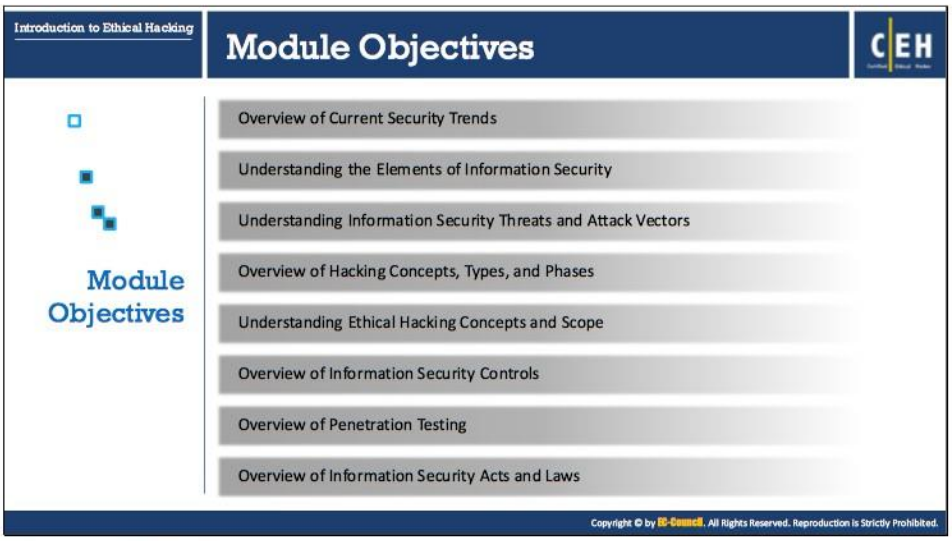
C|EH™
Certified Ethical Hacker

Module 01

Introduction to Ethical Hacking

This page is intentionally left blank.



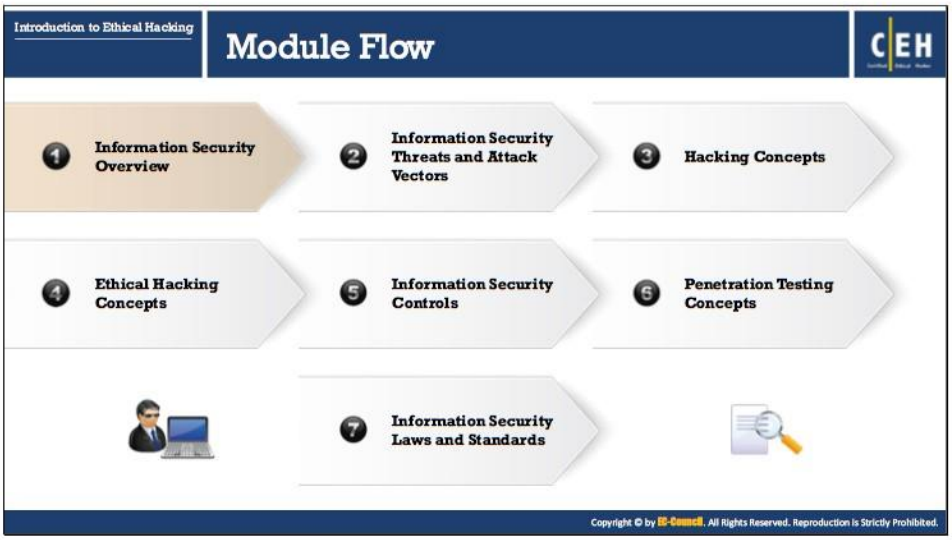
Module Objectives

Attackers break into systems for various reasons and purposes. Therefore, it is important to understand how malicious hackers attack and exploit systems, and the probable reasons behind those attacks. As Sun Tzu states in the Art of War, "If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat." It is the duty of system administrators and security professionals to guard their infrastructure against exploits by knowing the enemy—the malicious hacker(s)—who seeks to use the same infrastructure for illegal activities.

This module starts with an overview of the current security scenario and emerging threat vectors. It provides an insight into the different elements of information security. Later the module discusses hacking and ethical hacking concepts and ends with a brief discussion on information security controls, penetration testing process, and information security laws and Acts.

At the end of this module, you will be able to:

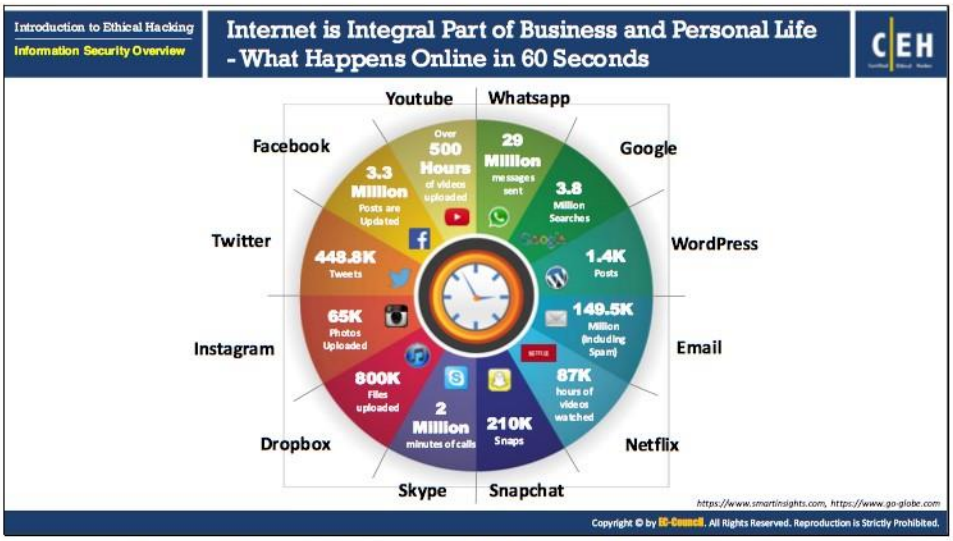
- Understand the current security trends
- Describe the elements of information security
- Explain information security threats and attack vectors
- Describe the hacking concepts, types, and phases
- Explain the ethical hacking concepts and scope
- Understand the information security controls (information security management, defense-in-depth, policies, procedures, awareness, physical security, incident management process, and risk management etc.)
- Understand the penetration testing process
- Know about the information security Acts and Laws



Information Security Overview

Information security refers to the protection or safeguard of information and information systems that use, store, and transmit information from unauthorized accesses, disclosures, alterations, and destructions. Information is the critical asset that organizations need to secure. If sensitive information falls in wrong hands, then the respective organization may suffer huge losses in terms of finances, brand reputation, customers, etc. In an attempt to understand how to secure such critical information resources, let us start with an overview of information security.

This section covers various statistics, threat predictions, and essential terminology pertaining to information security, elements of information security, as well as the security, functionality, and usability triangle.

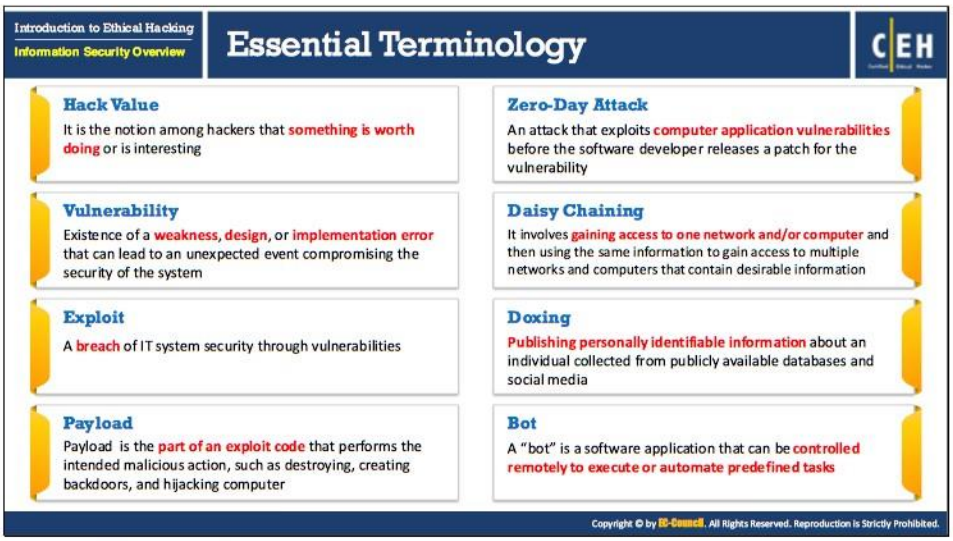


Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds

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

The Internet has become an integral part of modern business and personal life, as it helps in gaining information easily. Businesses and individuals rely on the Internet for various purposes such as browsing for content, social networking, communicating, shopping, downloading, and chatting, etc.

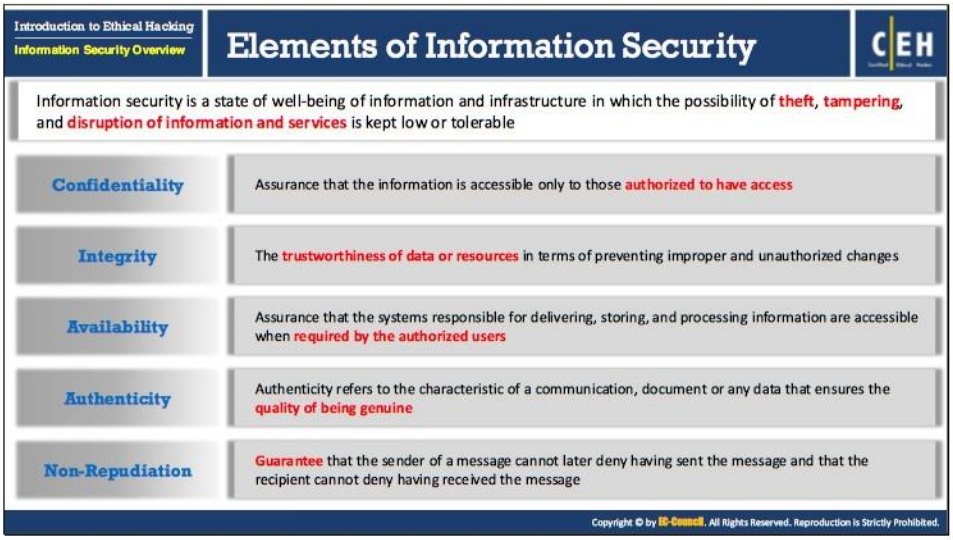
Currently there are approximately 3.81 billion Internet users around the world. It is general practice nowadays for a person to look for a particular solution on the Internet and find satisfaction from an appropriate solution. Along with the facility of finding various Internet services, one of the most important and popular rising topics of general interest nowadays is social networking websites. It is very common for people to use social networking websites for regular contact with friends and relatives. The image in the slide depicts what can happen online in just 60 seconds.



Essential Terminology

- **Hack Value:** Hack value is the notion among hackers to evaluate something that is worth doing or is interesting. Hackers derive great satisfaction from breaking down the toughest network security, and consider it their accomplishment as it is something that not everyone can do.
- **Vulnerability:** Vulnerability is the existence of weakness, design, or an implementation error that, when exploited, leads to an unexpected and undesirable event compromising the security of the system. Simply put, vulnerability is a security loophole that allows an attacker to enter the system by bypassing various user authentications.
- **Exploit:** An exploit is a breach of IT system security through vulnerabilities, in the context of an attack on a system or network. It also refers to malicious software or commands that can cause unanticipated behavior of legitimate software or hardware through attackers taking advantage of the vulnerabilities.
- **Payload:** Payload is the part of a malware or an exploit code that performs the intended malicious actions, which can include creating backdoor access to a victim's machine, damaging or deleting files, committing data theft and hijacking computer. Hackers use various methods to execute the payload. For example, they can activate a logic bomb, execute an infected program, or use an unprotected computer connected to a network.
- **Zero-Day Attack:** In a Zero-Day attack, the attacker exploits vulnerabilities in a computer application before the software developer can release a patch for them.
- **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.

- **Doxing:** Doxing refers to gathering and publishing personally identifiable information such as an individual's name and email address, or other sensitive information pertaining to an entire organization. People with malicious intent collect this information from publicly accessible channels such as the databases, social media and the Internet.
- **Bot:** A "bot" (a contraction of "robot") is a software application or program that can be controlled remotely to execute or automate predefined tasks. Hackers use bots as agents that carry out malicious activity over the Internet. Attackers use infected machines to launch distributed denial-of-service (DDoS) attacks, keylogging, spying, etc.



Elements of Information Security

Information security is defined as "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." It relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

- **Confidentiality**

  Confidentiality is the assurance that the information is accessible only to those who are authorized to have access. Confidentiality breaches may occur due to improper data handling or a hacking attempt. Confidentiality controls include data classification, data encryption, and proper equipment disposal (i.e. of DVDs, CDs, etc.).

- **Integrity**

  Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only the authorized people can update, add, and delete data to protect its integrity).

- **Availability**

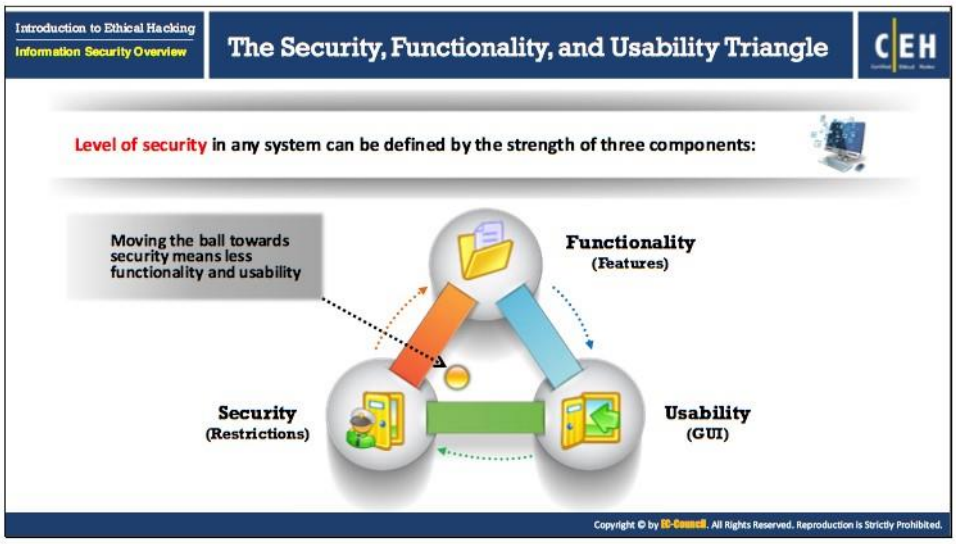
  Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain data availability can include redundant systems' disk arrays and clustered machines, antivirus software to stop malware from destroying networks, and distributed denial-of-service (DDoS) prevention systems.

- **Authenticity**

  Authenticity refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that a user is genuine, one who he / she claims to be. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, or documents.

- **Non-Repudiation**

  Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. Individuals and organization use digital signatures to ensure non-repudiation.



The Security, Functionality, and Usability Triangle

Technology is evolving at an unprecedented rate. As a result, new products that are reaching the market focus more on ease-of-use than on secure computing. Though technology was originally developed for "honest" research and academic purposes, it has not evolved at the same pace as users' proficiency. Moreover, in this evolution, system designers often overlook vulnerabilities during the intended deployment of the system. However, adding more built-in default security mechanisms allows users more competence. It is becoming difficult for system administrators and system security professionals to allocate resources, exclusively for securing systems, with the augmented use of computers for an increasing number of routine activities. This includes the time needed to check log files, detect vulnerabilities, and apply security update patches.

