Crime Penalty Enhancement** increases the criminal penalties associated with white- collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense
Title X	**Corporate Tax Returns** states that the Chief Executive Officer should sign the company tax return
Title XI	**Corporate Fraud Accountability** identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments

https://www.sec.gov

The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)

The Digital Millennium Copyright Act (DMCA)

- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO)
- It **defines legal prohibitions** against circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information

https://www.copyright.gov

Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets
- It includes
  - Standards for categorizing information and information systems by mission impact
  - Standards for minimum security requirements for information and information systems
  - Guidance for selecting appropriate security controls for information systems
  - Guidance for assessing security controls in information systems and determining security control effectiveness
  - Guidance for the security authorization of information systems

https://csrc.nist.gov

Cyber Law in Different Countries

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of " fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://www.fas.org
	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	http://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.saic.gov.cn
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	http://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net

Module Summary

- Complexity of security requirements is increasing day by day as a result of evolving technology, changing hacking tactics, emerging security vulnerabilities, etc.
- Hacker or cracker is one who accesses a computer system by evading its security system
- Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to ensure system security
- Ethical hackers help organization to better understand their security systems and identify the risks, highlight the remedial actions, and also reduce ICT costs by resolving those vulnerabilities
- Ethical hacker should posses platform knowledge, network knowledge, computer expert, security knowledge, and technical knowledge skills
- Ethical hacking is a crucial component of risk assessment, auditing, counter fraud, best practices, and good governance