Module 01

Introduction to Ethical Hacking

Learning Objectives

01 Explain Information Security Concepts

02 Explain Hacking Concepts and Different Hacker Classes

03 Explain Ethical Hacking Concepts and Scope

04 Explain Hacking Methodologies and Frameworks

05 Summarize the Techniques used in Information Security Controls

06 Explain the Importance of Applicable Security Laws and Standards

Objective 01

Explain Information Security Concepts

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 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 or unauthorized changes
Availability	Assurance that the systems responsible for delivering, storing, and processing information are accessible when **required by the authorized users**
Authenticity	Refers to the characteristic of a communication, document, or any data that ensures the **quality of being genuine**
Non-Repudiation	A **guarantee** that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Information Security Attacks: Motives, Goals, and Objectives

Attacks = Motive (Goal) + Method (TTP) + Vulnerability

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

Motives behind information security attacks

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

Tactics, Techniques, and Procedures (TTPs)

- Attackers attempt various attack techniques to **exploit vulnerabilities** in a computer system or security policy and controls to achieve their motives
- The term Tactics, Techniques, and Procedures (TTPs) refers to the **patterns of activities and methods** associated with specific threat actors or groups of threat actors

Tactics

- "Tactics" is defined as the **strategy** adopted by an attacker to perform the attack from the beginning to the end

Techniques

- "Techniques" is defined as **technical methods used by an attacker** to achieve intermediate results during the attack

Procedures

- "Procedure" is defined as a **systematic approach** adopted by threat actors **to launch an attack**

Vulnerability

- Refers to the existence of **weakness** in an asset that can be exploited by threat agents

Common Reasons behind the Existence of Vulnerability

1. Hardware or software misconfiguration
2. Insecure or poor design of the network and application
3. Inherent technology weaknesses
4. Careless approach of end users

Classification of Attacks

Passive Attacks	• Passive attacks do not tamper with the data and involve intercepting and **monitoring network traffic** and data flow on the target network • Examples include sniffing and eavesdropping
Active Attacks	• Active attacks tamper with the data in transit or **disrupt the communication** or services between the systems to bypass or break into secured systems • Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection
Close-in Attacks	• Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or **disrupt access** to information • Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attacks	• Insider attacks involve using privileged access to **violate rules** or intentionally cause a threat to the organization's information or information systems • Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attacks	• Distribution attacks occur when attackers **tamper with hardware** or **software** prior to installation • Attackers tamper with the hardware or software at its source or in transit

Information Warfare

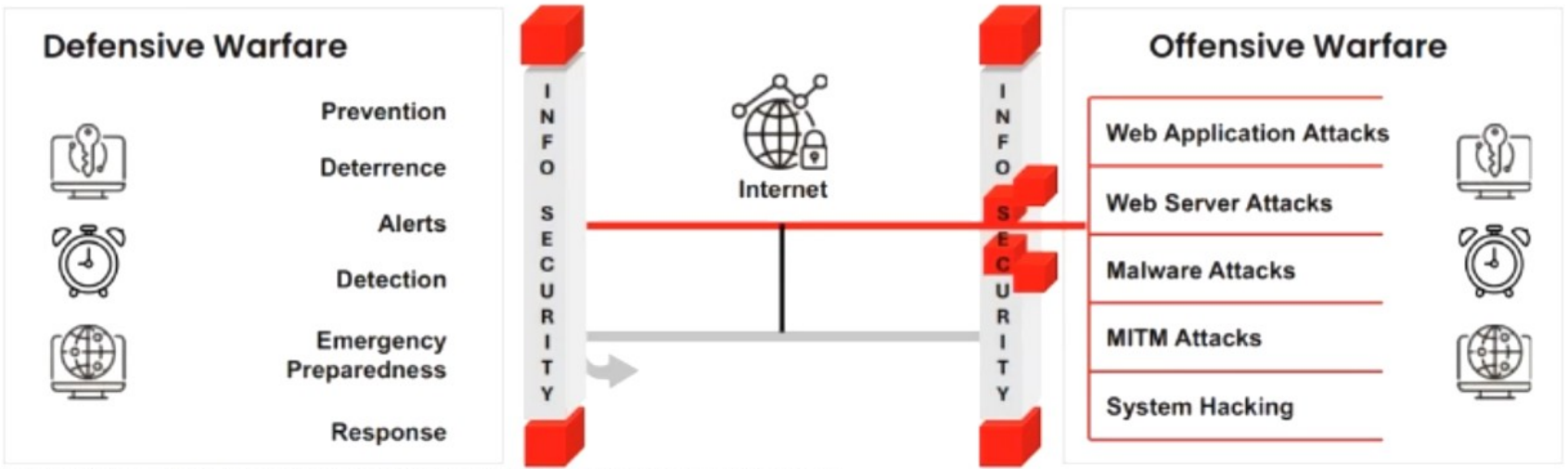
- The term information warfare or InfoWar refers to the **use of information and communication technologies (ICT)** to gain competitive advantages over an opponent

Defensive Information Warfare

Refers to all strategies and actions designed to **defend against attacks on ICT assets**

Offensive Information Warfare

Refers to information warfare that involves **attacks against the ICT assets** of an opponent



Objective 02

Explain Hacking Concepts and Different Hacker Classes

What is Hacking?

Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to a system's 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 and redistribute intellectual property, leading to **business loss**

Who is a Hacker?

