Introduction to Ethical Hacking

Module 01

Unmask the Invisible Hacker.




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 Management and Defense-in-Depth
- Overview of Policies, Procedures, and Awareness
- Overview of Physical Security and Controls
- Understanding Incident Management Process
- Overview of Vulnerability Assessment and Penetration Testing
- Overview of Information Security Acts and Laws

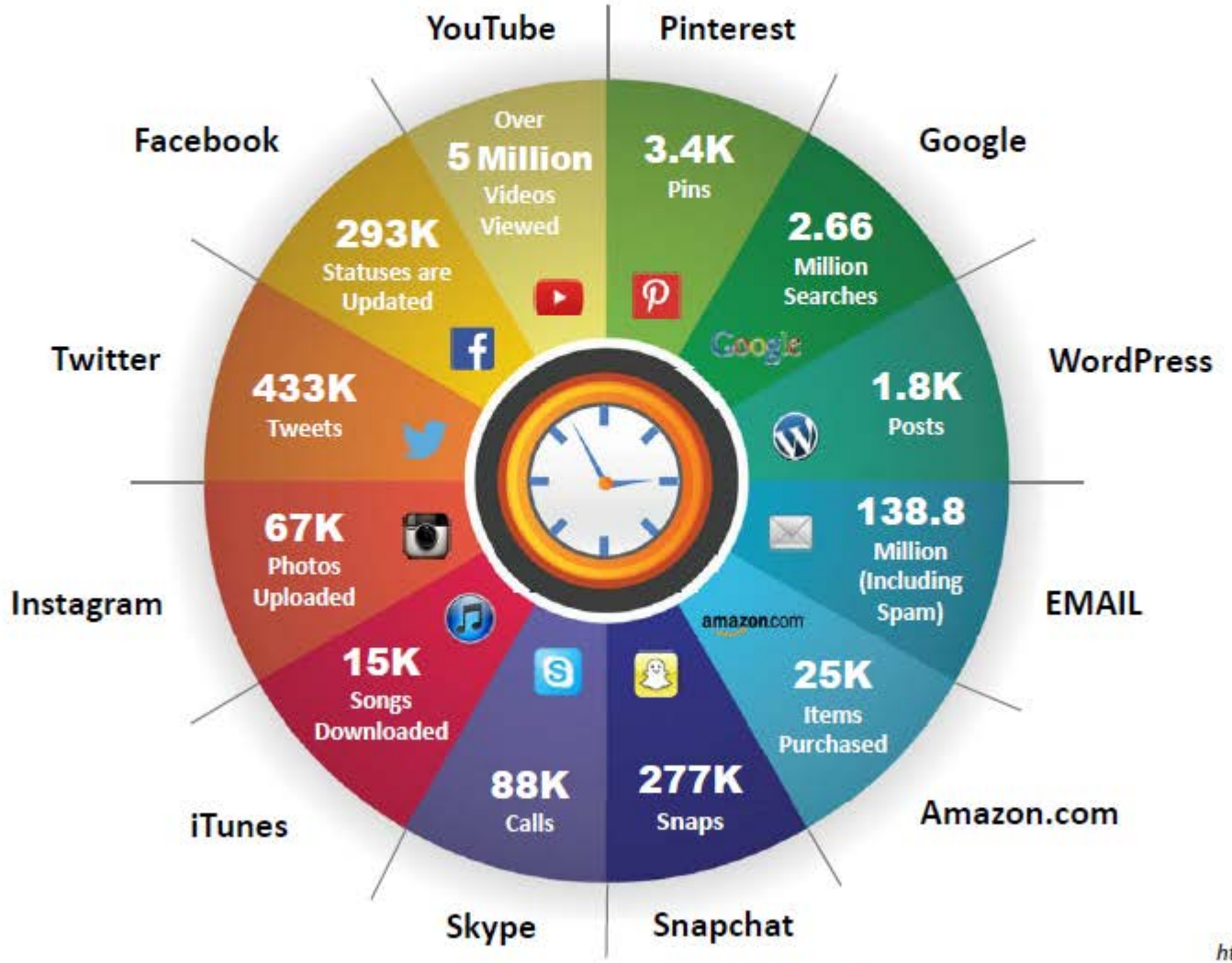


Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts, Types, and Phases
4. Ethical Hacking Concepts and Scope
5. Information Security Controls
6. Information Security Laws and Standards

Internet is Integral Part of Business and Personal Life

- What Happens Online in 60 Seconds



Case Study: eBay Data Breach

Records of **145 million** user were compromised

Records contained **passwords**, **email addresses**, **birth dates**, **mailing addresses** and other personal information

http://uk.reuters.com

Case Study: Google Play Hack

Google play

A **Turkish hacker has brought down Google Play's entire system** twice, preventing any downloads or uploads to it

The hacker uploaded a **malformed APK to Android app database** to test a vulnerability in the application. This caused **Denial of Service on Google Play**!