As routine activities consume system administrators' time, leaving less time for vigilant administration, there is little time to deploy measures and secure computing resources on a regular and innovative basis. This fact has increased the demand for dedicated security professionals to constantly monitor and defend ICT (Information and Communication Technology) resources.

Originally, to "hack" meant to possess extraordinary computer skills to explore hidden features of computer systems. In the context of information security, hacking is defined as the exploitation of vulnerabilities of computer systems and networks and requires great proficiency. However, today there are automated tools and codes available on the Internet that make it possible for anyone, who possesses the will, to succeed at hacking. However, mere compromise of system security does not denote hacking success. There are websites that insist on "taking back the Internet" as well as people who believe that they are doing everyone a

favor by posting details of their exploits. In reality, doing so serves to hamper the skill level required to become a successful attacker.

The ease with which system vulnerabilities can be exploited has increased while the knowledge curve required to perform such exploits has decreased. The concept of the elite "super attacker" is an illusion. However, the fast-evolving genre of "script kiddies" is largely comprised of lesser-skilled individuals having second-hand knowledge of performing exploits. One of the main impediments contributing to the growth of security infrastructure lies in the unwillingness of exploited or compromised victims to report such incidents for fear of losing the goodwill and faith of their employees, customers, or partners, and/or of losing market share. The trend of information assets influencing the market has seen more companies thinking twice before reporting incidents to law enforcement officials for fear of "bad press" and negative publicity.

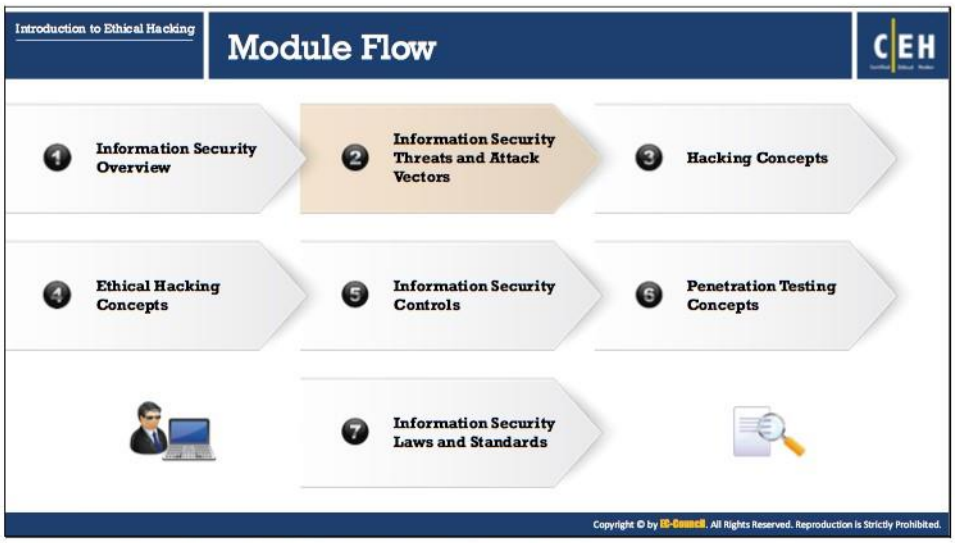
The increasingly networked environment, with companies often using their websites as single points of contact across geographical boundaries, makes it critical for administrators to take countermeasures to prevent exploits that can result in data loss. This is why corporations need to invest in security measures to protect their information assets.

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

- **Functionality**: The set of features provided by the system.
- **Usability**: The GUI components used to design the system for ease of use.
- **Security**: Restrictions imposed on accessing the components of the system.

The relationship between these three components is demonstrated by using a triangle because increase or decrease in any one of the component automatically affects the other two components. Moving the ball towards any of the three components means decreasing the intensity of other two components.

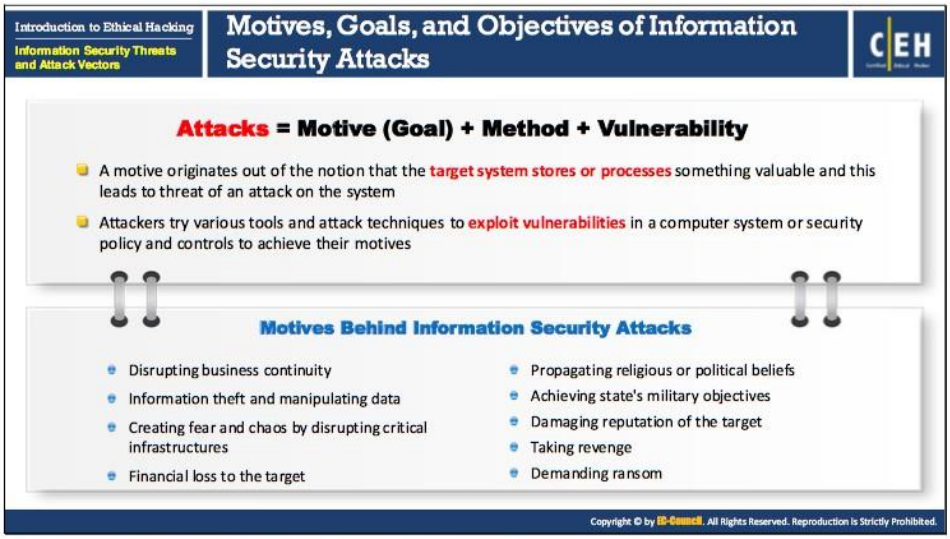
The diagram in the slide represents the relationship between functionality, usability, and security. For example, as shown in the slide above, if the ball moves towards Security it means increased security and decreased Functionality and Usability. If the ball is in the center of the triangle, then all the three components are balanced. If the ball moves towards usability it means an increased Usability and decreased Functionality as well as Security. For any implementation of security controls, all the three components have to be considered carefully and balanced to get acceptable functionality and usability with acceptable security.



Information Security Threats and Attack Vectors

There are various categories of information security threats, such as network threats, host threats, and application threats, and various attack vectors, such as viruses, worms, botnets, that might affect an organization's information security.

This section introduces you to the motives, goals, and objectives of information security attacks, top information security attack vectors, information security threat categories, and the types of attacks on a system.



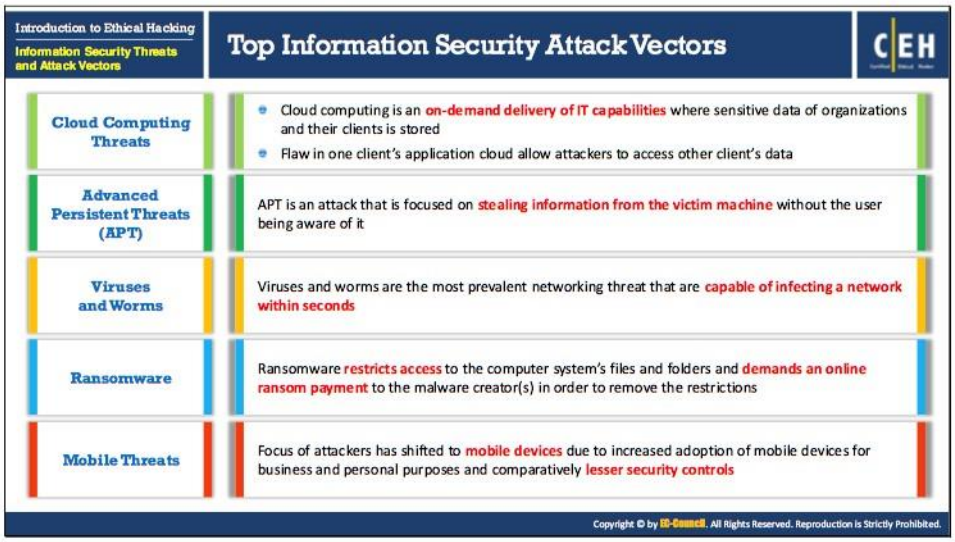
Motives, Goals, and Objectives of Information Security Attacks

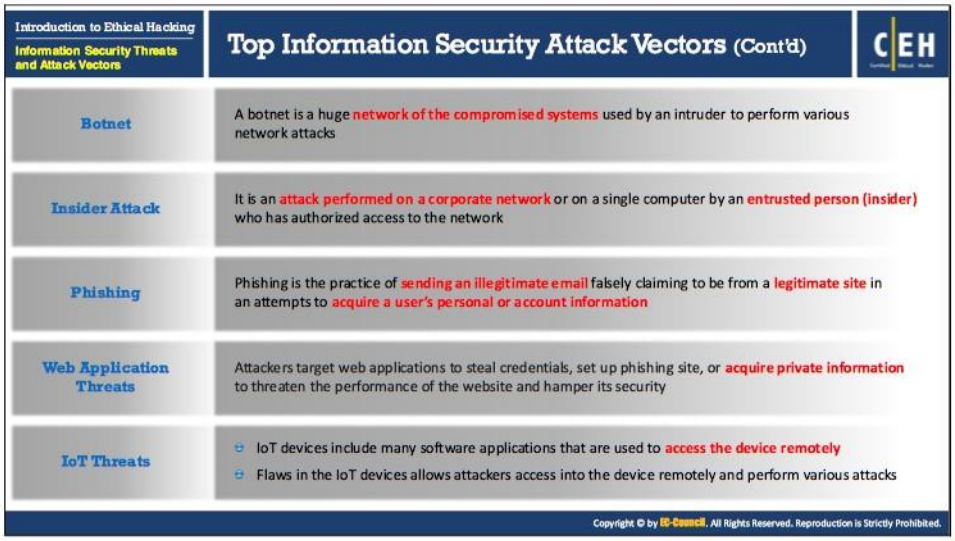
Attackers generally have motives (goals), and objectives behind information security attacks. A motive originates out of the notion that a target system stores or processes something valuable, which leads to the threat of an attack on the system. The purpose of the attack may be to disrupt the target organization's business operations, to steal valuable information for the sake of curiosity, or even to exact revenge. Therefore, these motives or goals depend on the attacker's state of mind, his/her reason for carrying out such an activity, as well as his/her resources and capabilities. Once the attacker determines his/her goal, he/she can employ various tools, attack techniques, and methods to exploit vulnerabilities in a computer system or security policy and controls.

Attacks = Motive (Goal) + Method + Vulnerability

Motives behind information security attacks

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





Top Information Security Attack Vectors

Below is a list of information security attack vectors through which an attacker can gain access to a computer or network server to deliver a payload or malicious outcome.

- **Cloud Computing Threats:** Cloud computing is an on-demand delivery of IT capabilities in which IT infrastructure and applications are provided to subscribers as a metered service over a network. Clients can store sensitive information on the cloud. Flaw in one

client's application cloud could potentially allow attackers to access another client's data.

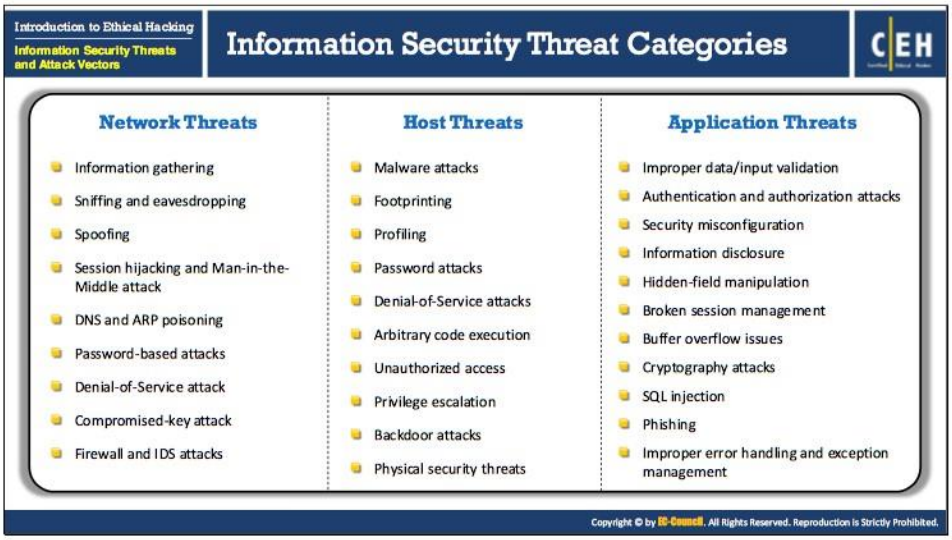
- **Advanced Persistent Threats (APT):** Advanced Persistent Threat (APT) is an attack that focuses on stealing information from the victim machine without its user being aware of it. These attacks are generally targeted at large companies and government networks. APT attacks are slow in nature, so the effect on computer performance and Internet connections is negligible. APTs exploit vulnerabilities in the applications running on a computer, operating system, and embedded systems.
- **Viruses and Worms:** Viruses and worms are the most prevalent networking threats, capable of infecting a network within seconds. A virus is a self-replicating program that produces a copy of itself by attaching to another program, computer boot sector or document. A worm is a malicious program that replicates, executes and spreads across network connections.

  Viruses make their way into the computer when the attacker shares a malicious file containing it with the victim through the Internet, or through any removable media. Worms enter a network when the victim downloads a malicious file, opens a spam mail or browses a malicious website.
- **Ransomware:** Ransomware is a type of a malware, which restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) in order to remove the restrictions. It is generally spread via malicious attachments to email messages, infected software applications, infected disks or compromised websites.
- **Mobile Threats:** Attackers are increasingly focusing on mobile devices, due to the increased adoption of smart phones for business and personal use and their comparatively fewer security controls.

  Users may download malware applications (APKs) onto their smartphones, which can damage other applications and data and convey sensitive information to attackers. Attackers can remotely access a smartphone's camera and recording app to view user activities and track voice communications, which can aid them in an attack.
- **Botnet:** A botnet is a huge network of compromised systems used by attackers to perform denial-of-service attacks. Bots, in a botnet, perform tasks such as uploading viruses, sending mails with botnets attached to them, stealing data, and so on. Antivirus programs might fail to find—or even scan for—spyware or botnets. Hence, it is essential to deploy programs specifically designed to find and eliminate such threats.
- **Insider Attack:** An insider attack is an attack by someone from within an organization who has authorized access to its network and is aware of the network architecture.
- **Phishing:** Phishing is a practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information. Attackers perform phishing attacks by distributing malicious links via some communication channel or mails to obtain private information like account numbers,

credit card numbers, mobile numbers, etc. from the victim. Attackers design emails to lure victims such a way that they appear to be from some legitimate source or at times they send malicious links that resemble a legitimate website.

- **Web Application Threats:** Web application attacks like SQL injection, cross-site scripting has made web applications a favorable target for the attackers to steal credentials, set up phishing site, or acquire private information. Majority of such attacks are the result of flawed coding and improper sanitization of input and output data from the web application. Web application attacks can threaten the performance of the website and hamper its security.
- **IoT Threats:** The IoT devices connected to the Internet have little or no security that makes them vulnerable to various types of attacks. These devices include many software applications that are used to access the device remotely. Due to the hardware constraints such as memory, battery, etc. these IoT applications do not include complex security mechanisms to protect the devices from attacks. These drawbacks make the IoT devices more vulnerable and allow attackers to access the device remotely and perform various attacks.



Information Security Threat Categories

There are three types of information security threats:

- **Network Threats**

  A network is the collection of computers and other hardware connected by communication channels to share resources and information. As the information travels from one system to the other through the communication channel, a malicious person might break into the communication channel and steal the information traveling over the network.