01

An intelligent individual with **excellent computer skills** who can create and explore computer software and hardware

02

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

03

Some hackers' intentions can either be to gain knowledge or to **probe and do illegal things**

Some hack with **malicious intent** such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data

Hacker and their Motivations

Hacker Classes	Background	Motivations	Cyber Activity	Potential Targets
Script Kiddies	Inexperienced, often young individuals using pre-made scripts or tools without understanding them	Thrill, recognition, fun	Running simple attacks like DDoS, defacing websites	Small websites, online games, forums
White Hat Hackers	Professionals in cybersecurity	Improving security, salary, reputation	Conducting penetration tests, vulnerability assessments	Corporations, government agencies
Black Hat Hackers	Individuals with extraordinary computing skills	Financial gain, data theft, causing harm	Malware creation, phishing, ransomware, data breaches	Financial institutions, individuals, enterprises
Gray Hat Hackers	Skilled hackers operating between ethical and unethical lines	Recognition, curiosity, financial gain	Vulnerability discovery without permission, sometimes reported	Various, including high-profile organizations
Hacktivists	Politically or socially motivated individuals or groups	Promoting a cause, social justice	DDoS attacks, defacing websites, data leaks	Government sites, corporations, political groups
State-Sponsored Hackers	Highly trained professionals working for government agencies	National security, espionage, political objectives	Cyber espionage, infrastructure sabotage, data theft	Other nations' government agencies, corporations

Hacker and their Motivations (Cont'd)

Hacker Classes	Background	Motivations	Cyber Activity	Potential Targets
Cyber Terrorists	Extremists using cyber attacks to promote political or religious beliefs	Spreading fear, political or ideological goals	Cyber attacks on critical infrastructure, spreading propaganda	Critical infrastructure, public services
Corporate Spies (Industrial Spies)	Individuals hired by companies to gather intelligence on competitors	Financial gain, competitive advantage	Industrial espionage, data theft, spying	Competitor companies
Blue Hat Hackers	Security professionals hired temporarily to test systems before product release	Improving product security, reputation	Conducting security audits, penetration testing	Technology companies, software firms
Red Hat Hackers	Vigilantes targeting black hat hackers using aggressive methods	Cyber justice, disrupting malicious activities	Hacking black hat infrastructure, disabling malicious networks	Cybercriminal groups, black hat hackers
Green Hat Hackers	Newcomers eager to learn hacking skills, often participating in online forums and communities	Learning, curiosity, recognition	Learning hacking techniques, experimenting with simple attacks	Various, typically low-risk targets

Objective 03

Explain Ethical Hacking Concepts and Scope

What is Ethical Hacking?

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

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

Ethical hackers perform security assessments for an 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 for counter attacks against malicious hackers** through anticipating the methods used to break into the system

Reasons why organizations recruit ethical hackers

To **prevent hackers** from gaining access to the organization's information systems

To **uncover vulnerabilities** in systems and explore their potential as a security 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 data**

To **enhance security awareness** at all levels in a business

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 **remedial actions**. It also reduces ICT costs by resolving vulnerabilities

Limitations

- Unless the businesses already know what 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 can only help the organization to better **understand its security system**; it is up to the organization to **place the right safeguards** on the network

Skills of an Ethical Hacker

Technical Skills

- In-depth **knowledge of major operating environments** such as Windows, Unix, Linux, and Macintosh
- In-depth **knowledge of networking** concepts, technologies, and related hardware and software
- A **computer expert** adept at technical domains
- **Knowledgeable about security areas** and related issues
- "**High technical**" **knowledge** for launching sophisticated attacks

Non-Technical Skills

- The **ability to learn** and adopt new technologies quickly
- **Strong work ethics** and good problem solving and communication skills
- Committed to the **organization's security policies**
- An awareness of **local standards and laws**

AI-Driven Ethical Hacking

Advancements in AI have led to more sophisticated cyber threats, as **hackers increasingly use AI-driven tools** to enhance and automate their attacks, **presenting significant challenges to cybersecurity**

AI-driven ethical hacking is a **modern approach to cybersecurity** where artificial intelligence (AI) technologies are used to **enhance the capabilities of ethical hackers**

Leveraging AI in ethical hacking enables professionals to **anticipate emerging threats**, **outpace malicious actors**, and **proactively mitigate risks**

AI-driven ethical hacking involves use of AI technologies such as **AI algorithms**, **machine learning models**, and **automation frameworks** to facilitate and automate ethical hacking efforts

Benefits: **1. Efficiency** **2. Accuracy** **3. Scalability** **4. Cost-Effectiveness**

How AI-Driven Ethical Hacking Helps Ethical Hacker?

AI-driven ethical hacking **enhances the efficiency, effectiveness, and scope of cybersecurity measures**, providing ethical hackers with powerful tools to safeguard digital assets against increasingly sophisticated cyber threats

1. Automation of Repetitive Tasks
2. Predictive Analysis
3. Advanced Threat Detection
4. Enhanced Decision Making
5. Adaptive Learning
6. Enhanced Reporting
7. Simulation and Testing
8. Scalability
9. Continuous Monitoring
10. Adaptive Defense Mechanisms

Myth: AI will Replace Ethical Hackers

Ai-driven ethical hacking is one of the valuable tool in the arsenal of ethical hackers, and not a replacement

- While AI technologies can **automate certain aspects of ethical hacking tasks** and improve efficiency, human expertise, creativity, and critical thinking remain indispensable in cybersecurity
- Ethical hacking **involves a complex and dynamic interplay of technical skills**, domain knowledge, and ethical considerations **that go beyond the capabilities of AI systems alone**
- Ethical hackers **possess a deep understanding of systems and networks**, as well as the ability to think like attackers, identify vulnerabilities, and craft effective mitigation strategies
- Although AI-driven ethical hacking can **assist ethical hackers by automating routine tasks**. However, **Human oversight is essential to interpret results**, validate findings, and make informed judgments based on contextual knowledge and ethical principles

ChatGPT-Powered AI Tools for Ethical Hackers

ChatGPT-Powered AI Tools leverage the **capabilities of OpenAI's ChatGPT model** to **assist ethical hackers** in various aspects of their work