http://wallstcheatsheet.com

Case Study: The Home Depot Data Breach

C|EH Certified Ethical Hacker

56 million debit and credit card numbers were stolen

Incident occurred due to **custom-built malware**

http://krebsonsecurity.com

Case Study: JPMorgan Chase Data Breach

C|EH Certified Ethical Hacker

Contact information for **76 million households** and **7 million small businesses** were compromised

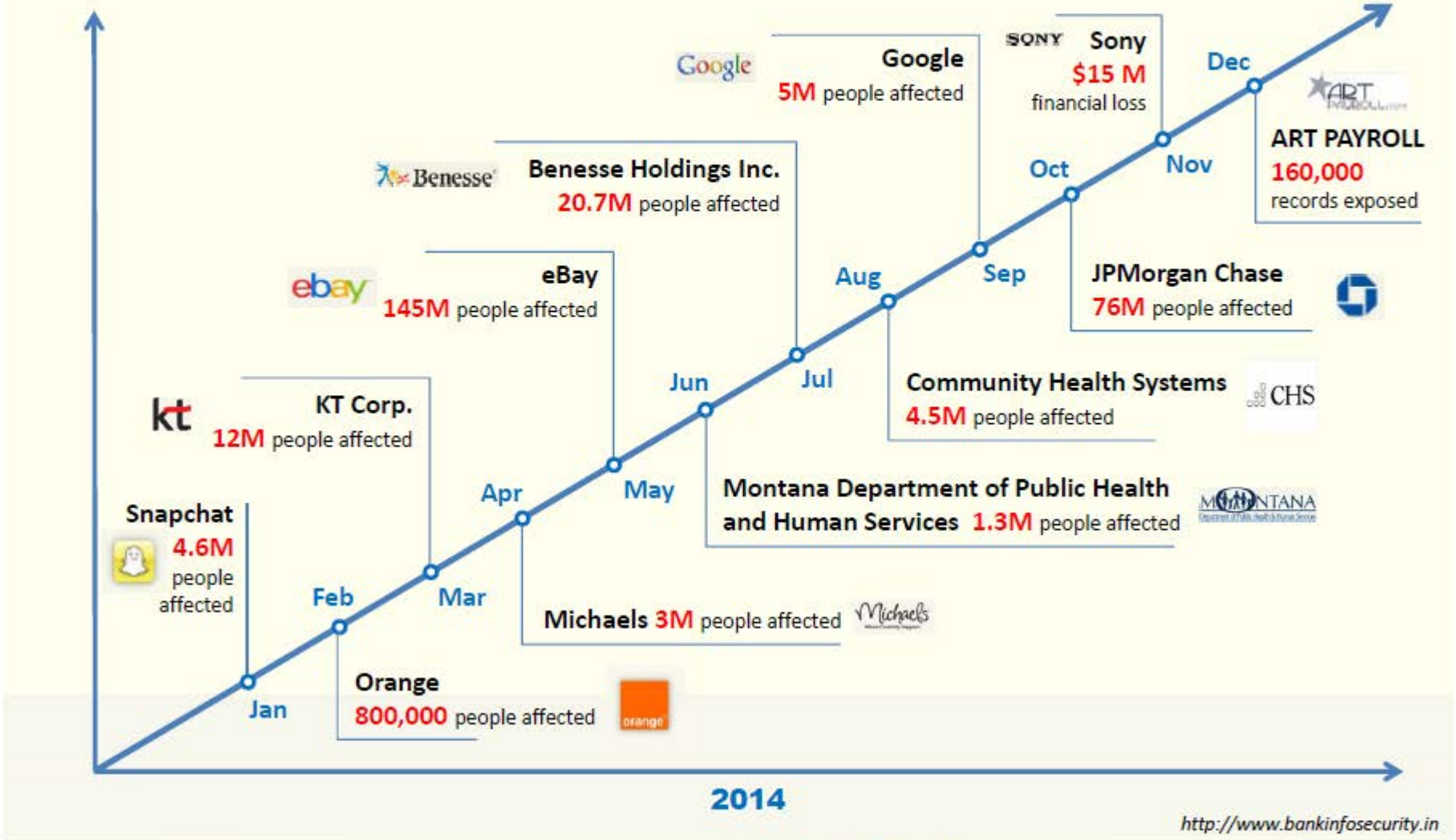
Incident occurred due to **attack on web applications**

JPMorganChase

http://dealbook.nytimes.com

Year of the Mega Breach

C|EH Certified Ethical Hacker



http://www.bankinfosecurity.in

Data Breach Statistics

C|EH Certified Ethical Hacker

There were over **3,007,682,404** data records lost or stolen since 2013 till Mar-2015

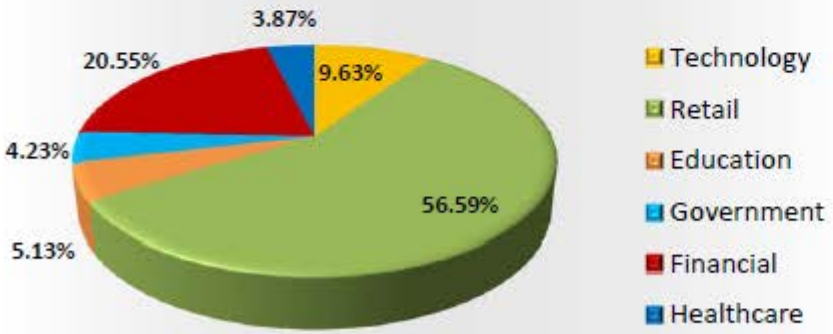
3,221,670 records lost **every day** in Jan-15