  Listed below are some of the network threats:

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

- **Host Threats**

  Host threats target a particular system on which valuable information resides. Attackers try to breach the security of the information system resource.

  Listed below are some of the host threats:

  - Malware attacks
  - Foot printing
  - Profiling
  - Password attacks

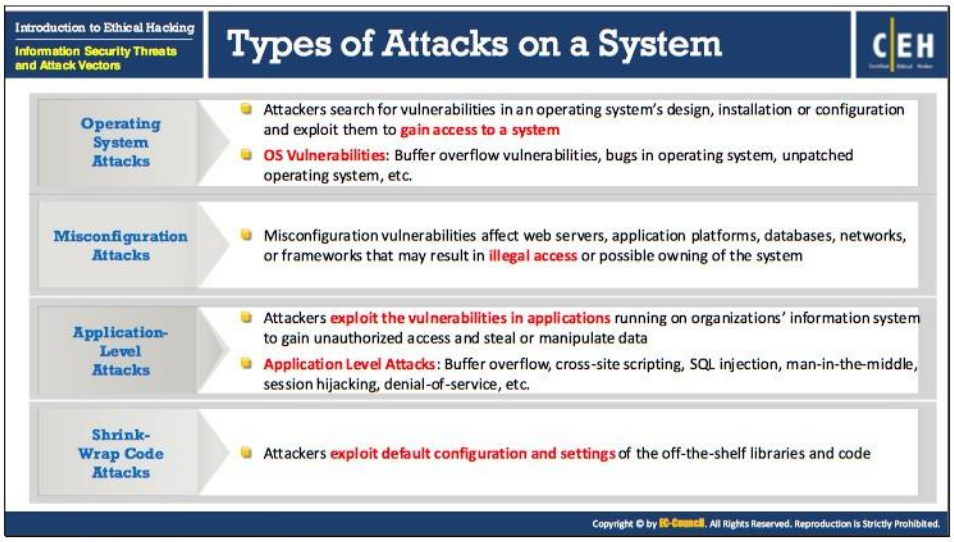
- Denial-of-Service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Backdoor attacks
- Physical security threats

- **Application Threats**

  Applications can be vulnerable if proper security measures are not taken while developing, deploying, and maintaining them. Attackers exploit the vulnerabilities present in an application to steal or destroy data.

  Listed below are some of the application threats:

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



Types of Attacks on a System

Many approaches exist for an attacker to gain access to the system. One common requirement for all such approaches is that the attacker finds and exploits a system's weakness or vulnerability.

- **Operating System Attacks**

  Today's Operating Systems (OS) are loaded with features and are increasingly complex. While users take advantage of these features, they are prone to more vulnerabilities, thus enticing attackers. Operating systems run many services such as graphical user interfaces (GUIs) that support applications and system tools, and enable Internet access. Extensive tweaking is required to lock them down. Attackers constantly look for OS vulnerabilities that allow them to exploit and gain access to a target system or network. To stop attackers from compromising the network, the system or network administrators must keep abreast of various new exploits and methods adopted by attackers, and monitor the networks regularly.

  By default, most operating systems' installation programs install a large number of services and open ports. This situation leads attackers to search for vulnerabilities. Applying patches and hot fixes is not easy with today's complex networks. Most patches and fixes tend to solve an immediate issue. In order to protect the system from operating system attacks in general, it is necessary to remove and/or disable any unneeded ports and services.

  Some OS vulnerabilities include:

  - Buffer overflow vulnerabilities
  - Bugs in the operating system

- An unpatched operating system

Attacks performed at the OS level include:

- Exploiting specific network protocol implementations
- Attacking built-in authentication systems
- Breaking file-system security
- Cracking passwords and encryption mechanisms

- **Misconfiguration Attacks**

Security misconfiguration or poorly configured security controls might allow attackers to gain unauthorized access to the system, compromise files, or perform other unintended actions. Misconfiguration vulnerabilities affect web servers, application platforms, databases, networks, or frameworks that may result in illegal access or possible system takeover. Administrators should change the default configuration of the devices before deploying them in the production network. To optimize the configuration of the machine, remove any unneeded services or software. Automated scanners detect missing patches, misconfigurations, use of default accounts, unnecessary services, and so on.

- **Application-Level Attacks**

Software developers are often under intense pressure to meet deadlines, which can mean they do not have sufficient time to completely test their products before shipping them, leaving undiscovered security holes. This is particularly troublesome in newer software applications that come with a large number of features and functionalities, making them more and more complex. An increase in the complexity means more opportunities for vulnerabilities. Attackers find and exploit these vulnerabilities in the applications using different tools and techniques to gain unauthorized access and steal or manipulate data.

Security is not always a high priority to software developers, and they handle it as an "add-on" component after release. This means that not all instances of the software will have the same level of security. Error checking in these applications can be very poor (or even nonexistent), which leads to:

- Buffer overflow attacks
- Sensitive information disclosure
- Cross-site scripting
- Session hijacking
- Man-in-the-middle attacks
- Denial-of-service attacks
- SQL injection attacks
- Phishing
- Parameter/form tampering
- Directory traversal attacks

Examples of Application-Level Attacks

- **Session Hijacking**

  Attackers may exploit session information in the vulnerable applications to perform session hijacking if the code implements a cookie less authentication. When the target tries to browse through a URL, the session or authentication token appears in the request URL instead of the secure cookie, to give access to the URL requested by the target. Here, an attacker using his or her skills and monitoring tools can hijack the targets' session and steal all sensitive information.

  Vulnerable Code

  Given below is the vulnerable code, which allows an attacker to perform session hijacking by exploiting the vulnerability present at the line 4.

```
1: <configuration>
2:  <system.web>
3:    <authentication mode="Forms">
4:    <forms cookieless="UseUri">
5:  </system.web>
6: </configuration>
```

  FIGURE 1.1: Session Hijacking Vulnerable Code

  Secure Code

  Use "UseCookies" instead of "UseUri" at line 4 in the above code to secure it from session hijacking attacks.

```
1: <configuration>
2:  <system.web>
3:    <authentication mode="Forms">
4:    <forms cookieless="UseCookies">
5:  </system.web>
6: </configuration>
```

  FIGURE 1.2: Session Hijacking Secure Code

- **Denial-of-Service**

  Denial of Service (DoS) is an attack on a computer or network that reduces, restricts, or prevents legitimate use of its resources. In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources.

  Vulnerable Code

  Shown below is the vulnerable code that allows an attacker to perform a denial-of-service attack, as it fails to release a connection resource.

```
1:  Statement stmnt = conn.createStatement ();
2:  ResultSet rsltset = stmnt.executeQuery ();
3:  stmnt.close ();
```

FIGURE 1.3: Denial-of-Service Vulnerable Code

Secure Code

You can use a "**`finally`**" block to secure the above code.

```
1:  Statement stmnt;
2:  try {stmnt = conn.createStatement ();
3:  stmnt.executeQuery (); }
4:  finally {
5:  If (stmnt! = null) {
6:  try { stmnt.close ();
7:  } catch (SQLException sqlexp) { }
8:  } catch (SQLException sqlexp) { }
```

FIGURE 1.4: Denial-of-Service Secure Code

- **Shrink-Wrap Code Attacks**

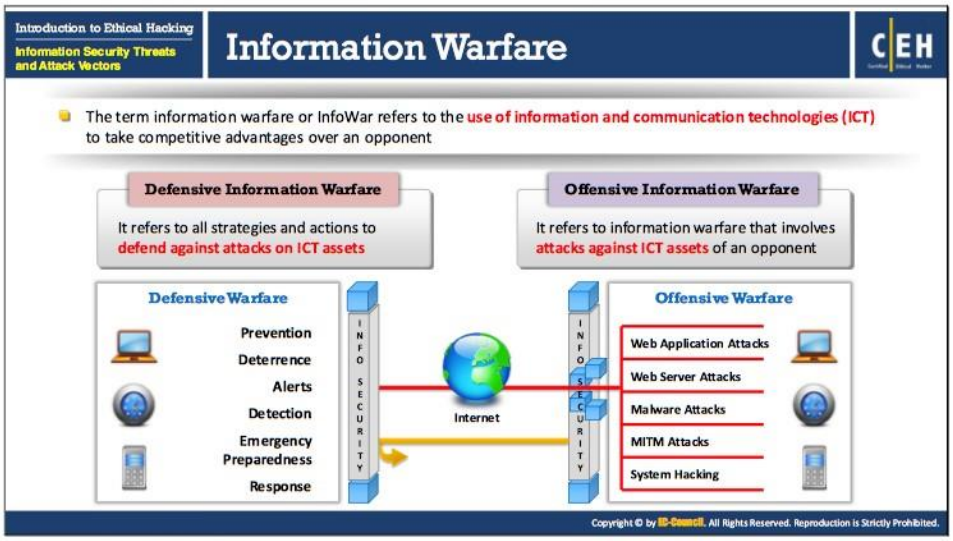
  Software developers often use free libraries and code licensed from other sources in their programs to reduce development time and cost. This means that large portions of many pieces of software will be the same, and if an attacker discovers vulnerabilities in that code, many pieces of software are at risk.

  Attackers exploit default configuration and settings of the off-the-shelf libraries and code. The problem is that software developers leave the libraries and code unchanged. They need to customize and fine-tune every part of their code in order to make it not only more secure, but different enough so that the same exploit will not work.

  Example of shrink-wrap code:

```
go_to = 'http://www3.strongdefenseiz.in/?g2cy6v=16fM3XOrqai1ld7QyKKZi9rmopqq12mJ7arisNmjoqPL1pibnaesiQ%3D%3D';
num_days = 4;
function ged(noDays){
    var today = new Date();
    var expr = new Date(today.getTime() + noDays*24*60*60*1000);
    return  expr.toGMTString();
}

function readCookie(cookieName){

    var start = document.cookie.indexOf(cookieName);
    if (start == -1){
document.cookie = "seenit88=yes; expires=" + ged(num_days);
window.location = go_to;

    } else {
    }
}

var lang = (navigator.language || navigator.systemLanguage || navigator.userLanguage || 'en').substr(0, 2).toLowerCase();
if (window.navigator.userAgent.indexOf ("MSIE") >= 0){
if(lang == 'en' || lang == 'de' || lang == 'fr' || lang == 'it' || lang == 'pl' || lang == 'br'){
window.onFocus=readCookie("seenit88");

}
}
```

FIGURE 1.5: An Example of Shrink-Wrap Code



Information Warfare

Source: *http://www.iwar.org.uk*

The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) for competitive advantages over an opponent. Examples of information warfare weapons include viruses, worms, Trojan horses, logic bombs, trap doors, nano machines and microbes, electronic jamming, and penetration exploits and tools.

Martin Libicki has divided information warfare into the following categories:

- **Command and control warfare (C2 warfare):** In the computer security industry, C2 warfare refers to the impact an attacker possesses over a compromised system or network that they control.
- **Intelligence-based warfare:** Intelligence-based warfare is a sensor-based technology that directly corrupts technological systems. According to Libicki, "intelligence-based warfare" is a warfare that consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battle space.
- **Electronic warfare:** According to Libicki, electronic warfare uses radio electronic and cryptographic techniques to degrade communication. Radio electronic techniques attack the physical means of sending information, whereas cryptographic techniques use bits and bytes to disrupt the means of sending information.
- **Psychological warfare:** Psychological warfare is the use of various techniques such as propaganda and terror to demoralize one's adversary in an attempt to succeed in the battle.

- **Hacker warfare:** According to Libicki, the purpose of this type of warfare can vary from shutdown of systems, data errors, theft of information, theft of services, system monitoring, false messaging, and access to data. Hackers generally use viruses, logic bombs, Trojan horses, and sniffers to perform these attacks.
- **Economic warfare:** According to Libicki, economic information warfare can affect the economy of a business or nation by blocking the flow of information. This could be especially devastating to organizations that do a lot of business in the digital world.
- **Cyber warfare:** Libicki defines cyber warfare as the use of information systems against the virtual personas of individuals or groups. It is the broadest of all information warfare and includes information terrorism, semantic attacks (similar to Hacker warfare, but instead of harming a system, it takes the system over and the system will be perceived as operating correctly), and simula-warfare (simulated war, for example, acquiring weapons for mere demonstration rather than actual use).

Each form of the information warfare, mentioned above, consists of both defensive and offensive strategies.

- **Defensive Information Warfare**: Involves all strategies and actions to defend against attacks on ICT assets.
- **Offensive Information Warfare:** Involves attacks against ICT assets of an opponent.

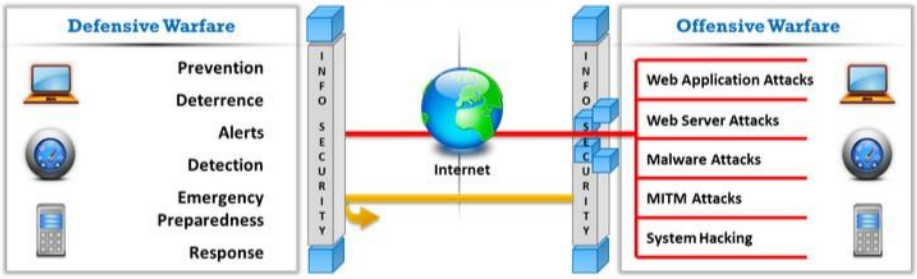
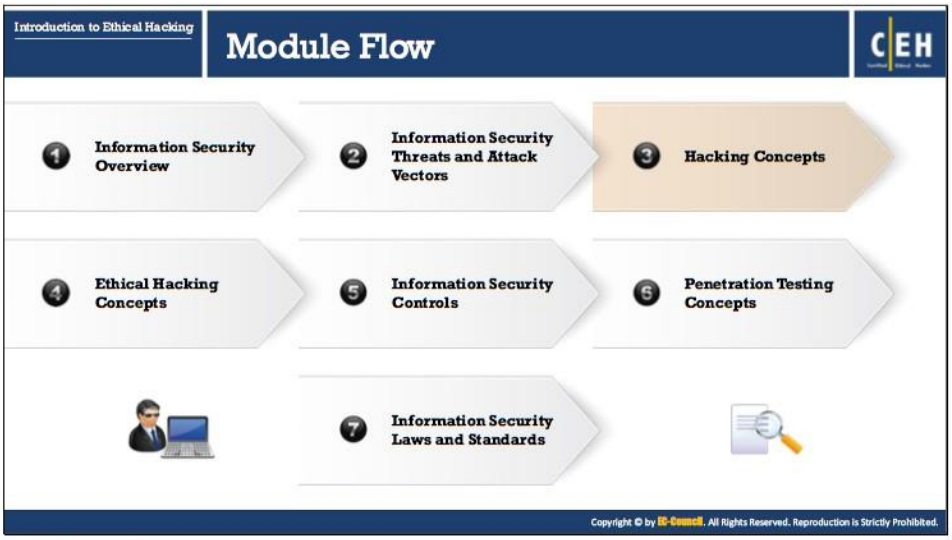
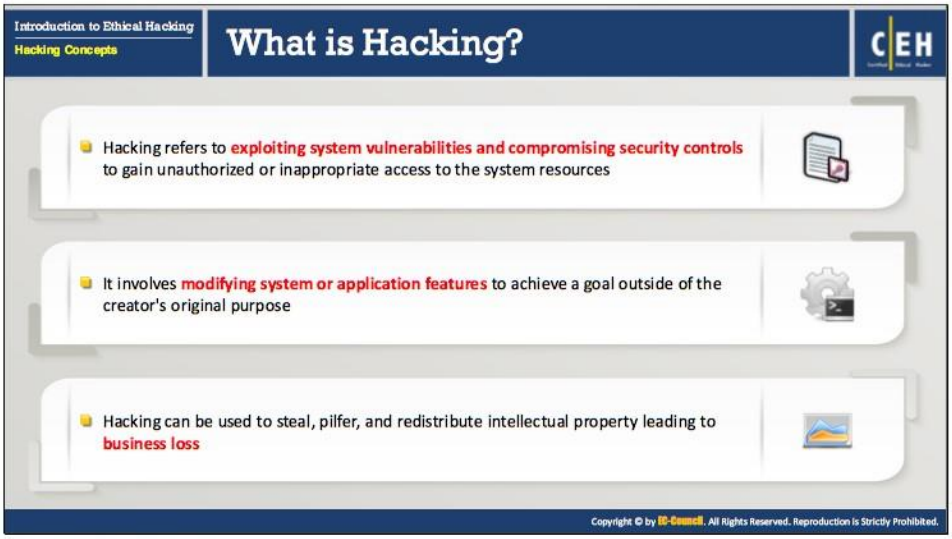


FIGURE 1.6: Block Diagram of Information Warfare



Hacking Concepts

This section deals with basic concepts of hacking: what is hacking, who is a hacker, and hacker classes—the five distinct hacking phases that one should be familiar with before proceeding with ethical hacking methodology.