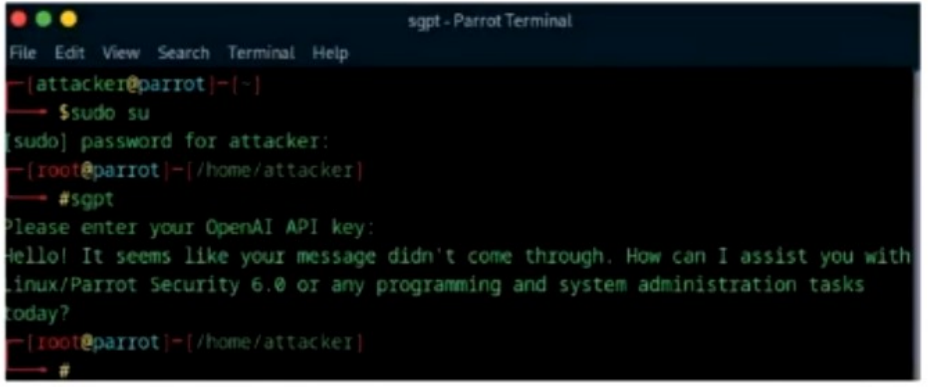
Features of ChatGPT-Powered AI Tools

Configure and collect data from a wide range of sources, including social media, forums, websites, and public databases

By using natural language processing (NLP) and machine learning, provide real-time assistance, automate tasks, and enhance the capabilities of security professionals

Integration with threat intelligence databases to provide context and additional information about identified threats

ShellGPT An AI-powered tool that ethical hackers and cybersecurity professionals can use to perform various tasks



ChatGPT-Powered AI Tools:	HackerGPT	PentestGPT	Bug Hunter GPT	h4ckGPT	Ethical Hacker GPT
	https://chat.hackerai.co	*https://github.com*	*https://chatgpt.com*	*https://chatgpt.com*	*https://chatgpt.com*