134,236 records **every hour**

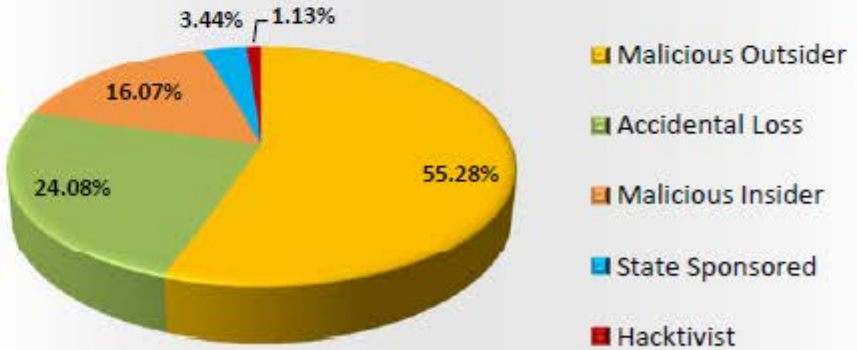
2,237 records **every minute**

37 records **every second**

Data Records Lost/Stolen by Industry



Breach by Source



Source: http://breachlevelindex.com (Jan 2014 – Dec 2014)

Malware Trends in 2014

C|EH Certified Ethical Hacker

Source code leaks accelerated malware release cycles

Old school malware techniques made a comeback

Growth of 64-bit malware increased

Malware researcher evasion became more popular

Mobile SMS-forwarding malware are becoming ubiquitous

Account takeover moved to the victim's device

Attacks on corporate and personal data in the cloud increased

Exploit kits continued to be a primary threat for Windows

https://www.trusteer.com; http://www.sophos.com

Malware Trends in 2014 (Cont'd)

C|EH Certified Ethical Hacker

Attackers increasingly **lure executives** and compromise organizations via professional social networks

Redkit, Neutrino, and other exploit kits struggled for power in the wake of the **Blackhole** Author Arrest

Java remains highly exploitable and highly exploited – with expanded repercussions

Mistakes are made in "**offensive**" security due to misattribution of an attack's source