What is Hacking?

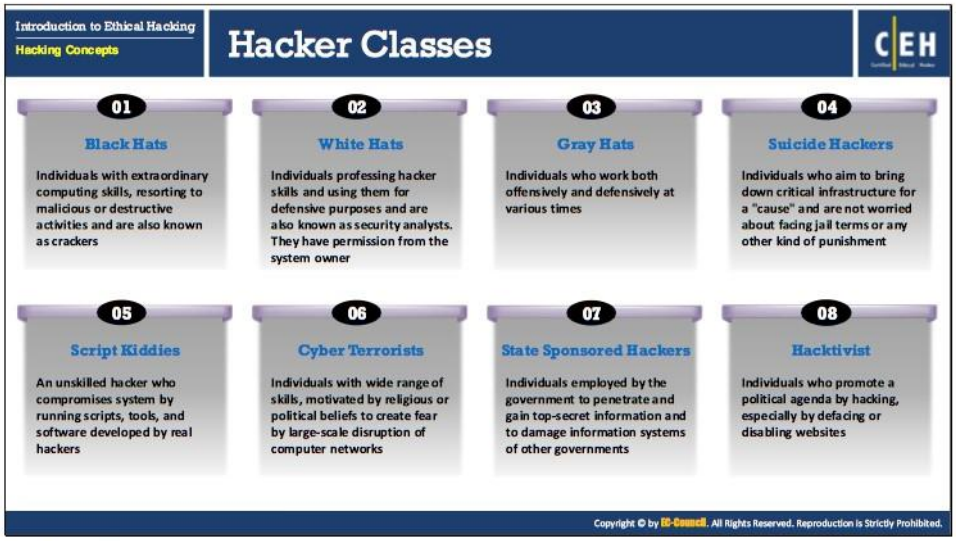
Hacking in the field of computer security refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to system resources. It involves modifying system or application features to achieve a goal outside its creator's original purpose. Hacking can be done to steal, pilfer, and redistribute intellectual property, thus leading to business loss.

Hacking on computer networks is generally done by means of scripts or other network programming. Network hacking techniques include creating viruses and worms, performing denial-of-service (DoS) attacks, establishing unauthorized remote access connections to a device using Trojans/backdoors, creating botnets, packet sniffing, phishing, and password cracking. The motive behind hacking could be to steal critical information and/or services, for thrill, intellectual challenge, curiosity, experiment, knowledge, financial gain, prestige, power, peer recognition, vengeance and vindictiveness, and so on.

Who is a Hacker?

A hacker is a person, who breaks into a system or network without any authorization to destroy, steal sensitive data, or performs malicious attacks. Hacker is an intelligent individual with excellent computer skills, along with the ability to create and explore into the computer's software and hardware. Usually a hacker would be a skilled engineer or programmer with enough knowledge to discover vulnerabilities in a target system. She/he is generally a subject expert and enjoys learning the details of various programming languages and computer systems.

For some hackers, hacking is a hobby to see how many computers or networks they can compromise. Their intention can be either 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.



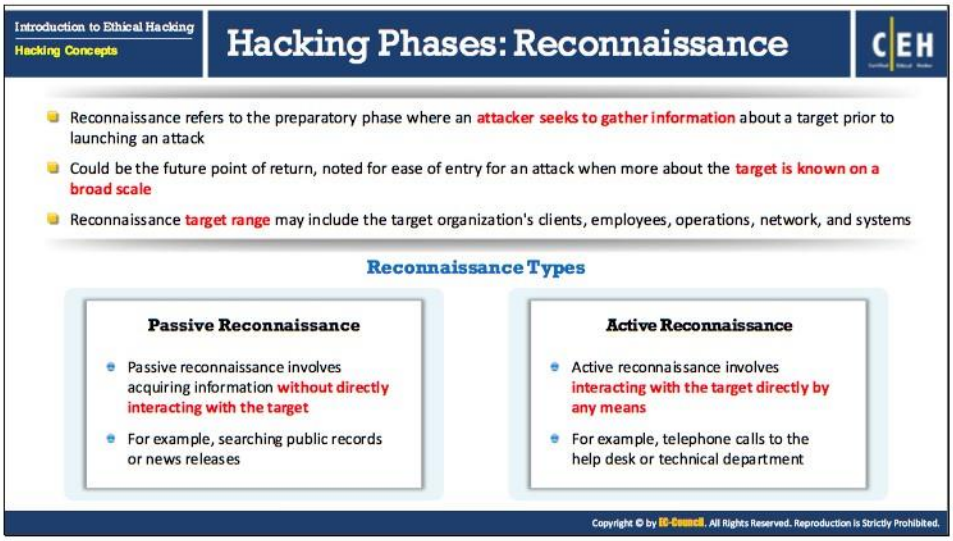
Hacker Classes

Hackers usually fall into one of the following categories, according to their activities:

- **Black Hats:** Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hacker is often involved with criminal activities. They are also known as crackers.
- **White Hats:** White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner.
- **Gray Hats:** Gray hats are the individuals who work both offensively and defensively at various times. Gray hats fall between white and black hats. Gray hats might help hackers in finding various vulnerabilities of a system or network and at the same time help vendors to improve products (software or hardware) by checking limitations and making them more secure.
- **Suicide Hackers:** Suicide hackers are 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. Suicide hackers are similar to suicide bombers, who sacrifice their life for an attack and are thus not concerned with the consequences of their actions.
- **Script Kiddies:** Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers. They usually focus on the quantity of attacks rather than the quality of the attacks that they initiate.

- **Cyber Terrorists:** Cyber terrorists are individuals with a wide range of skills, motivated by religious or political beliefs to create fear of large-scale disruption of computer networks.
- **State Sponsored Hackers:** State sponsored hackers are individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments.
- **Hacktivist:** Hacktivism is when hackers break into government or corporate computer systems as an act of protest. Hacktivists use hacking to increase awareness of their social or political agendas, as well as themselves, in both the online and offline arenas. They are individuals who promote a political agenda by hacking, especially by defacing or disabling websites.

  Common hacktivist targets include government agencies, multinational corporations, or any other entity that they perceive as a threat. It remains a fact, however, that gaining unauthorized access is a crime, irrespective of their intentions.



Hacking Phases

In general, there are five phases of hacking:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Hacking Phase: Reconnaissance

Reconnaissance refers to the preparatory phase in which an attacker gathers as much information as possible about the target prior to launching the attack. In this phase, the attacker draws on competitive intelligence to learn more about the target. It 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.

This phase allows attackers to plan the attack. This may take some time as the attacker gathers as much information as possible. Part of this reconnaissance may involve social engineering. A social engineer is a person who convinces people to reveal information such as unlisted phone numbers, passwords, and other sensitive information. For instance, the hacker could call the target's Internet service provider and, using whatever personal information previously obtained, convince the customer service representative that the hacker is actually the target, and in doing so, obtain even more information about the target.

Another reconnaissance technique is dumpster diving. Dumpster diving is, simply enough, looking through an organization's trash for any discarded sensitive information. Attackers can use the Internet to obtain information such as employees' contact information, business partners, technologies currently in use, and other critical business knowledge. But dumpster diving may provide them with even more sensitive information, such as user names, passwords, credit card statements, bank statements, ATM receipts, Social Security numbers, private telephone numbers, checking account numbers, and any number of other things.

Searching for the target company's web site in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information.

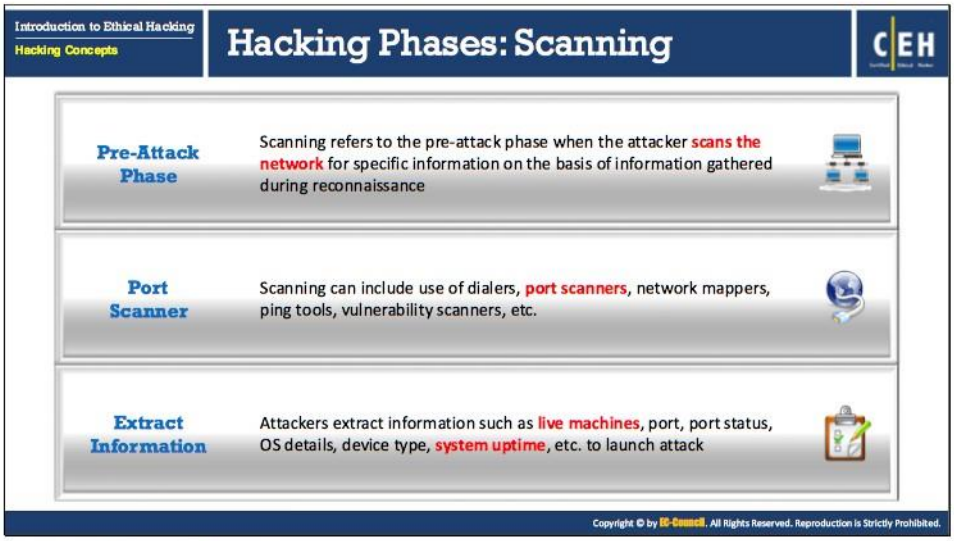
Reconnaissance Types

Reconnaissance techniques are broadly categorized into active and passive.

When an attacker is using passive reconnaissance techniques, she/he does not interact with the target directly. Instead, the attacker relies on publicly available information, news releases, etc.

Active reconnaissance techniques, on the other hand, involve direct interactions with the target system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications. Attackers use active reconnaissance when there is a low probability of detection of these activities. For example, telephone calls to the help desk or technical department.

As an ethical hacker, you must be able to distinguish among the various reconnaissance methods, and advocate preventive measures in the light of potential threats. Companies, on their part, must address security as an integral part of their business and/or operational strategy, and be equipped with the proper policies and procedures to check for potential vulnerabilities.



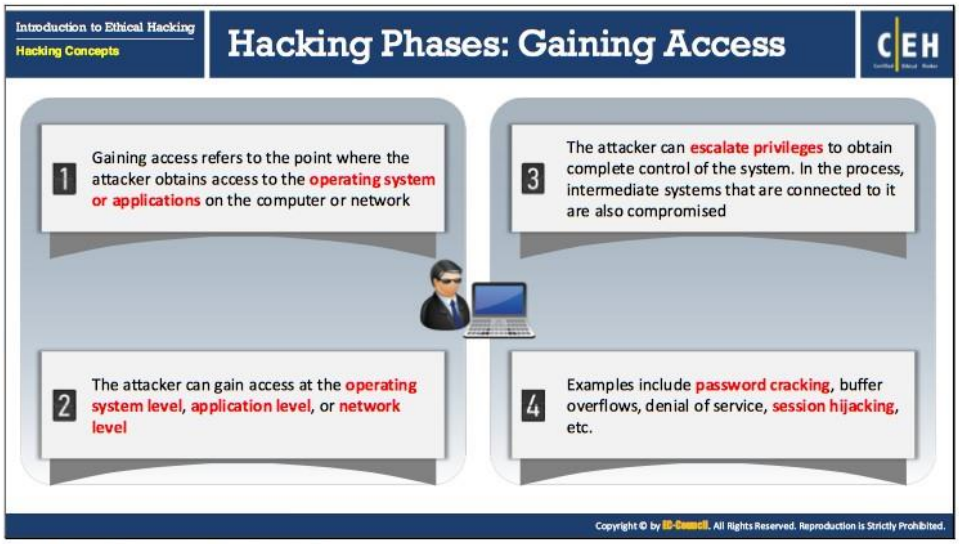
Hacking Phase: Scanning

Scanning is the phase immediately preceding the attack. Here, the attacker uses the details gathered during reconnaissance to scan the network for specific information. Scanning is a logical extension of active reconnaissance, and in fact, some experts do not differentiate scanning from active reconnaissance. There is a slight difference, however, in that scanning involves more in-depth probing on the part of the attacker. Often the reconnaissance and scanning phases overlap, and it is not always possible to separate the two. An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as the standard Windows utility Traceroute. Alternatively, they can use tools such as Cheops to add additional information to Traceroute's results.

Scanning can include use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, etc. Attackers extract information such as live machines, port, port status, OS details, device type, system uptime, etc. to launch attack.

Port scanners detect listening ports to find information about the nature of services running on the target machine. The primary defense technique against port scanners is to shut down services that are not required, as well as to implement appropriate port filtering. However, attackers can still use tools to determine the rules implemented by the port filtering.

The most commonly used tools are vulnerability scanners, which can search for thousands of known vulnerabilities on a target network. This gives the attacker an advantage because he or she only has to find a single means of entry, while the systems professional has to secure as much vulnerability as possible by applying patches. Organizations that use intrusion detection systems still have to remain vigilant, because attackers can and will use evasion techniques at every step of the way.

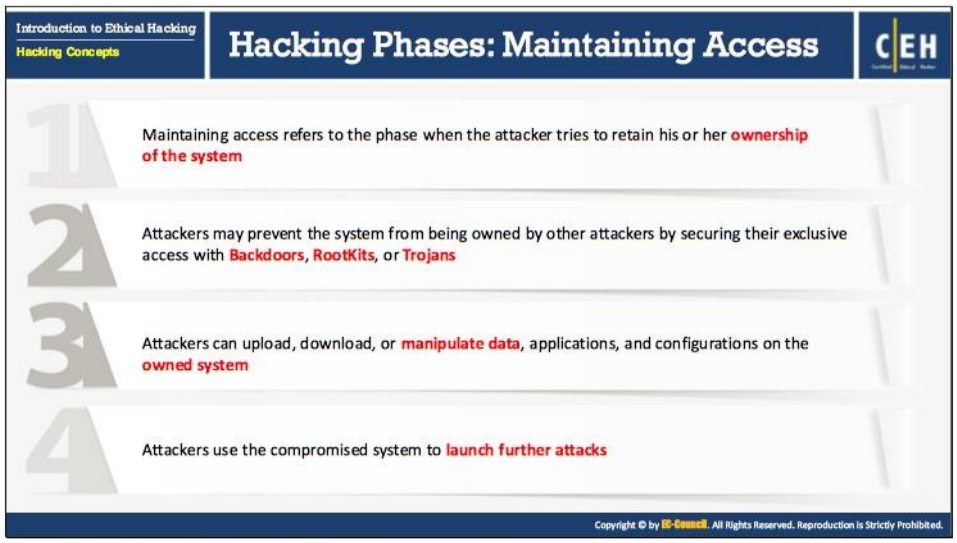


Hacking Phase: Gaining Access

This is the phase in which real hacking occurs. Attackers use vulnerabilities identified during the reconnaissance and scanning phase to gain access to the target system and network. 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. Even though attackers can cause plenty of damage without gaining any access to the system, the impact of unauthorized access is catastrophic. For instance, external denial-of-service attacks can either exhaust resources or stop services from running on the target system. Ending processes can stop a service, using a logic bomb or time bomb, or even reconfiguring and crashing the system. Thus attackers can exhaust system and network resources by consuming all outgoing communication links.