Objective 04

Explain Hacking Methodologies and Frameworks

CEH Ethical Hacking Framework

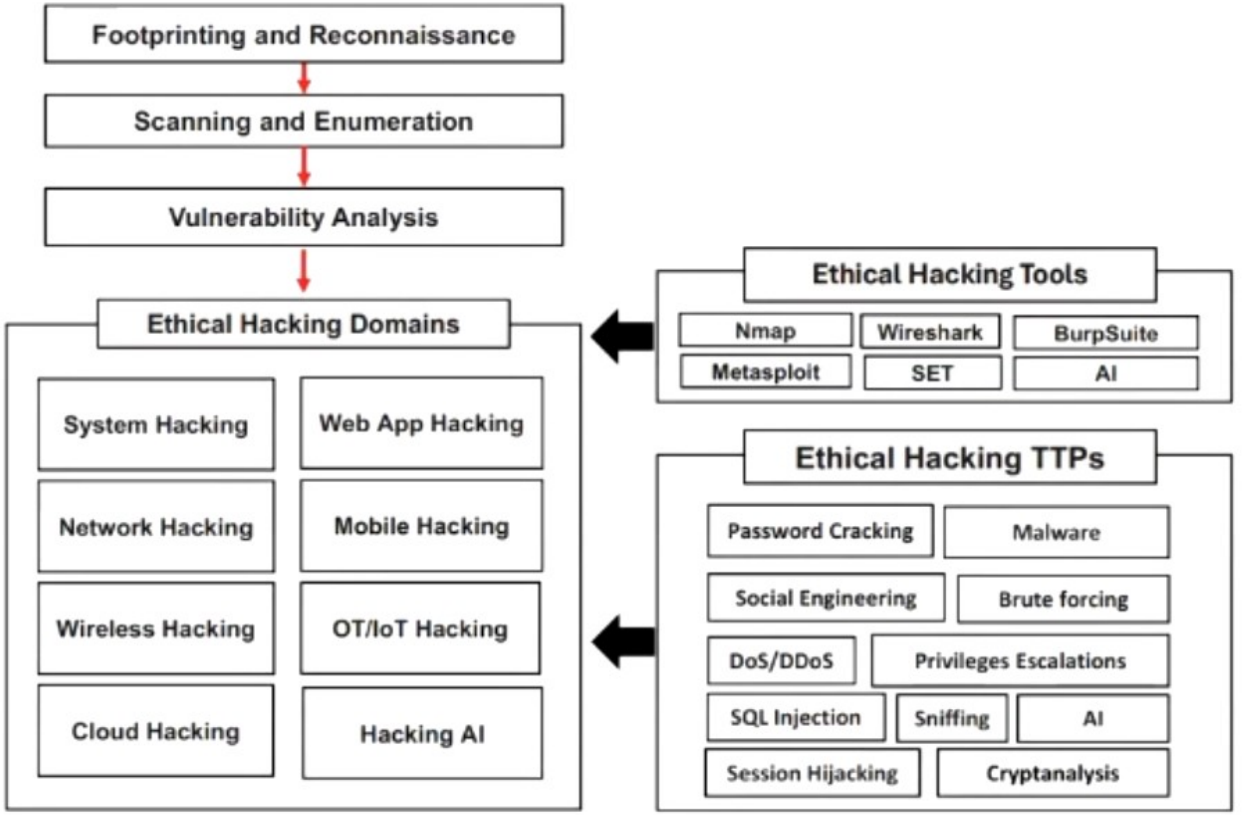
Phase 1: Reconnaissance

Phase 2: Vulnerability Scanning

Phase 3: Gaining Access

Phase 4: Maintaining Access

Phase 5: Clearing Tracks



Cyber Kill Chain Methodology

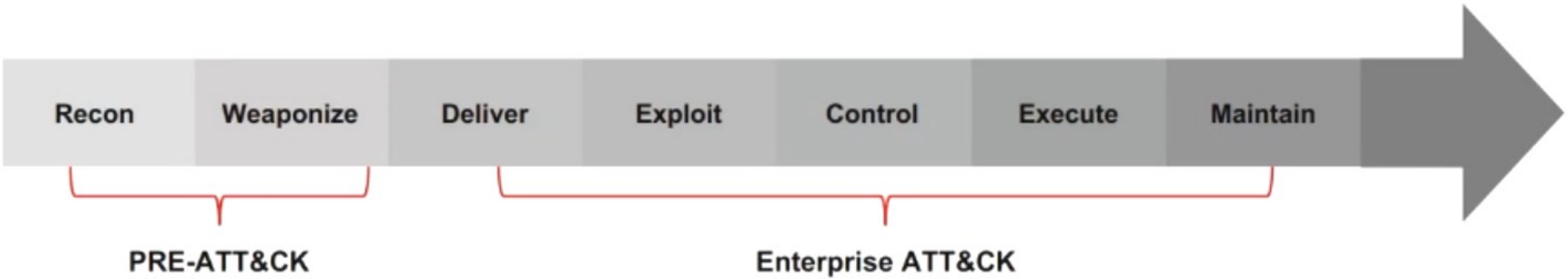
- The cyber kill chain methodology is a component of intelligence-driven defense for the identification and **prevention of malicious intrusion activities**
- It provides greater insight into attack phases, which helps security professionals to understand the **adversary's tactics, techniques, and procedures beforehand**

MITRE ATT&CK Framework

1. MITRE ATT&CK is a globally accessible knowledge base of **adversary tactics and techniques** based on real-world observations

2. The ATT&CK knowledge base is used as a foundation for the development of specific **threat models** and methodologies in the private sector, **government**, and the **cybersecurity product** and service community

3. The 14 tactic categories within ATT&CK for Enterprise are derived from the later stages (exploit, control, maintain, and execute) of the seven stages of the **Cyber Kill Chain**



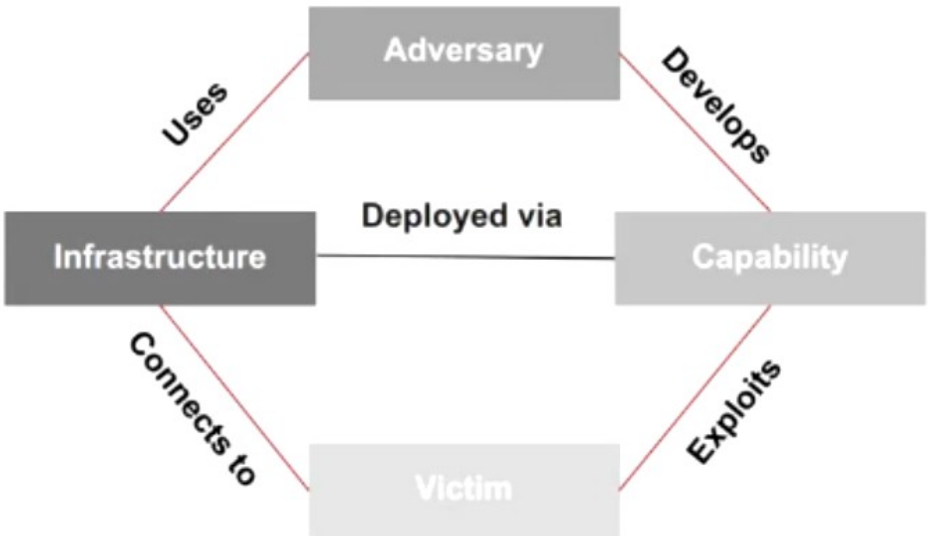
https://attack.mitre.org

Diamond Model of Intrusion Analysis

- The Diamond Model offers a framework for **identifying the clusters of events** that are correlated on any of the systems in an organization
- It can control the **vital atomic element** occurring in any intrusion activity, which is referred to as the Diamond event
- Using this model, **efficient mitigation approaches** can be developed, and analytic efficiency can be increased

Adversary	An opponent "**who**" was behind the attack
Victim	The target that has been exploited or "**where**" the attack was performed
Capability	The attack strategies or "**how**" the attack was performed
Infrastructure	"**what**" the adversary used to reach the victim

Meta Features of Diamond Model



Objective 05

Summarize the Techniques used in Information Security Controls

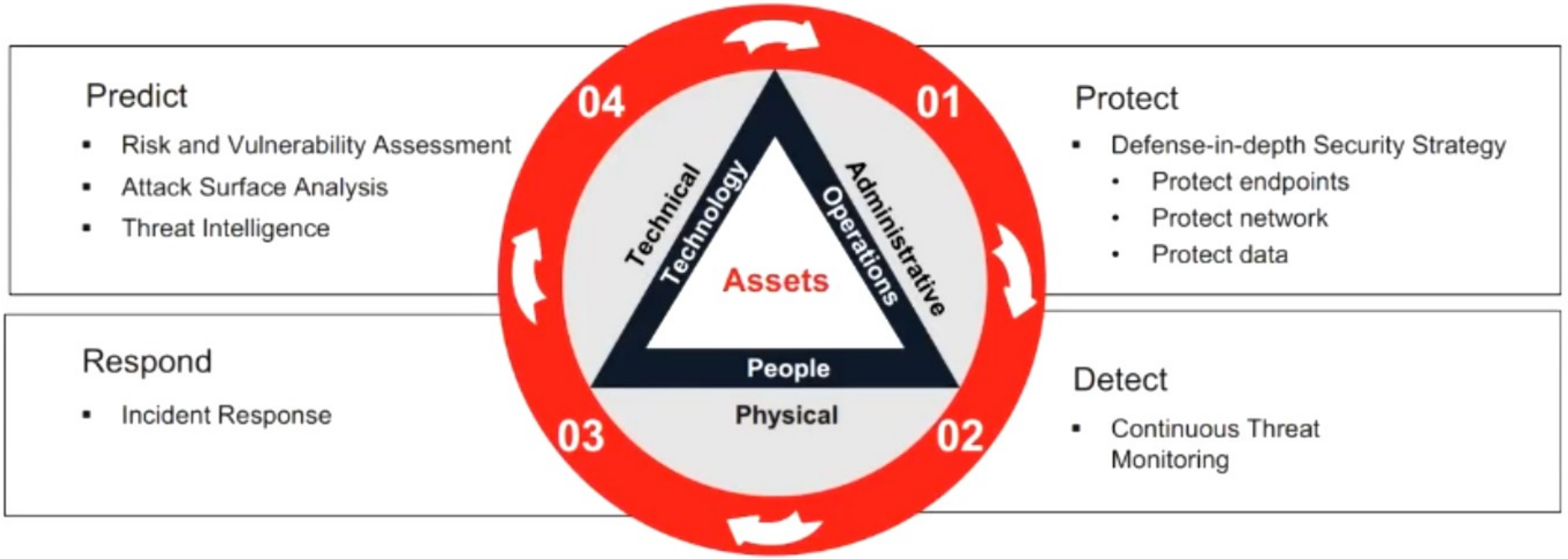
Information Assurance (IA)