Attackers are more **interested in cloud data** than your network

Cybercriminals are **targeting the weakest links in the "data-exchange chain"**

The **sheer volume of advanced malware** is decreasing

Major **data-destruction attacks** are increasing

http://community.websense.com

Essential Terminology

C|EH Certified Ethical Hacker

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

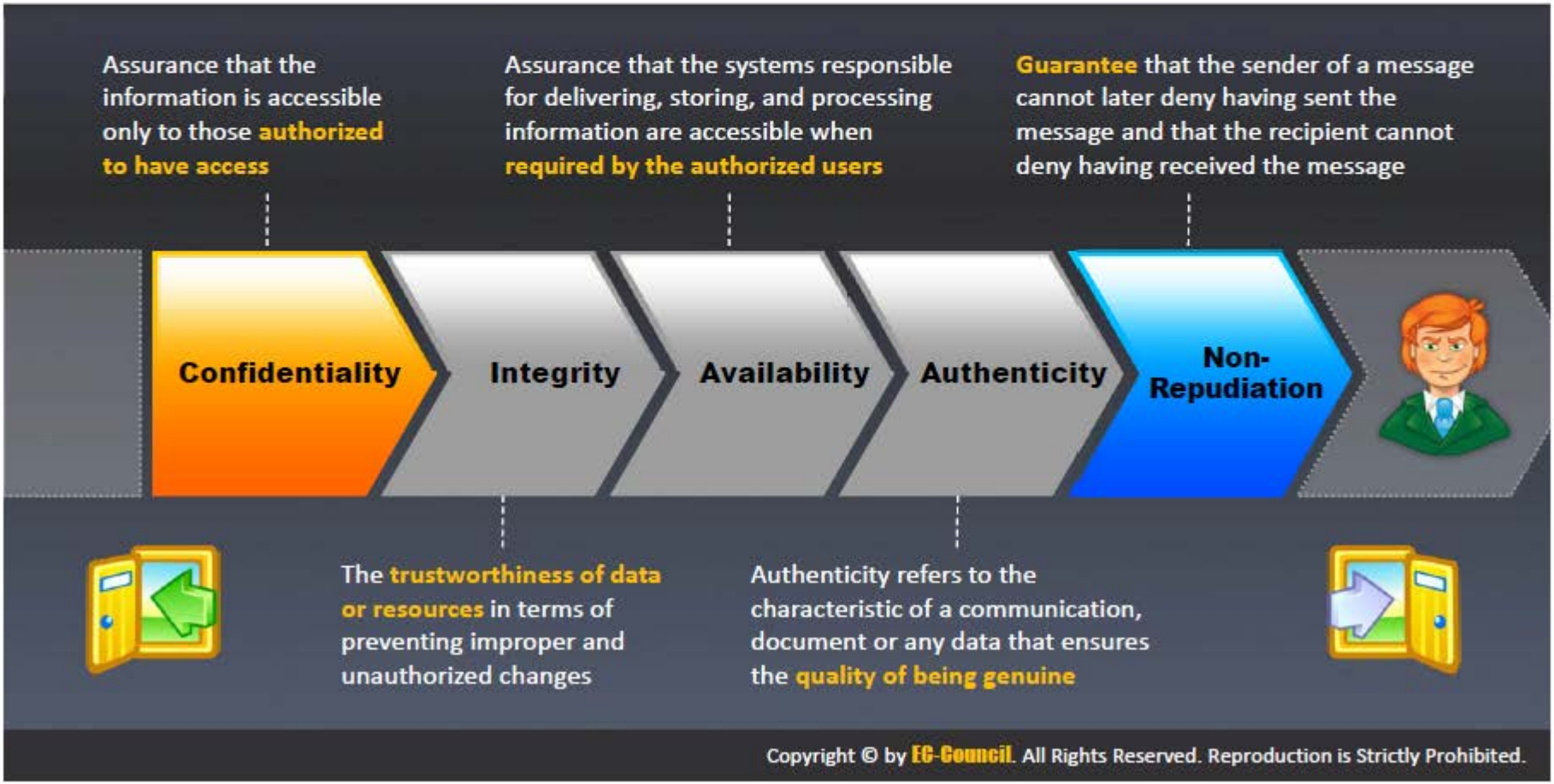
Bot

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

Elements of Information Security

C|EH Certified Ethical Hacker

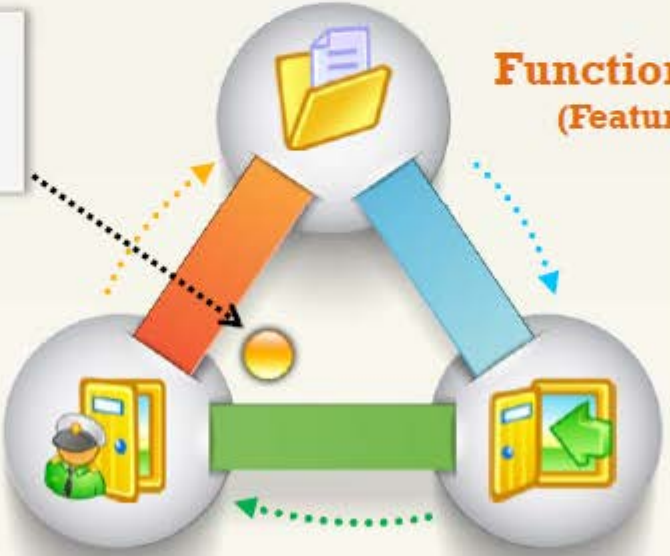
Information security is a state of well-being of information and infrastructure in which the possibility of **theft**, **tampering**, and **disruption of information and services** is kept low or tolerable



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, Types, and Phases
4. Ethical Hacking Concepts and Scope
5. Information Security Controls
6. Information Security Laws and Standards

Motives, Goals, and Objectives of Information Security Attacks

C|EH Certified Ethical Hacker

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
- Manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Propagating religious or political beliefs
- Achieving state's military objectives
- Damaging reputation of the target
- Taking revenge

Top Information Security Attack Vectors

C|EH Certified Ethical Hacker

Cloud Computing Threats

- Cloud computing is an **on-demand delivery of IT capabilities** where sensitive data of organization's and clients is stored
- Flaw in one client's application cloud allow attackers to access other client's data

Advanced Persistent Threats

APT is an attack that focus 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**

Mobile Threats

Focus of attackers has shifted to **mobile devices** due to the increased adoption of mobile devices for business and personal purposes and comparatively **lesser security controls**

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

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
- 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
- Broken session management
- Buffer overflow issues
- Cryptography attacks
- SQL injection
- 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.