Attackers gain access to the target system locally (offline), over a LAN, or over the Internet. Examples include password cracking, stack-based buffer overflows, denial-of-service, and session hijacking. Using a technique called spoofing to exploit the system by pretending to be a legitimate user or different systems, they can send a data packet containing a bug to the target system in order to exploit a vulnerability. Packet flooding also breaks the availability of essential services. Smurf attacks attempt to cause users on a network to flood each other with data, making it appear as if everyone is attacking each other, and leaving the hacker anonymous.

A hacker's chances of gaining access into a target system depend on several factors, such as the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained. Once an attacker gains access to the target system, he/she then tries to escalate privileges in order to take complete control of the target system. In the process, intermediate systems that are connected to it are also compromised.



Hacking Phase: Maintaining Access

Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system. Once an attacker gains access to the target system with admin/root level privileges (thus owning the system), he or she is able to use both the system and its resources at will, and can either use the system as a launch pad to scan and exploit other systems, or to keep a low profile and continue exploiting the system. Both these actions can cause a great amount of damage. For instance, the hacker could implement a sniffer to capture all network traffic, including Telnet and FTP (file transfer protocol) sessions with other systems, and then transmit that data wherever he or she pleases.

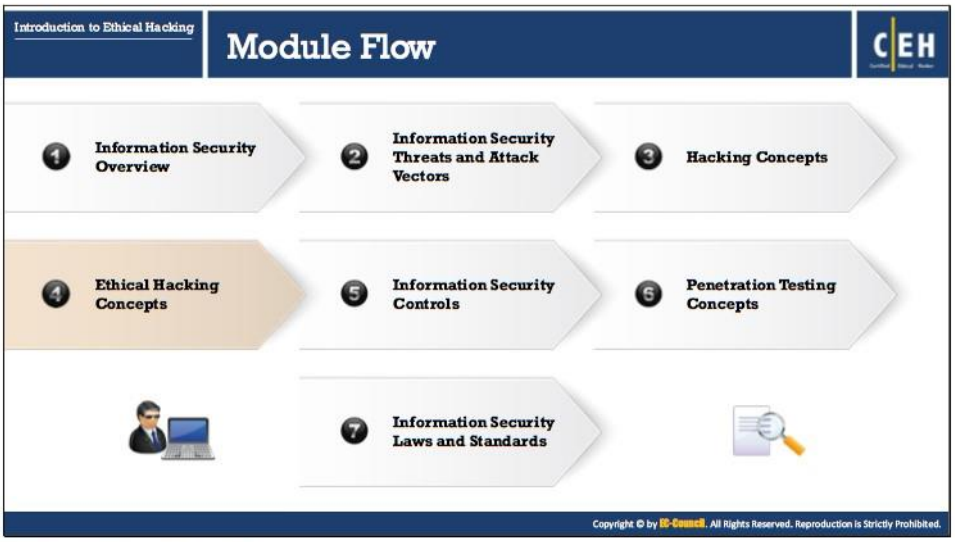
Attackers who choose to remain undetected remove evidence of their entry and install a backdoor or a Trojan to gain repeat access. They can also install rootkits at the kernel level to gain full administrative access to the target computer. Rootkits gain access at the operating system level, while a Trojan horse gains access at the application level. Both rootkits and Trojans require users to install them locally. In Windows systems, most Trojans install themselves as a service and run as local system, with administrative access.

Attackers can upload, download, or manipulate data, applications, and configurations on the owned system and can also use Trojans to transfer user names, passwords, and any other information stored on the system. They can maintain control over the system for a long time by closing up vulnerabilities to prevent other hackers from taking control from them, and sometimes, in the process, render some degree of protection to the system from other attacks. Attackers use the compromised system to launch further attacks.

Hacking Phase: Clearing Tracks

For obvious reasons, such as avoiding legal trouble and maintaining access, attackers will usually attempt to erase all evidence of their actions. Clearing tracks refers to the activities carried out by an attacker to hide malicious acts. The attacker's intentions include continuing access to the victim's system, remaining unnoticed and uncaught, deleting evidence that might lead to his/her prosecution. They use utilities such as PsTools (*https://docs.microsoft.com*) tools or Netcat or Trojans to erase their footprints from the system's log files. Once the Trojans are in place, the attacker has most likely gained total control of the system and can execute scripts in the Trojan or rootkit to replace critical system and log files to hide their presence in the system. Attackers always cover their tracks to hide their identity.

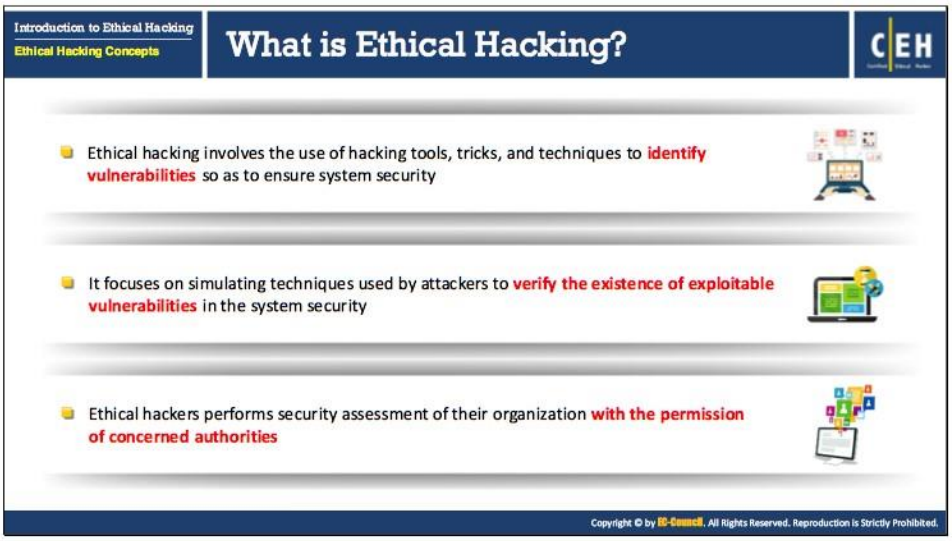
Other techniques include steganography and tunneling. Steganography is the process of hiding data in other data, for instance image and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Attackers can use even a small amount of extra space in the data packet's TCP and IP headers to hide information. An attacker can use the compromised system to launch new attacks against other systems or as a means of reaching another system on the network undetected. Thus, this phase of the attack can turn into another attack's reconnaissance phase. System administrators can deploy host-based IDS (intrusion detection systems) and antivirus software in order to detect Trojans and other seemingly compromised files and directories. As an ethical hacker, you must be aware of the tools and techniques that attackers deploy, so that you are able to advocate and implement countermeasures, detailed in subsequent modules.



Ethical Hacking Concepts

An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain access to a computer system are similar irrespective of the hacker's intensions.

This section provides an overview of ethical hacking, why ethical hacking is necessary, the scope and limitations of ethical hacking, and the skills of an ethical hacker.



What is Ethical Hacking?

Ethical hacking is the practice of employing computer and network skills in order to assist organizations in testing their network security for possible loopholes and vulnerabilities. White Hats (also known as security analysts or ethical hackers) are the individuals or experts who perform ethical hacking. Nowadays, most organizations (private companies, universities, government organizations, etc.) are hiring White Hats to assist them in enhancing their cyber security. They perform hacking in ethical ways, with the permission of the network/system owner and without the intention to cause harm. Ethical hackers report all vulnerabilities to the system and network owner for remediation, thereby increasing the security of an organization's information system. Ethical hacking involves the use of hacking tools, tricks, and techniques typically used by an attacker, to verify the existence of exploitable vulnerabilities in the system security.

Today, the term hacking is closely associated with illegal and unethical activities. There is continuing debate as to whether hacking can be ethical or not, given the fact that unauthorized access to any system is a crime. Consider the following definitions:

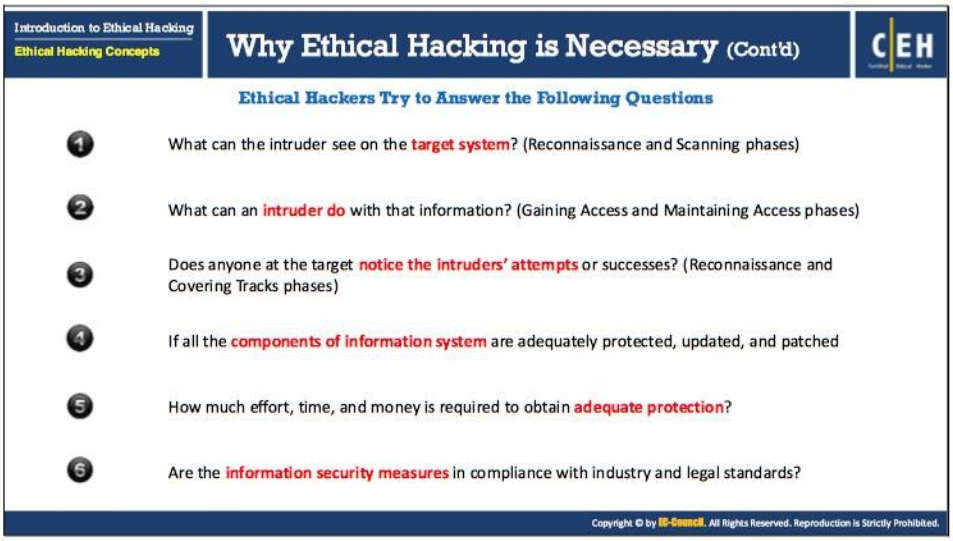
- The noun "hacker" refers to a person who enjoys learning the details of computer systems and stretching his or her capabilities.
- The verb "to hack" describes the rapid development of new programs or the reverse engineering of existing software to make it better or more efficient in new and innovative ways.
- The terms "cracker" and "attacker" refer to persons who employ their hacking skills for offensive purposes.

- The term "ethical hacker" refers to security professionals who employ their hacking skills for defensive purposes.

Most companies use IT professionals to audit their systems for known vulnerabilities. Although this is a beneficial practice, crackers are usually more interested in using newer, lesser-known vulnerabilities, and so these by-the-numbers system audits do not suffice. A company needs someone who can think like a cracker, keep up with the newest vulnerabilities and exploits, and can recognize potential vulnerabilities where others cannot. This is the role of the ethical hacker.

Ethical hackers usually employ the same tools and techniques as hackers, with the important exception that they do not damage the system. They evaluate system security, update the administrators regarding any discovered vulnerabilities, and recommend procedures for patching those vulnerabilities.

The important distinction between ethical hackers and crackers is consent. Crackers are attempting to gain unauthorized access to systems, while ethical hackers are always completely open and transparent about what they are doing and how they are doing it. Ethical hacking is therefore always legal.



Why Ethical Hacking is Necessary

As technology is growing at a faster pace, so is the growth in the risks associated with it. 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. Ethical hacking helps to predict the various possible vulnerabilities well in advance and rectify them without incurring any kind of attack from outsiders. As hacking involves creative thinking, vulnerability testing and security

audits cannot ensure that the network is secure. To achieve security, organizations need to implement a "defense-in-depth" strategy by penetrating their networks to estimate vulnerabilities and expose them.

Reasons why organizations recruit ethical hackers

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

An ethical hacker's evaluation of a client's information system security seeks answers to three basic questions:

1. **What can an attacker see on the target system?**

   Normal security checks by system administrators will often overlook several vulnerabilities. An ethical hacker will have to think about what an attacker would see during the reconnaissance and scanning phases of an attack.

2. **What can an intruder do with that information?**

   The ethical hacker needs to discern the intent and purpose behind the attacks to determine appropriate countermeasures. During the gaining-access and maintaining-access phases of an attack, the ethical hacker needs to be one step ahead of the hacker in order to provide adequate protection.

3. **Are the attackers' attempts being noticed on the target systems?**

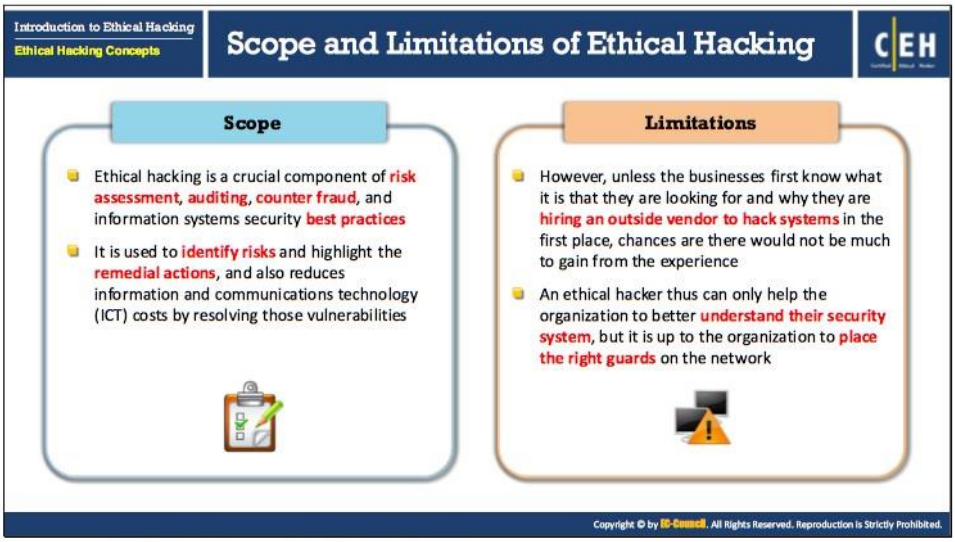
   Sometimes attackers will try for days, weeks, or even months to breach a system. Other times they will gain access, but will wait before doing anything damaging, instead take their time in assessing the potential use of exposed information. During the reconnaissance and covering tracks phases, the ethical hacker should notice and stop the attack.

After carrying out attacks, hackers may clear their tracks by modifying log files and creating backdoors, or by deploying Trojans. Ethical hackers need to investigate whether such activities have been recorded and what preventive measures have been taken. This not only provides them with an assessment of the attacker's proficiency, but also gives them insight into the existing security measures of the system being evaluated. The entire process of ethical hacking and subsequent patching of discovered vulnerabilities depends on questions such as:

- What is the organization trying to protect?
- Against whom or what are they trying to protect it?
- Are all the components of information system adequately protected, updated, and patched?

- How much time, effort, and money is the client willing to invest to gain adequate protection?
- Are the information security measures in compliance to industry and legal standards?

Sometimes, in order to save on resources or prevent further discovery, the client might decide to end the evaluation after the first vulnerability is found; therefore, it is important that the ethical hacker and the client work out a suitable framework for investigation beforehand. The client must be convinced of the importance of these security exercises through concise descriptions of what is happening and what is at stake. The ethical hacker must also remember to convey to the client that it is never possible to guard systems completely, but they can always be improved.