- IA refers to the assurance that the **integrity**, **availability**, **confidentiality**, and **authenticity** of information and information systems is protected during the 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 strategies**
3. **Identifying network vulnerabilities and threats**
4. **Identifying problem and resource requirements**
5. **Creating plans for identified resource requirements**
6. **Applying appropriate information assurance controls**
7. **Performing certification and accreditation**
8. **Providing information assurance training**

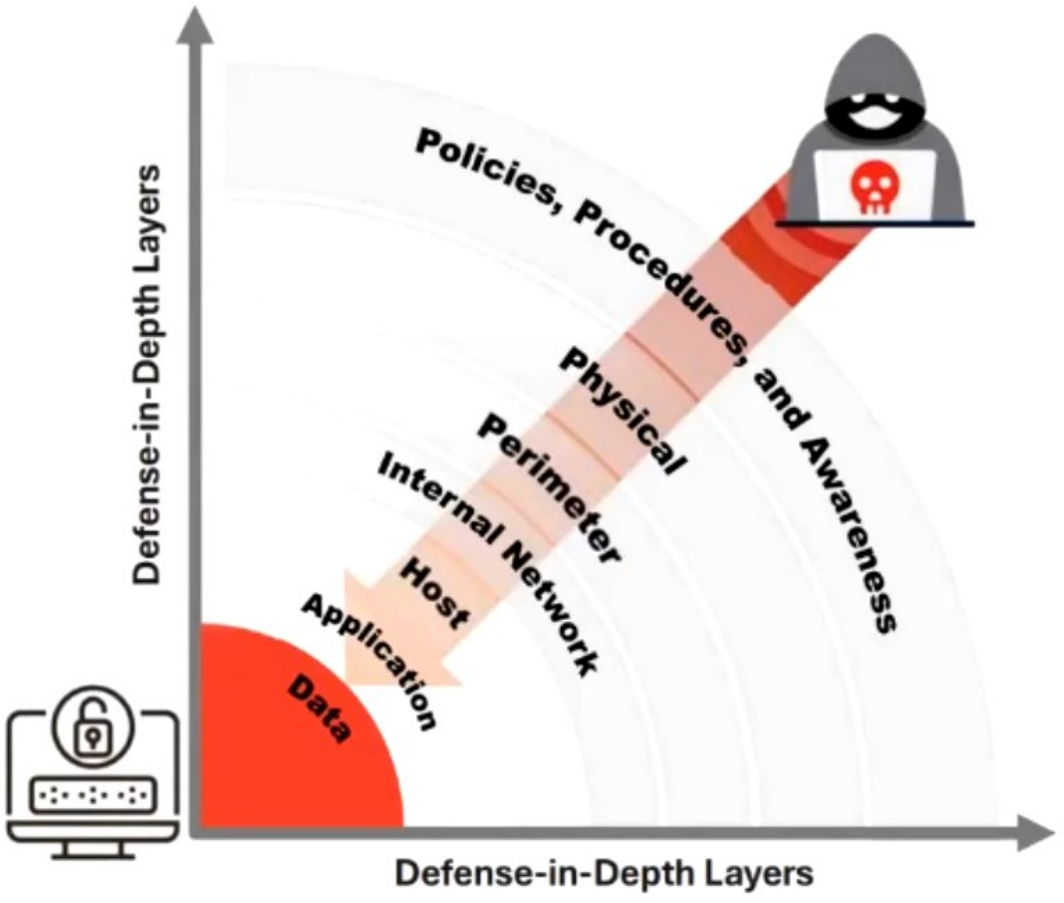
Continual/Adaptive Security Strategy

- Organizations should adopt **adaptive security strategy**, which involves implementing all the four network security approaches
- The adaptive security strategy consists of four security activities corresponding to each security approach



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 the system and its data because a break in one layer only leads the attacker to the next layer



What is Risk?

- Risk refers to the 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 or impact** of the risk

Risk Levels

Risk Level	Action
Extreme or High	• Immediate measures should be taken to combat risk • Identify and impose controls to reduce risk to a reasonably low level
Medium	• No urgent action is required • 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					
	Likelihood		Insignificant	Minor	Moderate	Major	Severe
81 - 100%		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

Note: This is an example of a risk matrix. Organizations need to create their own risk matrix based on their business needs