Mis-configuration 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

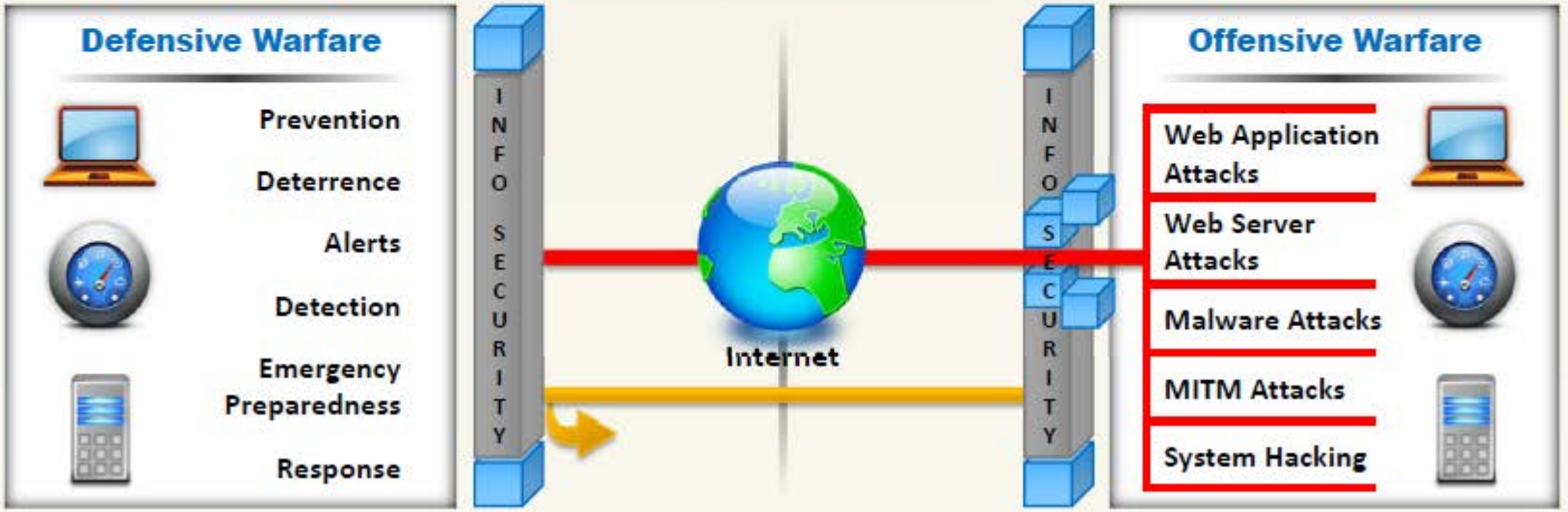
The term information warfare or InfoWar refers to the **use of information and communication technologies (ICT)** to take competitive advantages over an opponent

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, Types, and Phases
4. Ethical Hacking Concepts and Scope
5. Information Security Controls
6. 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?

C|EH Certified Ethical 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

CEH Certified Ethical Hacker

1 Black Hats

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

2 White Hats

Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts

3 Gray Hats

Individuals who work both offensively and defensively at various times

4 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

5 Script Kiddies

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

6 Cyber Terrorists

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

7 State Sponsored Hackers

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

8 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

Scanning can include use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, etc.

Port Scanner

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

C|EH Certified Ethical Hacker

- Reconn-aissance
- Scanning
- **Gaining Access**
- Mainta-ining Access
- Clearing Tracks

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

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

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

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

Hacking Phases: Maintaining Access

01 Maintaining access refers to the phase when the attacker tries to retain his or her **ownership of the system**

02 Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **Backdoors**, **RootKits**, or **Trojans**

03 Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**

04 Attackers use the compromised system to **launch further attacks**

Hacking Phases: Clearing Tracks

01

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

02

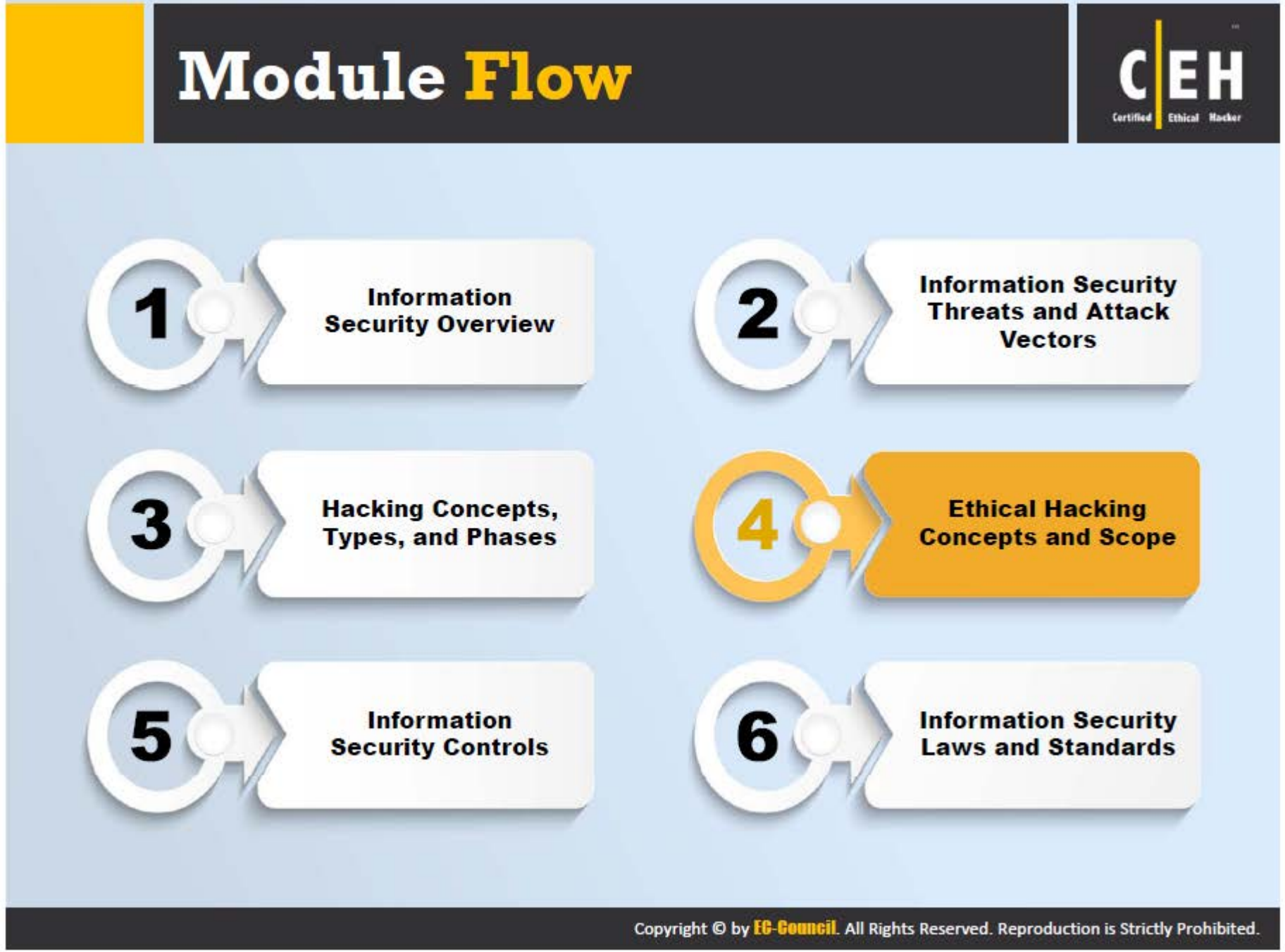
The attacker's intentions include: **Continuing access** to the victim's system, remaining **unnoticed and uncaught**, deleting evidence that might lead to his prosecution