Scope and Limitations of Ethical Hacking

Security experts broadly categorize computer crimes into two categories: crimes facilitated by a computer and those in which the computer is the target.

Ethical hacking is a structured and organized security assessment, usually as part of a penetration test or security audit and 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, and also to reduce Information and Communications Technology (ICT) costs by resolving those vulnerabilities.

Ethical hackers determine the scope of the security assessment according to the client's security concerns. Many ethical hackers are members of a "Tiger Team." A tiger team works together to perform a full-scale test covering all aspects of the network, as well as physical and system intrusion.

An ethical hacker should know the penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or security audit should begin until a signed legal document giving the ethical hacker express permission to perform the hacking activities is received from the target organization. Ethical hackers need to be judicious with their hacking skills and recognize the consequences of misusing those skills.

The ethical hacker must follow certain rules to fulfill the ethical and moral obligations. An ethical hacker must do the following:

- Gain authorization from the client and have a signed contract giving the tester permission to perform the test.
- Maintain confidentiality when performing the test and follow a Nondisclosure Agreement (NDA) with the client for the confidential information disclosed during the

test. The information gathered might contain sensitive information and the ethical hacker must not disclose any information about the test or the confidential company data to a third party.

- Perform the test up to but not beyond the agreed-upon limits. For example, ethical hackers should perform DoS attacks only if they have previously been agreed upon with the client. Loss of revenue, goodwill, and worse could befall an organization whose servers or applications are unavailable to customers because of the testing.

The following steps provide a framework for performing a security audit of an organization, which will help in ensuring that the test is organized, efficient, and ethical:

- Talk to the client, and discuss the needs to be addressed during the testing.
- Prepare and sign NDA documents with the client.
- Organize an ethical hacking team, and prepare a schedule for testing.
- Conduct the test.
- Analyze the results of the testing, and prepare a report.
- Present the report findings to the client.

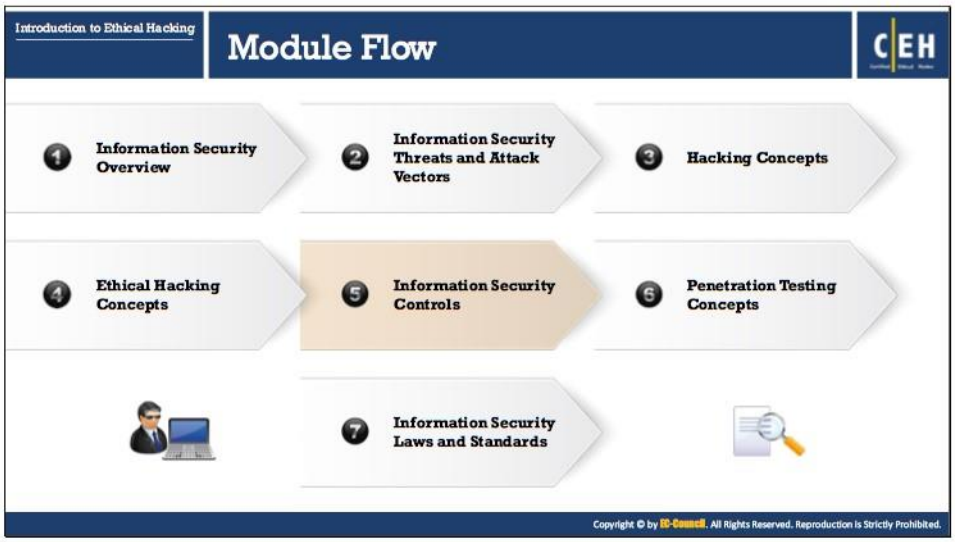
However, there are limitations too. Unless the businesses first know what they are looking for and why they are hiring an outside vendor to hack systems in the first place; chances are there would not be much to gain from the experience. An ethical hacker thus can only help the organization to better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

Skills of an Ethical Hacker

It is essential for an ethical hacker to acquire knowledge and skills to become an expert hacker and use this knowledge in a lawful manner. The technical and non-technical skills to be a good ethical hacker are discussed below:

- **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
  - Knowledge of security areas and related issues
  - High technical knowledge to launch the sophisticated attacks
- **Non-Technical Skills**

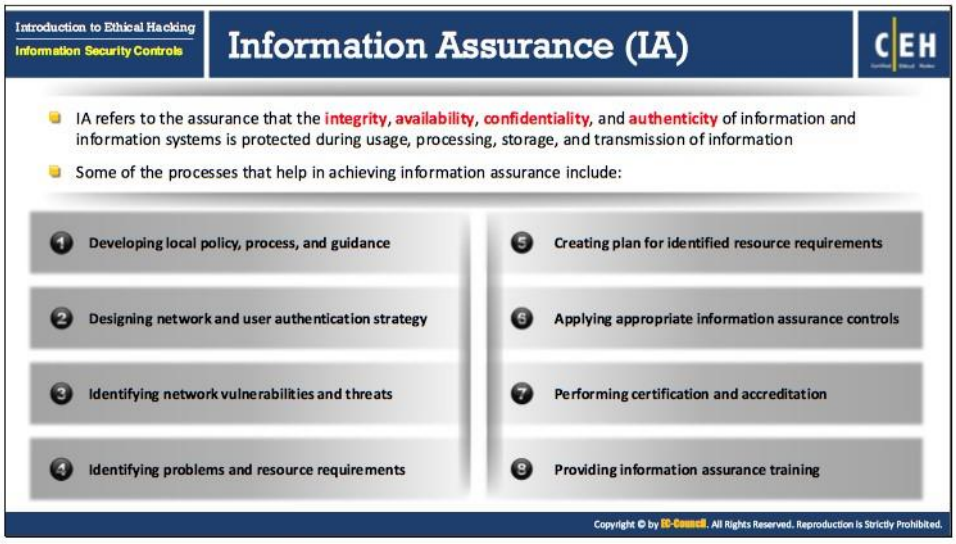
  Some of the non-technical characteristics of an ethical hacker include:
  - Ability to quickly learn and adapt new technologies
  - Strong work ethics and good problem solving and communication skills
  - Commitment to an organization's security policies
  - Awareness of local standards and laws



Information Security Controls

Information security controls prevent the occurrence of unwanted events and reduce risk to the organization's information assets. The basic security concepts critical to information on the Internet are confidentiality, integrity, and availability; those related to the persons accessing information are authentication, authorization, and non-repudiation. Information is the greatest asset to an organization, and it is a must to secure it by means of, for example, various policies, creating awareness, and employing security mechanisms.

This section deals with Information Assurance (IA), defense-in-depth, information security policies, physical security, risk management, threat modeling, incident management, access controls, Identity and Access Management (IAM), data loss prevention, data backup and recovery, and others.

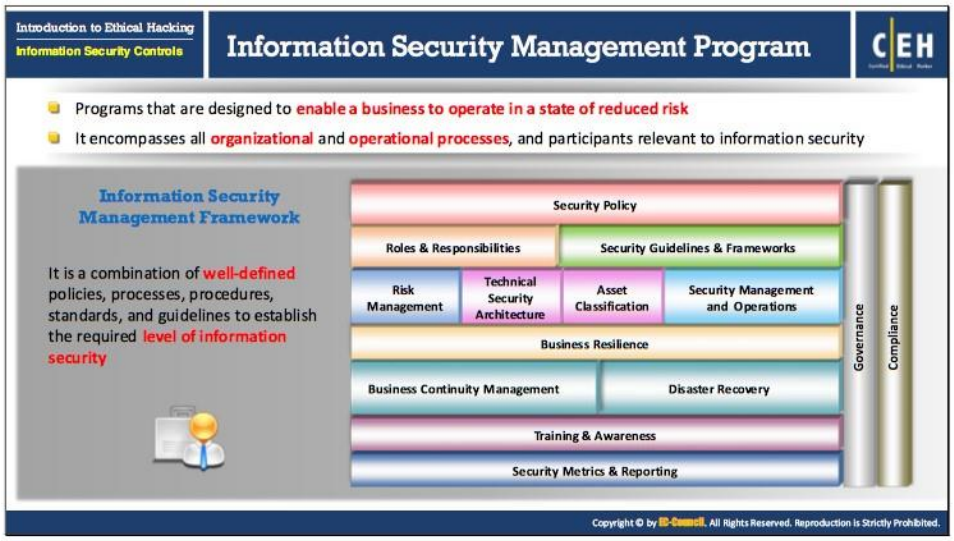


Information Assurance (IA)

IA refers to the assurance of the integrity, availability, confidentiality, and authenticity of information and information systems during usage, processing, storage, and transmission of information. Security experts accomplish the information assurance with the help of physical, technical, and administrative controls. Information Assurance and Information Risk Management (IRM) ensures that only authorized personnel access and use information. This helps in achieving information security and business continuity.

Some of the processes that help in achieving information assurance include:

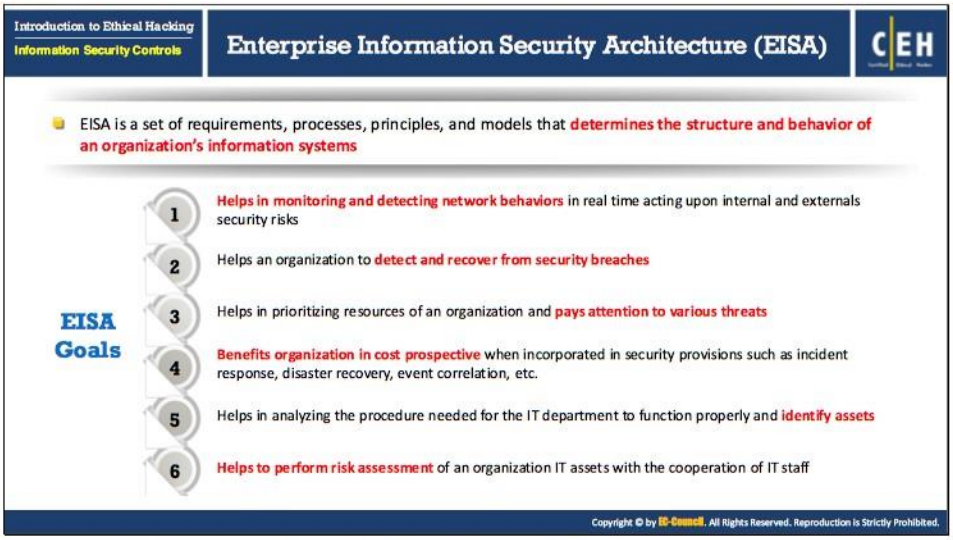
- Developing local policy, process, and guidance in such a way that the information systems are maintained at an optimum security level.
- Designing network and user authentication strategy — A secure network ensures the privacy of user records and other information on the network. Implementing an effective user authentication strategy secures the information systems data.
- Identifying network vulnerabilities and threats — Vulnerability assessments outline the security posture of the network. Performing vulnerability assessments in search of network vulnerabilities and threats help to take proper measures to overcome them.
- Identifying problems and resource requirements.
- Creating plan for identified resource requirements.
- Applying appropriate information assurance controls.
- Performing Certification and Accreditation (C&A) process of information systems helps to trace vulnerabilities, and implement safety measures to nullify them.
- Providing information assurance training to all personnel in federal and private organizations brings among them an awareness of information technology.



Information Security Management Program

Today's information security management programs encompass more than just firewalls and passwords. They are organization-wide programs that enable the business to operate in a state of reduced risk. Information security should be an ongoing process that—when fully developed—will position an organization to address the right security issues, so that the business can fulfill its objectives. The effective management of information security in an organization or enterprise encompasses all organizational and operational processes and participants relevant to information security.

The Information Security Management Framework is a combination of well-defined policies, processes, procedures, standards, and guidelines needed to establish the required level of information security.



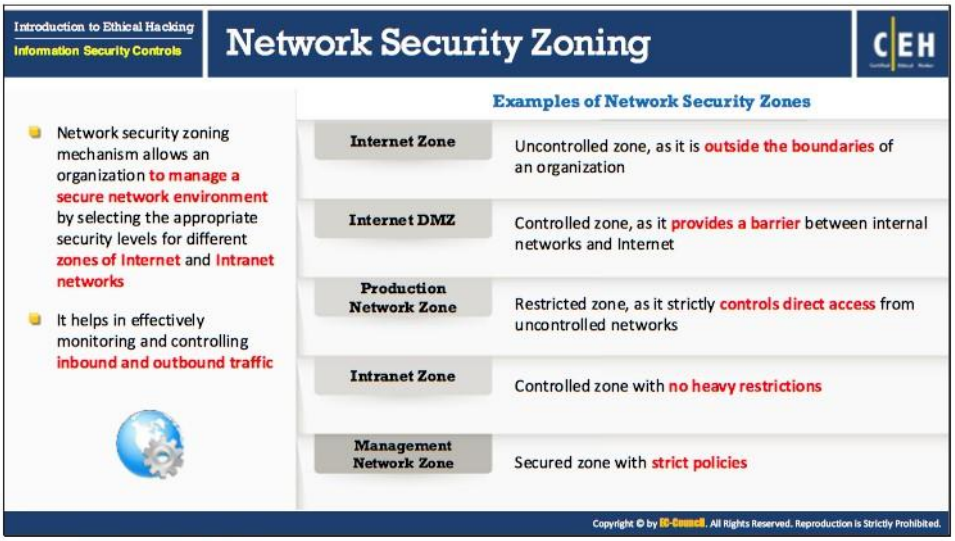
Enterprise Information Security Architecture (EISA)

EISA is a set of requirements, processes, principles, and models that determine the current and/or future structure and behavior of an organization's security processes, information security systems, personnel, and organizational sub-units. It ensures that the security architecture and controls are in alignment with the organization's core goals and strategic direction.

Though EISA deals with information security, it relates more broadly to the security practice of business optimization. Thus, it also addresses business security architecture, performance management and security process architecture. The main objective of implementing EISA is to make sure that IT security is in alignment with business strategy.

The following are the goals of EISA:

- To help in monitoring and detecting network behaviors in real time acting upon internal and externals security risks.
- To help an organization detect and recover from security breaches.
- To aid in prioritizing resources of an organization and pay attention to various threats.
- To benefit the organization in cost prospective when incorporated in security provisions such as incident response, disaster recovery, and event correlation, etc.
- To help in analyzing the procedures needed for the IT department to identify assets and function properly.
- To help perform risk assessment of an organization's IT assets with the cooperation of IT staff.



Network Security Zoning

A security zone is an area within a network that consists of a group of systems and other components with the same characteristics, all of which serve to manage a secure network environment. The network security zoning mechanism allows an organization to efficiently manage a secure network environment by selecting the appropriate level of security for different zones of Internet and intranet networks. It also enforces the organization's Internet security policies, according to the origin of the Web content and helps in effectively monitoring and controlling inbound and outbound traffic.