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

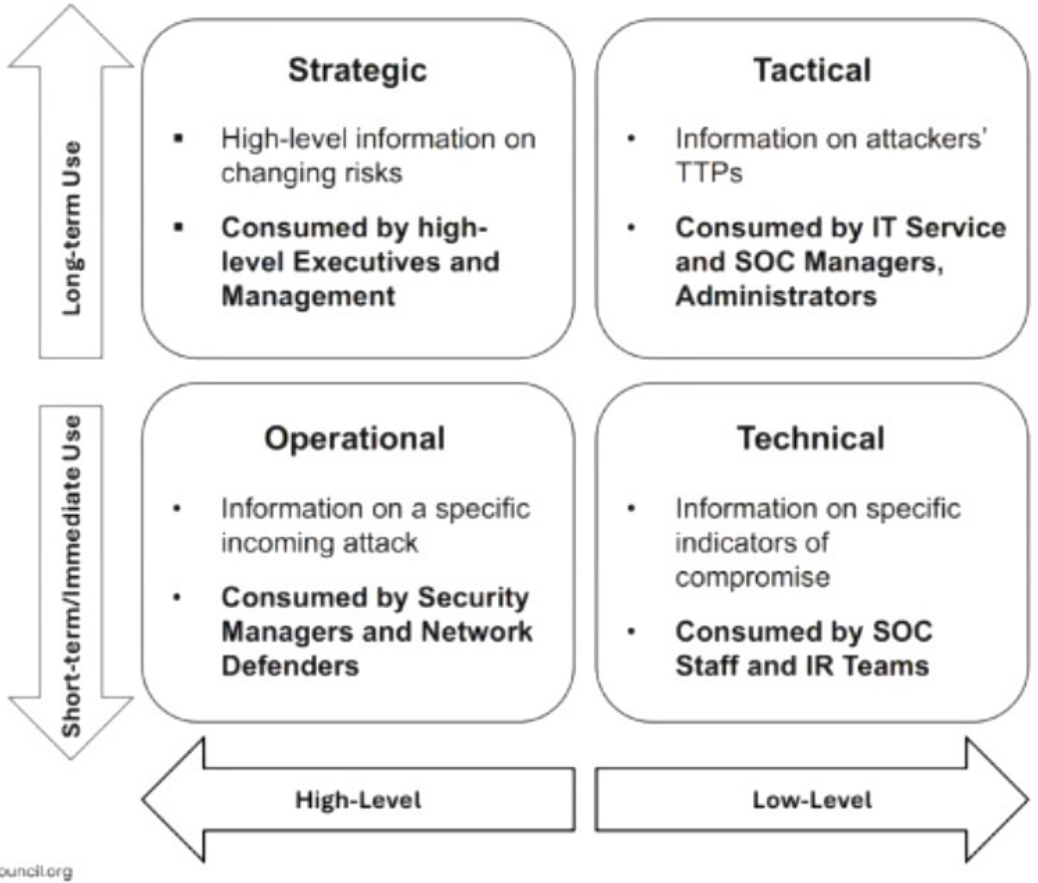
Risk Identification	**Identifies the sources**, causes, consequences, and other details of the internal and external risks affecting the security of the organization
Risk Assessment	**Assesses the organization's risk** and provides an estimate of the likelihood and impact of the risk
Risk Treatment	**Selects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

Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) is defined as the **collection and analysis of information** about threats and adversaries and the drawing of patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyber-attacks

Cyber threat intelligence helps the organization to **identify and mitigate various business risks** by converting unknown threats into known threats; it helps in implementing various advanced and proactive defense strategies

Types of Threat Intelligence



Threat Intelligence Lifecycle

1. Planning and Direction

- Define intelligence requirements
- Make a collection plan
- Form an intelligence team
- Send requests for data collection
- Plan and set requirements for other phases

2. Collection

- Collect required data that satisfies intelligence goals
- Collection sources include
  - OSINT
  - HUMINT
  - IMINT
  - MASINT, etc.

3. Processing and Exploitation

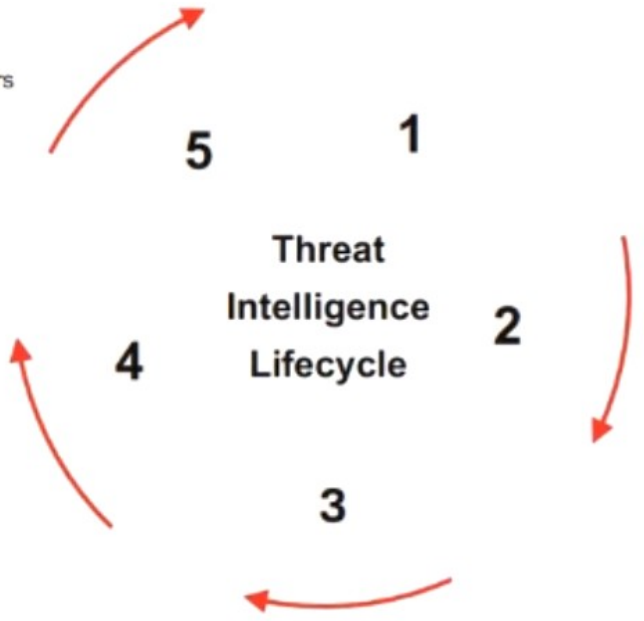
- Process raw data for exploitation
- Convert processed data into usable format for data analysis

4. Analysis and Production

- Combine information from phase 3 into a single entity
- Include facts, findings, and forecasts
- Analysis should be
  - Objective
  - Timely
  - Accurate
  - Actionable
- Perform confidence-based analysis

5. Dissemination and Integration

- Deliver the intelligence to the intended consumers at different levels
  - Strategic (High-Level Business Strategies)
  - Tactical (TTPs)
  - Operational (Specific Threats)
  - Technical (IoCs)