03

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

Attackers always cover tracks to hide their identity

Module Flow



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

C|EH Certified Ethical Hacker

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

Ethical hacking is necessary as it **allows to 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

Why Ethical Hacking is Necessary (Cont'd)

C|EH Certified Ethical Hacker

Ethical Hackers Try to Answer the Following Questions

What can the intruder see on the **target system**? (Reconnaissance and Scanning phases)

What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)

Does anyone at the target **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)

If all the **components of information system** are adequately protected, updated, and patched

How much effort, time, and money is required to obtain **adequate protection**?

Are the **information security measures** in compliance to industry and legal standards?

Skills of an Ethical Hacker

C|EH Certified 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, Types, and Phases
4. Ethical Hacking Concepts and Scope
5. Information Security Controls
6. 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**

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

1 Identify Security Objectives

Helps to determine how much **effort need to put** on subsequent steps

2 Application Overview

Identify the **components**, **data flows**, and trust boundaries

3 Decompose Application

Helps you to find more relevant and more **detailed threats**

4 Identify Threats

Identify threats relevant to your **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**

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 breeches**
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 buffer** 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 polices**

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

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

Types of Security Policies

C|EH Certified Ethical Hacker




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

Examples of Security Policies

C|EH Certified Ethical Hacker

Access Control Policy

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

Remote-Access Policy

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

Firewall-Management Policy

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

Network-Connection Policy

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

Passwords Policy

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

User-Account Policy

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

Information-Protection Policy

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

Special-Access Policy

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

Email Security Policy

It is created to govern the proper usage of corporate email

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

C|EH Certified Ethical Hacker

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 of the 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 work 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 law suits 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

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:

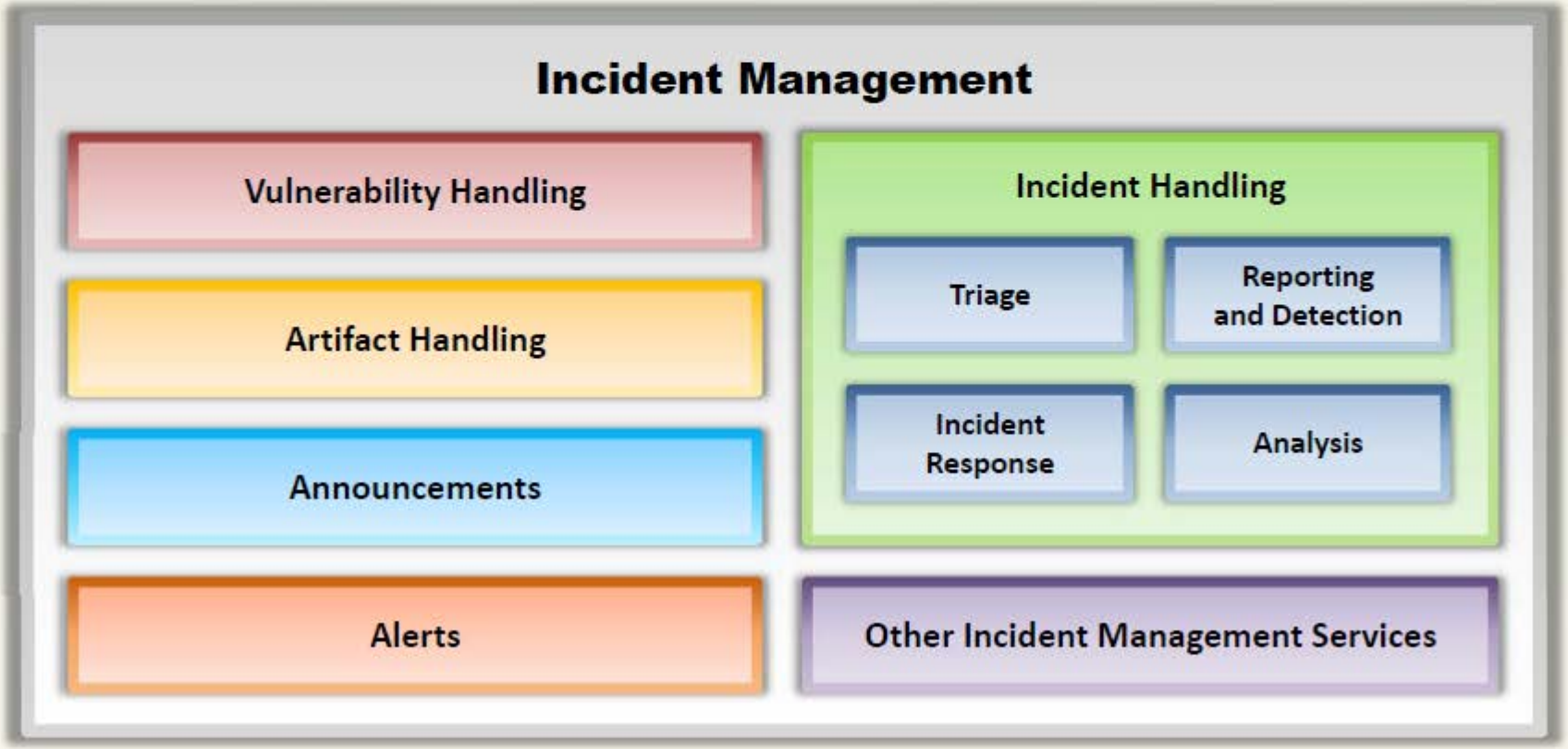
- Environmental threats
  - Floods
  - Fire
  - Earthquakes
  - Dust
- Man made threats
  - Terrorism
  - Wars
  - Explosion
  - Dumpster diving and theft
  - Vandalism

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

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

C|EH Certified Ethical Hacker

Managing security issues by taking a **proactive approach** towards the customers' security vulnerabilities and **by responding effectively** to potential information security incidents

Providing a **single point of contact** for reporting security incidents and issues

Developing or **reviewing** the processes and procedures that must be followed in response to an incident

Reviewing **changes in legal and regulatory requirements** to ensure that all processes and procedures are valid

Managing the response to an incident and ensuring that **all procedures are followed** correctly in order **to minimize** and **control the damage**

Reviewing existing controls and recommending steps and technologies to **prevent future security incidents**

Identifying and **analyzing** what has happened during an incident, including the impact and threat

Establishing **relationship with local law enforcement agency**, **government agencies**, key partners, and suppliers

What is Vulnerability Assessment?

Vulnerability assessment is an **examination of the ability of a system or application**, including current security procedures and controls, to withstand assault

It recognizes, measures, and classifies security vulnerabilities in a **computer system**, **network**, and **communication channels**

A vulnerability assessment may be used to:

Identify weaknesses that could be exploited

Predict the effectiveness of additional security measures in protecting information resources from attack

Types of Vulnerability Assessment

C|EH Certified Ethical Hacker

Active Assessment

Uses a network scanner to find hosts, services, and vulnerabilities

External Assessment

Assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world

Passive Assessment

A technique used to sniff the network traffic to find out active systems, network services, applications, and vulnerabilities present

Application Assessments

Tests the web infrastructure for any misconfiguration and known vulnerabilities

Host-based Assessment

Determines the vulnerabilities in a specific workstation or server

Network Assessments

Determines the possible network security attacks that may occur on the organization's system

Internal Assessment

A technique to scan the internal infrastructure to find out the exploits and vulnerabilities

Wireless Network Assessments

Determines the vulnerabilities in organization's wireless networks

Network Vulnerability Assessment Methodology

Phase I – Acquisition

- Collect documents required to:
  - Review **laws and procedures** related to network vulnerability assessment
  - **Identify and review document related to network security**
  - Review the **list of previously discovered vulnerabilities**

Phase II - Identification

- Conduct **interviews with customers and employees** involved in system architecture design, and administration
- Gather **technical information about all network components**
- Identify different industry standards which network security system complies to