Properties of security zone:

- Active security policies that enforce rules on the traffic in transit (traffic that can pass through the firewall) and the action to be taken against it
- Pre-defined screening options that detect and block the malicious traffic
- Address book (IP addresses and address sets) to recognize members, so that policies can be applied
- List of interfaces in the zone

Examples of network security zones include:

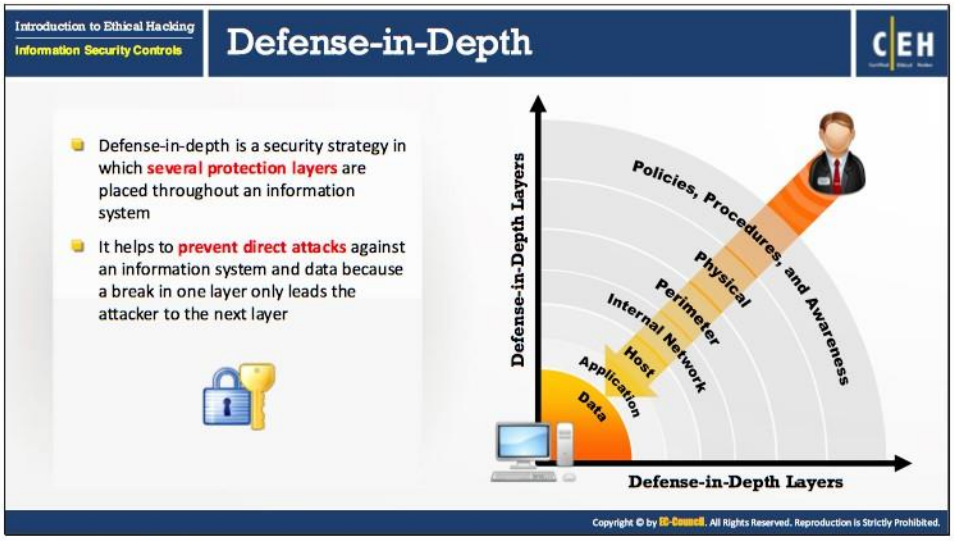
- **Internet Zone:** The Internet zone, also known as the untrusted zone, is the part of the Internet that is outside the boundaries of an organization. It is highly susceptible to security breaches, as there may be little or no security controls that can block an invasion.
- **Internet DMZ:** The Internet DMZ ("demilitarized zone"; also called a controlled zone) is a controlled, Internet-facing zone that typically contains Internet-facing components of

network web servers and email gateways through which employees of an organization directly communicate. It acts as a barrier between the organization's private network and its public network. The Internet DMZ uses a firewall at each of the two gateway faces, which enable the control of:

- Traffic entering the hosts in a DMZ from the Internet
- Traffic leaving from the hosts in a DMZ to the Internet
- Traffic entering the hosts in a DMZ from internal (private) networks
- Traffic leaving from the hosts in a DMZ to internal networks

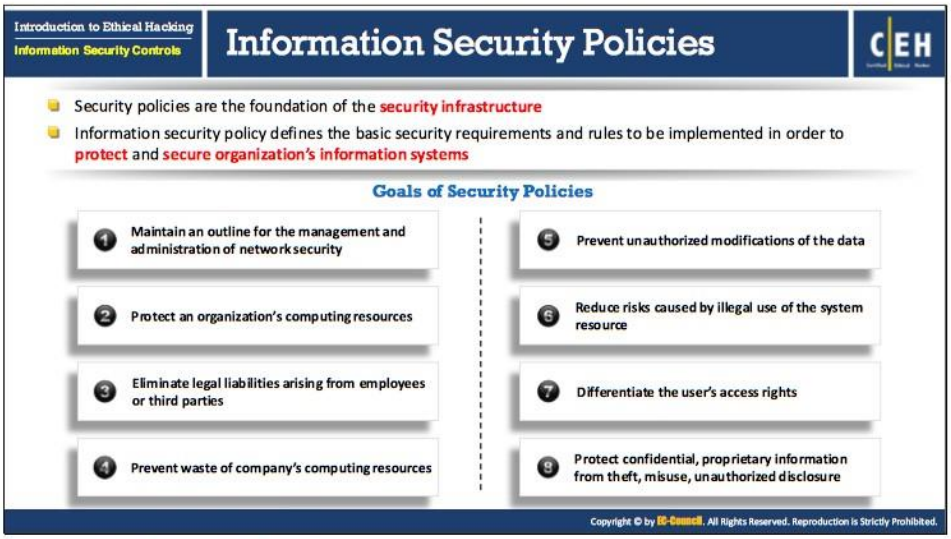
Security administrators may install access control software in the DMZ to monitor and control user access to resources stored in the restricted and other controlled zones.

- **Production Network Zone:** The production network zone, also known as a restricted zone, supports functions for which access should be limited. It strictly controls direct access from uncontrolled networks. Typically, a restricted zone employs one or more firewalls to filter inbound and outbound traffic.
- **Intranet Zone:** The intranet zone, also known as a controlled zone, contains a set of hosts in an organization's network located behind a single firewall or set of firewalls, and generally has less restriction. This zone is not heavily restricted in use, but it has an appropriate span of control set up to ensure that network traffic does not compromise the operation of significant business functions.
- **Management Network Zone or Secured Zone:** Access to this zone is limited to authorized users. Access to one area of the zone does not necessarily apply to another area of the zone. It is a secured zone with strict policies.



Defense-in-Depth

Defense-in-depth is a security strategy in which security professionals use several protection layers throughout an information system. This strategy uses the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier. Defense-in-depth helps to prevent direct attacks against an information system and its data because a break in one layer only leads the attacker to the next layer. If a hacker gains access to a system, defense-in-depth minimizes any adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent a recurrence of intrusion.



Information Security Policies

Security policies form the foundation of a 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. Without them, it is impossible to protect the company from possible lawsuits, lost revenue, and bad publicity, not to mention the basic security attacks. A security policy is a high-level document or set of documents that describes, in detail, the security controls to implement in order to protect the company. It maintains confidentiality, availability, integrity, and asset values.

A security policy also protects the company from threats such as unauthorized access, theft, fraud, vandalism, fire, natural disasters, technical failures, and accidental damage. In addition, it protects against cyber-attack, malicious threats, international criminal activity foreign intelligence activities, and terrorism.

Policies are not technology specific and accomplish three things:

- They reduce or eliminate legal liability of employees and third parties.
- They protect confidential and proprietary information from theft, misuse, unauthorized disclosure, or modification.
- They prevent wastage of the company's computing resources.

All security policies must be documented properly and they should focus on the security of all departments in an organization. Management should take into consideration the areas in which security is most important, and prioritize its actions accordingly, but it is very important to look into each department for possible security breaches and ways to protect against them.

The following information security systems in an organization might require more attention in terms of security:

- Encryption mechanisms
- Access control devices
- Authentication systems
- Firewalls
- Antivirus systems
- Web sites
- Gateways
- Routers and switches

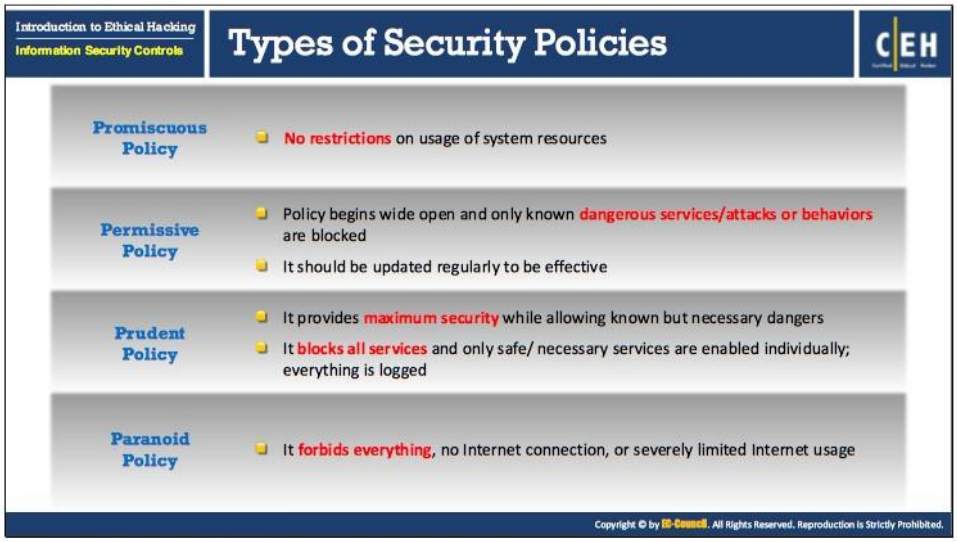
There are two types of security policies: technical security and administrative security policies. Technical security policies describe the configuration of the technology for convenient use; administrative security policies address how all persons should behave. All employees must agree to and sign both the policies.

In an organization the high-level management is responsible for the implementation of the organization's security policies. High-level officers involved in the implementation of the policies include the following:

- Director of Information Security
- Chief Security Officer

The following are the goals of security policies:

- To maintain an outline for the management and administration of network security
- To protect an organization's computing resources
- To eliminate legal liabilities arising from employees or third parties
- To prevent wastage of company's computing resources
- To prevent unauthorized modifications of the data
- To reduce risks caused by illegal use of the system resource
- To differentiate the user's access rights
- To protect confidential, proprietary information from theft, misuse, and unauthorized disclosure



Types of Security Policies

A security policy is a document that contains information about the way the company plans to protect its information assets from known and unknown threats. These policies help to maintain the confidentially, availability, and integrity of information. The four major types of security policy are as follows:

- **Promiscuous Policy**

  This policy does not impose any restrictions on the usage of system resources. For example, with a promiscuous Internet policy, there is no restriction on Internet access. A user can access any site, download any application, and access a computer or a network from a remote location. While this can be useful in corporate businesses where people who travel or work at branch offices need to access the organizational networks, many malware, virus, and Trojan threats are present on the Internet and due to free Internet access, this malware can come as attachments without the knowledge of the user. Network administrators must be extremely alert while choosing this type of policy.

- **Permissive Policy**

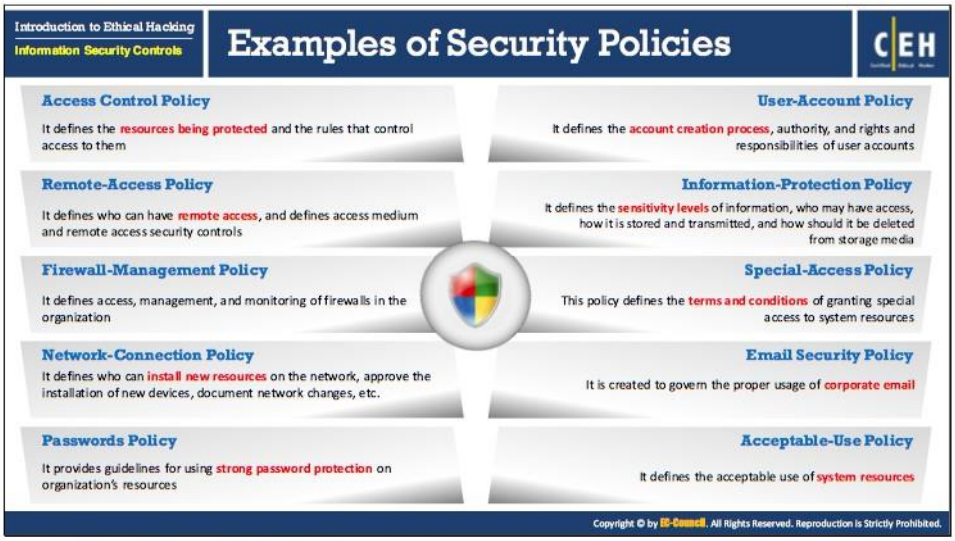
  Policy begins wide-open and only the known dangerous services/attacks or behaviors are blocked. For example, in a permissive Internet policy, the majority of Internet traffic is accepted, but several known dangerous services and attacks are blocked. Because only known attacks and exploits are blocked, it is impossible for administrators to keep up with current exploits. Administrators are always playing catch-up with new attacks and exploits. This policy should be updated regularly to be effective.

- **Prudent Policy**

  A prudent policy starts with all the services blocked. The administrator enables safe and necessary services individually. It logs everything, such as system and network activities. It provides maximum security while allowing only known but necessary dangers.

- **Paranoid Policy**

  A paranoid policy forbids everything. There is a strict restriction on all use of company computers, whether it is system usage or network usage. There is either no Internet connection or severely limited Internet usage. Due to these overly severe restrictions, users often try to find ways around them.

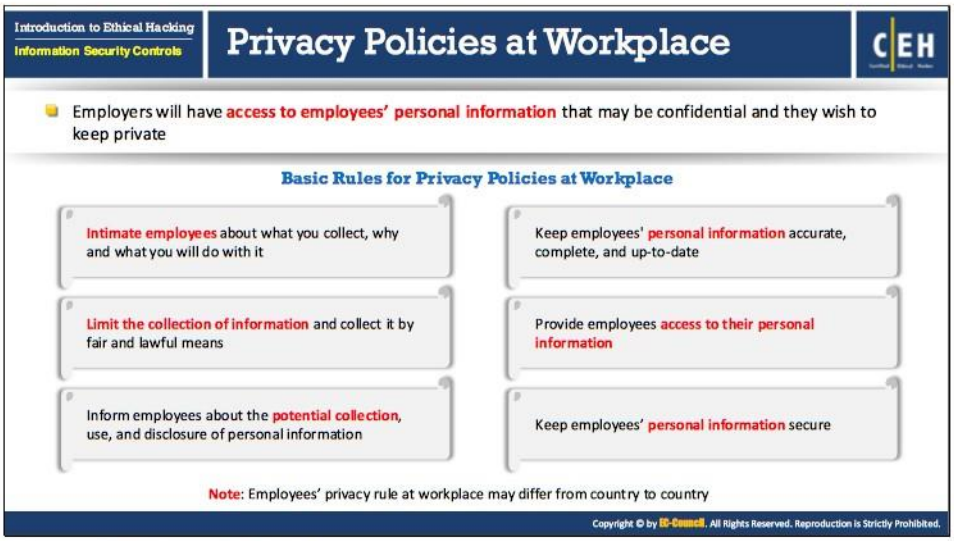


Examples of Security Policies

Given below are examples of security policies that organizations use worldwide to secure their assets and important resources.

- **Access Control Policy:** Access control policy outlines procedures that help in protecting the organizational resources and the rules that control access to them. It enables organizations to track their assets.
- **Remote-Access Policy:** A remote-access policy contains a set of rules that define authorized connections. It defines who can have remote access, the access medium and remote access security controls. This policy is necessary in larger organizations in which networks are geographically spread, and those in which employees work from home.
- **Firewall-Management Policy:** A firewall-management policy defines a standard to handle application traffic, such as Web or e-mail. This policy describes how to manage, monitor, protect, and update firewalls in the organization. It identifies network applications, vulnerabilities associated with applications, and creates an application-traffic matrix showing protection methods.
- **Network-Connection Policy:** A network-connection policy defines the set of rules for secure network connectivity, including standards for configuring and extending any part of the network, policies related to private networks, and detailed information about the devices attached to the network. It protects against unauthorized and unprotected connections that allow hackers to enter into the organization's network and affect data integrity and system integrity. It permits only authorized persons and devices to connect to the network and defines who can install new resources on the network, as well as approve the installation of new devices, and document network changes, etc.