Threat Modeling

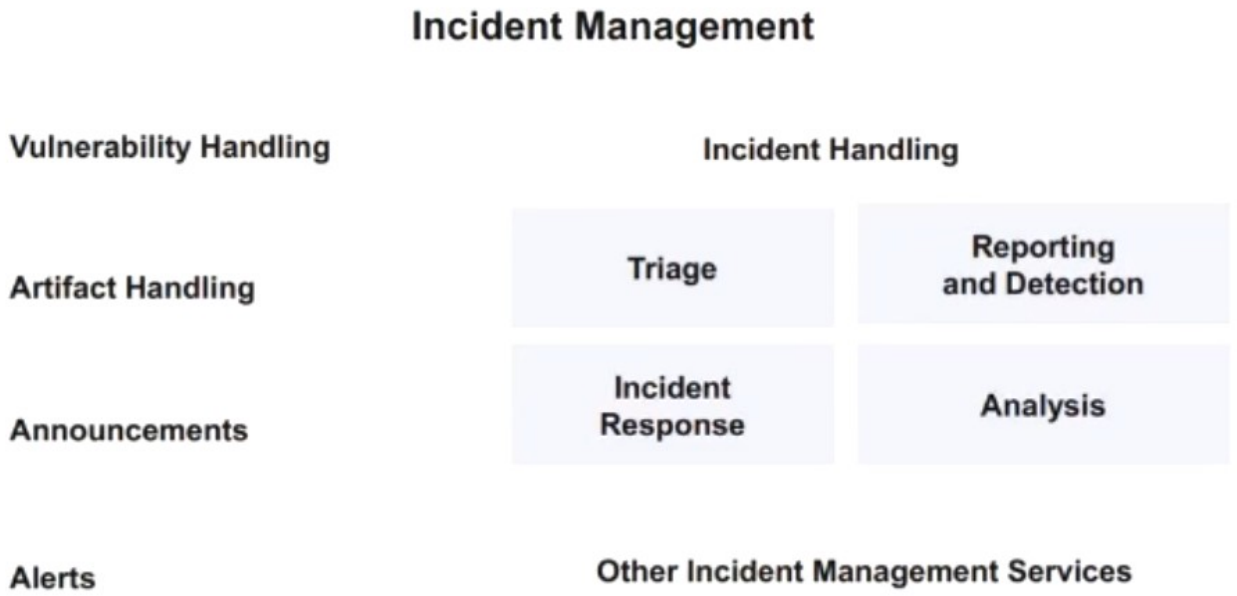
Threat modeling is a **risk assessment approach** for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects the security of an application

Threat Modeling Process

1 **Identify Security Objectives**	Helps to determine how much **effort needs to be put** toward subsequent steps
2 **Application Overview**	Identify the **components**, **data flows**, and trust boundaries
3 **Decompose the Application**	Helps to find more relevant and more **detailed threats**
4 **Identify Threats**	Identify threats relevant to the **control** scenario and context using the information obtained in steps 2 and 3
5 **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 Handling and Response

Incident handling and response (IH&R) is the **process of taking organized and careful steps** when reacting to a security incident or cyberattack

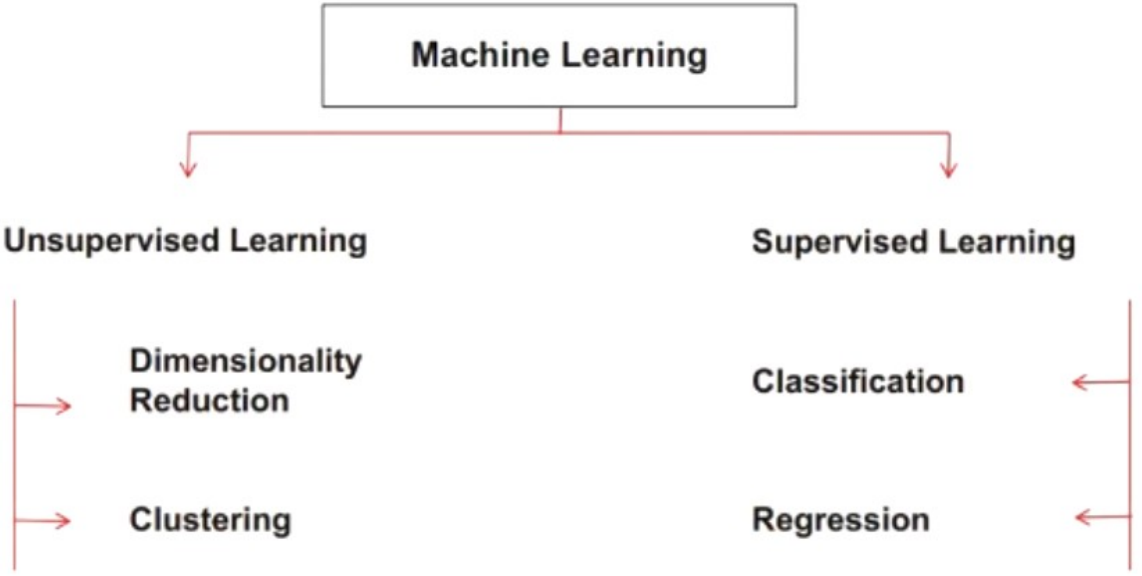
Steps involved in the IH&R process:

1. **Preparation**
2. **Incident Recording and Assignment**
3. **Incident Triage**
4. **Notification**
5. **Containment**
6. **Evidence Gathering and Forensic Analysis**
7. **Eradication**
8. **Recovery**
9. **Post-Incident Activities**
   - Incident Documentation
   - Incident Impact Assessment
   - Review and Revise Policies
   - Close the Investigation
   - Incident Disclosure

Role of AI and 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 computing power**, **data collection**, and **storage capabilities**
- ML is an **unsupervised self-learning system** that is used to define what the normal network looks like, along with its devices, and then to backtrack and **report any deviations or anomalies** in real-time
- AI and ML in cyber security helps in **identifying new exploits and weaknesses**, which can then be easily analyzed to mitigate further attacks

- ML classification techniques:
  - Supervised learning makes use of algorithms that input a **set of labeled training data**, with the 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



How Do AI and ML Prevent Cyber Attacks?