Phase III - Analyzing

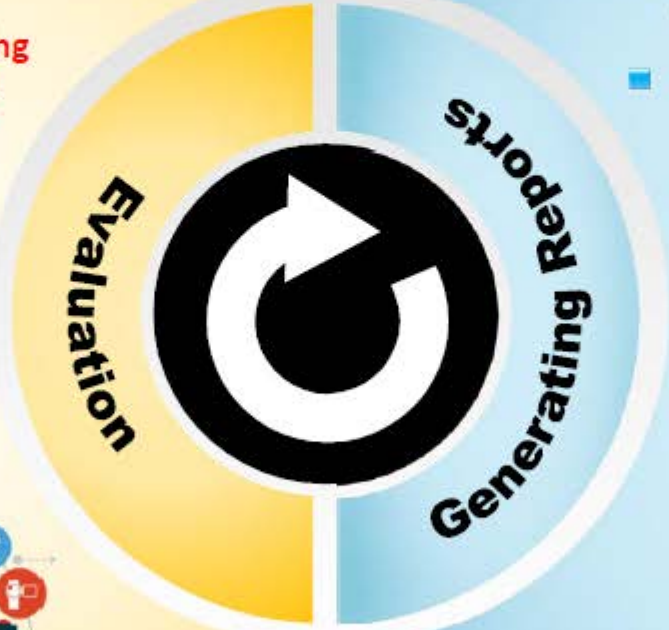
- Review interviews
- **Analyze the results** of previous vulnerability assessment
- Analyze security vulnerabilities and **identify risks**
- Perform **threat and risk analysis**
- Analyze the effectiveness of **existing security controls**
- Analyze the effectiveness of **existing security policies**

Network Vulnerability Assessment Methodology (Cont'd)

C|EH Certified Ethical Hacker

Phase IV - Evaluation

- Determine the probability of exploitation of **identified vulnerabilities**
- Identify the gaps between **existing and required security measures**
- **Determine the controls** required to mitigate the identified vulnerabilities
- **Identify upgrades** required to the network vulnerability assessment process



Phase V - Generating Reports

- The result of analysis must be presented in a **draft report** to be evaluated for further variations
- **Report should contain:**
  - Task rendered by each team member
  - Methods used and findings
  - General and specific recommendations
  - Terms used and their definitions
  - Information collected from all the phases
- All documents must be **stored in a central database** for generating the final report

Vulnerability Research

C|EH Certified Ethical Hacker

- The process of **discovering vulnerabilities and design flaws** that will open an operating system and its applications to attack or misuse
- Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote)

An administrator needs vulnerability research:

To gather information about **security trends**, **threats**, and **attacks**

To find **weaknesses**, and alert the network administrator before a **network attack**

To know **how to recover** from a network attack

To **get information** that helps to prevent the security problems

Vulnerability Research Websites

C|EH Certified Ethical Hacker

CodeRed Center
http://www.eccouncil.org

Microsoft Vulnerability Research (MSVR)
http://technet.microsoft.com

Security Magazine
http://www.securitymagazine.com

SecurityFocus
http://www.securityfocus.com

Help Net Security
http://www.net-security.org

HackerStorm
http://www.hackerstorm.co.uk

SC Magazine
http://www.scmagazine.com

Computerworld
http://www.computerworld.com

HackerJournals
http://www.hackerjournals.com

WindowsSecurity
http://www.windowsecurity.com

Penetration Testing

C|EH Certified Ethical Hacker

01

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

02

Security measures are actively analyzed for design weaknesses, technical flaws and vulnerabilities

03

A penetration test will not only point out vulnerabilities, but will also **document** how the weaknesses can be exploited

04

The results are delivered comprehensively in a **report**, to executive management and technical audiences

Why Penetration Testing

C|EH Certified Ethical Hacker

- 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

C|EH Certified Ethical Hacker

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

C|EH Certified Ethical Hacker

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 performs penetration test on an information system with **no or a 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

C|EH Certified Ethical Hacker

01 Black-box

No prior knowledge of the infrastructure to be tested

- Blind Testing
- Double Blind Testing

02 White-box

Complete knowledge of the infrastructure that needs to be tested

03 Grey-box

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



Phases of Penetration Testing

C|EH Certified Ethical Hacker

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 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**

Penetration Testing Methodology

C|EH Certified Ethical Hacker

Penetration Testing Methodology (Cont'd)

Module Flow

1. Information Security Overview
2. Information Security Threats and Attack Vectors
3. Hacking Concepts, Types, and Phases
4. Ethical Hacking Concepts and Scope
5. Information Security Controls
6. 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

C|EH Certified Ethical Hacker

- 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:

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

http://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

http://www.hhs.gov

Sarbanes Oxley Act (SOX)

C|EH Certified Ethical Hacker

- 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)

C|EH Certified Ethical Hacker

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

http://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

http://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"	http://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	http://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	http://www.justice.gov
	Privacy Act of 1974	http://www.justice.gov
	National Information Infrastructure Protection Act of 1996	http://www.nrotc.navy.mil
	Computer Security Act of 1987	http://csrc.nist.gov
	Freedom of Information Act (FOIA)	http://www.foia.gov
	Computer Fraud and Abuse Act	http://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	http://www.ftc.gov

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	http://www.comlaw.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	http://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.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	http://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	http://www.laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	http://www.statutes.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	http://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	http://home.heinonline.org
	Industrial Design Protection Act	http://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	http://www.wipo.int
	Computer Hacking	http://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	http://www.mosstingrett.no
Hong Kong	Article 139 of the Basic Law	http://www.basiclaw.gov.hk

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