1. Password Protection and Authentication
2. Phishing Detection and Prevention
3. Threat Detection
4. Vulnerability Management
5. Behavioral Analytics
6. Network Security
7. AI-based Antivirus
8. Fraud Detection
9. Botnet Detection
10. AI to Combat AI Threats

Objective 06

Explain the Importance of Applicable 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 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

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 the termination of payment card processing privileges

ISO/IEC Standards

Standard	Description
ISO/IEC 27001:2022	Specifies the requirements and a framework for **establishing**, **implementing**, **maintaining**, and continually improving an **Information Security Management System (ISMS)**
ISO/IEC 27701:2019	Extends ISO/IEC 27001 to include **privacy management**, focusing on protecting PII and implementing a **Privacy Information Management System (PIMS)**
ISO/IEC 27002:2022	Outlines **best practices** and control objectives **for critical cybersecurity areas**, including access control, cryptography, and security personnel
ISO/IEC 27005:2022	Provides guidelines for **information security risk management** to support the requirements of an ISMS as specified in ISO/IEC 27001
ISO/IEC 27018:2019	Offers code of practice specifically focused on the **protection of personally identifiable information (PII) in public clouds**
ISO/IEC 27032:2023	Explains the relationship between internet, web, network security, and cybersecurity, providing an overview of **internet security**, and identifying key stakeholders and their roles
ISO/IEC 27033-7:2023	Proposes guidelines for the implementation of **network virtualization security**
ISO/IEC 27036-3:2023	Provides guidelines for securing hardware, software, and services **supply chains**
ISO/IEC 27040:2024	Provides technical requirements and guidance for achieving **data storage security** through planning, design, documentation, and implementation

https://www.iso.org

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Set 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 the 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 ensure the **confidentiality**, **integrity**, and **availability of electronically protected health information**
National Identifier Requirements	Requires that health care providers, health plans, and employers have standard national numbers that identify them attached to **standard transactions**
Enforcement Rule	Provides the 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
- The key requirements and provisions of SOX are organized into **11 titles**:

Title I	Public Company Accounting Oversight Board (PCAOB)	Title VI	Commission Resources and Authority
Title II	Auditor Independence	Title VII	Studies and Reports
Title III	Corporate Responsibility	Title VIII	Corporate and Criminal Fraud Accountability
Title IV	Enhanced Financial Disclosures	Title IX	White Collar Crime Penalty Enhancement
Title V	Analyst Conflicts of Interest	Title X	Corporate Tax Returns
Title XI	Corporate Fraud Accountability		

https://www.sec.gov

The Digital Millennium Copyright Act (DMCA) and the 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 the legal prohibitions** against the 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 security authorization of information systems

https://csrc.nist.gov

General Data Protection Regulation (GDPR)

- GDPR regulation was put into effect on May 25, 2018 and one of the **most stringent privacy and security laws globally**
- The GDPR will **levy harsh fines** against those who violate its privacy and security standards, with penalties reaching tens of millions of euros

GDPR Data Protection Principles

- **Lawfulness, fairness, and transparency**: Processing must be lawful, fair, and transparent to the data subject
- **Purpose limitation**: You must process data for the legitimate purposes specified explicitly to the data subject when you collected it
- **Data minimization**: You should collect and process only as much data as necessary for the purposes specified
- **Accuracy**: You must keep personal data accurate and up to date
- **Storage limitation**: You may only store personally identifying data for as long as necessary for the specified purpose
- **Integrity and confidentiality**: Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g., by using encryption)
- **Accountability**: The data controller is responsible for demonstrating GDPR compliance with all these principles

https://gdpr.eu

Data Protection Act 2018 (DPA)

- The **DPA 2018** sets out the framework for data protection law in the **UK**
- It **updates** and **replaces** the Data Protection Act 1998 and came into effect on 25 May, 2018
- The DPA is an act to make provision for the regulation of the processing of information relating to **individuals**; to make provision in connection with the **Information Commissioner's functions** under specific regulations relating to information; to make provision for a direct **marketing code** of practice, and connected purposes

- The DPA **protects individuals** concerning the processing of personal data, in particular by:
  - Requiring **personal data to be processed lawfully** and fairly, based on the data subject's consent or another specified basis,
  - **Conferring rights** on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and
  - **Conferring functions** on the Commissioner, giving the holder of that office responsibility to monitor and enforce their provisions

https://www.legislation.gov.uk

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.bitlaw.com
	The Electronic Communications Privacy Act	https://bja.ojp.gov
	Foreign Intelligence Surveillance Act	https://bja.ojp.gov
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.congress.gov
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://www.energy.gov
	Identity Theft and Assumption Deterrence Act	https://www.ftc.gov
	California Consumer Privacy Act (CCPA)	https://oag.ca.gov
	California Privacy Rights Act	https://thecpra.org

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	https://www.cybercrimelaw.net
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994	
	Computer Misuse Act 1990	
	The Network and Information Systems Regulations 2018	
	Communications Act 2003	
	The Privacy and Electronic Communications (EC Directive) Regulations 2003	
	Investigatory Powers Act 2016	
	Regulation of Investigatory Powers Act 2000	
China	Copyright Law of the 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)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	https://www.ipindia.gov.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1959)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademarks Act (R.S.C., 1985, c. T-13), Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
	Personal Information Protection and Electronic Documents Act (PIPEDA)	https://www.priv.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.wipo.int
South Korea	Copyright Act (amended up to Act No. 19597 of August 8, 2023)	https://www.wipo.int
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Brazilian General Data Protection Law (LGPD)	https://iapp.org
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk
Philippines	Republic Act No. 10175	https://lawphil.net

Module Summary

- This module discussed elements of information security, information security attacks, and information warfare
- It also discussed hacking concepts and hacker classes
- This module also covered ethical hacking concepts such as the scope and limitations of ethical hacking, skills, and along with AI-driven ethical hacking in detail
- It discussed various hacking methodologies and frameworks including CEH ethical hacking framework, cyber kill chain methodology, MITRE ATT&CK framework, and diamond model for intrusion analysis
- It discussed information security controls such as defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI and ML
- This module ended with a detailed discussion of various information security acts and laws from around the world
- The next module will go into detail about how attackers, as well as ethical hackers and pen testers, perform footprinting to collect information about the target of an evaluation before an attack or audit