- **Password Policy:** A password policy is a set of rules framed to increase system security by encouraging users to employ strong passwords to access an organization's resources and keep them secure.
- **User Account Policy:** User account policies provide guidelines to secure access to a system. It defines the account creation process, and authority, rights and responsibilities of user accounts. It outlines the requirements for accessing and maintaining the accounts on a system. This is especially important for large websites for which users have accounts on many systems. Users have to read and sign an account policy.
- **Information-Protection Policy:** Information-protection policies define the standards to reduce the danger of misuse, destruction, and loss of confidential information. It defines the sensitivity levels of information, who may have access, how it is stored and transmitted, and how it should be deleted from storage media. They give guidelines to process, store, and transfer confidential information.
- **Special-Access Policy:** A special-access policy determines the terms and conditions of granting special access to system resources. It defines a set of rules to create, utilize, monitor, control, remove, and update those accounts with special access privileges, such as those of technical support staff and security administrators.
- **Email Security Policy:** An email security policy governs the proper usage of the corporate email. For example, a company needs an email policy to protect against email threats (phishing attacks and confidential leaks), to stop any misconduct at the initial stage (asking employees to report when unknown or offensive emails are received), to minimize company liability for employees' action, to educate employees in email etiquette, and to warn employees of monitoring their emails.
- **Acceptable-Use Policy:** Acceptable-use policies consist of some rules decided by network and website owners. This type of policy defines the proper use of computing resources and states the responsibilities of users to protect the information available in their accounts.



Privacy Policies at Workplace

Nowadays, to ensure that employees are working efficiently, employers are making use of technology to log/monitor employees' activities at the workplace. Employers have access to employees' personal information, such as their phone number, address, bank account number, PAN number, which may be confidential or otherwise private. That way, employers are able to monitor web-browsing records, video surveillance, keystroke monitoring, and so on.

This could create some concern among employees for fear that their private information may be misused. And therefore, it is important to maintain a balance between employers' "need to know" policy and employees' "right to privacy", and employers need to follow some basic rules for privacy policies at work place:

- Before collecting an employee's information, the employer should give a prior intimation to the respective employee about the type of information required, its purpose, and its use.
- The employer must collect only the required information about an employee, and it should be obtained by fair and lawful means.
- The employer should inform the employee about the information collected and it should be used only for the intended and stated purpose, with the employee's prior consent.
- The employer has to keep employee's personal information accurate, complete, and up-to-date.
- The employer has to provide the employee an access to their personal information.
- The employer has to assure the security of employee's personal information.

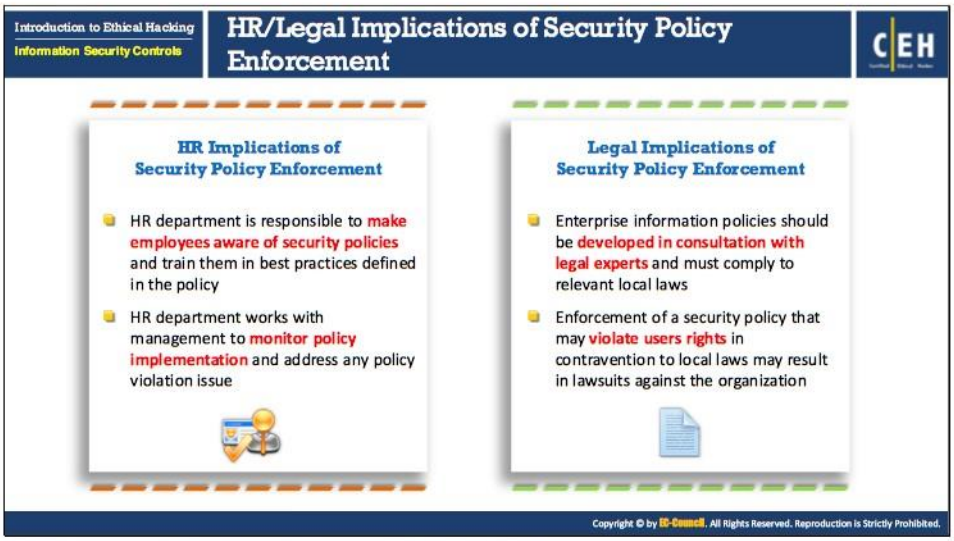
Note: Employee workplace privacy rules may differ from country to country.

Steps to Create and Implement Security Policies

Implementing security policies reduces the success rate and the risk of attacks. Thus, every company must have its own security policies, which are dependent on its business. In general, an organization's security policy development team consists of an Information Security Team (IST), Technical Writer(s), Technical Personnel, Legal Counsel, Human Resources, an Audit and Compliance Team, and User Groups.

To create and implement security policies an organization should:

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 the final version available to all the staff in the organization
6. Ensure that every member of the staff reads, understands and signs the policy
7. Deploy tools to enforce the policies
8. Train and educate employees about the policy
9. Regularly review and update



HR/Legal Implications of Security Policy Enforcement

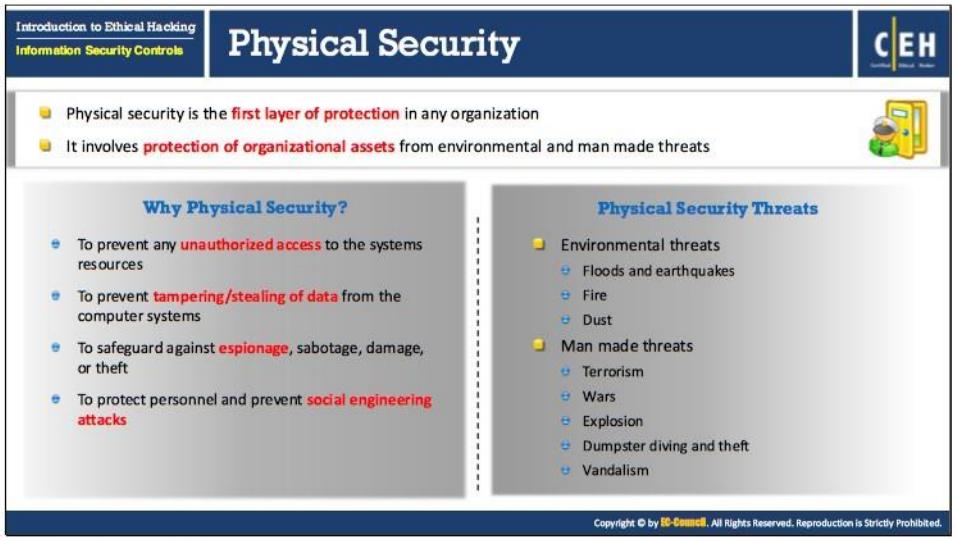
An organization's Human Resource (HR) department is responsible for making its employees aware of the company security policy and procedures, and train them in best practices defined in the policy, to protect the organization's infrastructure, clients, and the workforce. On the other hand, the HR department must work with the management to monitor policy implementation and address policy violation issues.

HR professionals must do the following to uphold the company's security policy:

- In the staff recruitment process, HR professionals must conduct background checks on prospective hires, with the consent of those individuals. In general, background checks include criminal history investigations and credit reports.
- The HR professional must implement a company code of conduct, which contains clear instructions for safeguarding sensitive information about the organization and its respective clients. All the employees working in the organization must have a copy of this report and ensure that all the new hires sign an agreement to abide by the code of conduct. Eventually, the organization should update the policy to contain the implementation of new processes or procedures.
- HR professionals must constantly interact with IT staff to ensure the encryption of all the sensitive files, ensure the proper use of security controls, help them learn to securely access data, and know the rules to follow in doing so.
- Unscrupulous employees may violate the security policies and share sensitive information with the employer's competitors. HR professionals must investigate for all such security violations and take the appropriate disciplinary action.

Legal implications of Security Policy Enforcement

Organizations should develop enterprise information policies in consultation with legal experts, and must comply with relevant local laws. Enforcement of a security policy that violates users' rights in contravention to local laws can result in lawsuits against the organization.



Physical Security

Physical security involves the protection of organizational assets from environmental and man-made threats. It is the first layer of protection in any organization and is described as the certain safety measures that deny unauthorized access to organizational assets, and protects personnel and property from damage or harm (e.g. espionage, theft, or terrorist attacks). It involves the use of multiple layers of interdependent systems, which include CCTV surveillance, security guards, protective barriers, locks, access control protocols, and so on.

Physical security helps to:

- **Prevent any unauthorized access to the system resources**: Physical security protects information from unauthorized users and implements controls so that the authorized users do not inadvertently or intentionally misuse or compromise the integrity and availability of the information.
- **Prevent tampering/stealing of data from the computer systems**: Insiders can use USB or other portable devices to steal information from a computer. Security administrators deploy monitoring tools that trigger an alarm if an insider connects an external device to any of the systems in the network.
- **Safeguard against espionage, sabotage, damage, or theft**: Companies deploy surveillance systems, CCTVs, alarm systems, security guards, etc. to monitor and safeguard the organization's assets. Security administrators also use an access card authentication system for server rooms, file areas, communication closets, off-site backups, phone rooms, IT equipment, and other areas to which only a limited number of people have access.

- **To protect personnel and prevent social engineering attacks**: Physical security personnel and internal employees need periodic physical security awareness training to protect themselves from social engineering attacks.

Physical security is perhaps the most overlooked aspect of security. Categories of physical security threats are:

- **Natural/Environmental Threats**

  This type of threat includes the results of naturally occurring events, including:

  - **Floods:** Administrators should conduct periodic inspections to check for water seepage, especially during times of heavy precipitation. They should also check water detectors periodically. Administrators should be aware of proper shutdown procedures, and must perform exercise drills regularly.
  - **Fire and Smoke:** Administrators should periodically check the proper placement and functioning of fire alarms and extinguishers. They should also install smoke detectors throughout the building(s). The designated smoking area should be as far as possible from computer systems.
  - **Earthquakes:** Even minor earthquakes may cause dust and debris to fall on computer equipment. Plastic sheets should be readily available in the system room. Covering computing assets in an emergency may mitigate the damage. Operators should properly cover magnetic tapes to prevent wear and tear.
  - **Dust:** Dust that naturally accumulates on hardware hinders its performance. Dust can seriously hinder a computer's ability to cool down. Even if the computer's case is closed, dust can still get in through drive openings. An effective way to remove dust from the inside of a CPU is to blow it away from the motherboard and other components using compressed air.

- **Man-made Threats**

  The biggest threat to the physical components of an organization and its network are from human errors, be they intentional or unintentional. For example, human error includes hitting the wrong button, and unplugging the wrong cord.

  Man-made threats include:

  - **Terrorism**

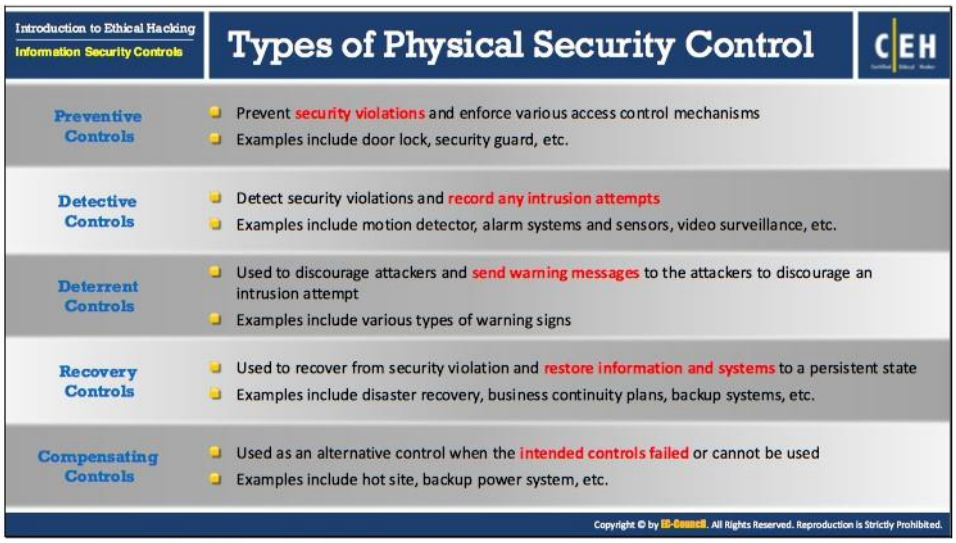
    Terrorist activities include the following:

    - Assassinations
    - Bombings
    - Random killings
    - Hijackings

  - **Wars:** Wherever they occur, wars destroy the major buildings, industries, and infrastructures and change the economic conditions of countries. Also, pollution can spread due to bombs and expelled gases.

- **Explosion:** To prevent explosions chemicals should be isolated and kept away from computers.
- **Dumpster diving and theft:** "Dumpster diving" involves searching the garbage of the targeted company in order to acquire important information. Attackers search for information such as phone numbers, credit card numbers, and other information commonly thrown away in dustbins. Attackers can also use discarded storage media such as floppy disks, CDs, and tapes to obtain important information.

  Lack of proper security may result in equipment theft. A guard on the premises can help prevent this.
- **Vandalism:** Disgruntled or former employees may try to compromise the system. In addition, in a case in which a disaster causes panic, the system might be mishandled.



Types of Physical Security Control

The physical security controls are categorized based on their functionality and the plane of application. Based on their functionality, the types of security control include:

- **Preventive Controls**

  These controls prevent security violations and enforce various access control mechanisms. Preventive controls may be physical, administrative, or technical. Examples include door lock, security guard, etc.

- **Detective Controls**

  These controls detect security violations, and record any intrusion attempts. These controls act when preventive controls fail. Examples include motion detector, alarm systems and sensors, video surveillance, etc.

- **Deterrent Controls**

  These controls may not prevent access directly. They are used to discourage attackers and send warning messages to the attackers to discourage an intrusion attempt. Examples include various types of warning signs.

- **Recovery Controls**

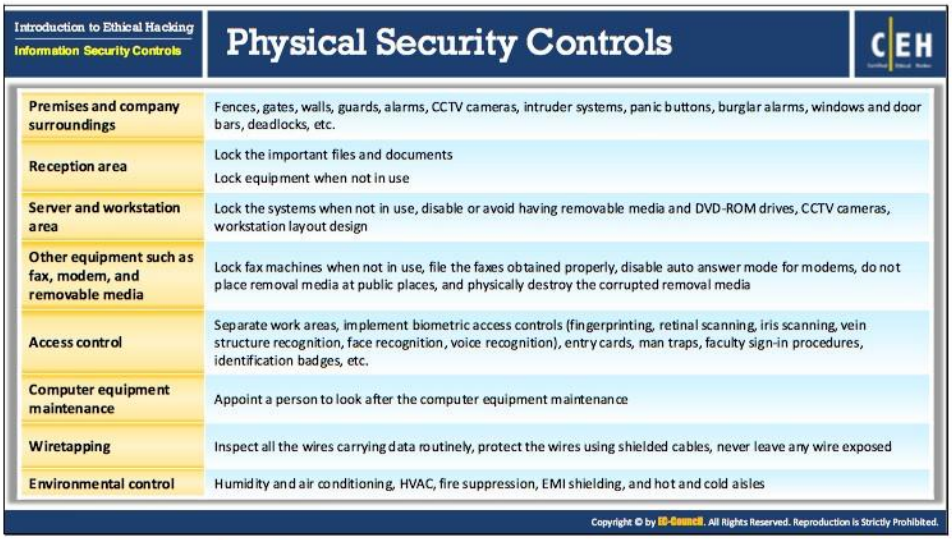
  These controls are used in a more serious condition to recover from security violation and restore information and systems to a persistent state. Examples include disaster recovery, business continuity plans, backup systems, etc.

- **Compensating Controls**

  These controls are used as an alternative control when the intended controls fail or cannot be used. They do not prevent any attack attempt but try to restore using other means like restoring from backup. Examples include hot site, backup power system, etc.

Based on the plane, types of security control include:

- Physical security controls such as doors, secure facilities, fire extinguishers, flood protection, etc.
- Administrative security controls such as organization's policies, procedures and guidelines to provide information security
- Technical security controls such as IDS/IPS, firewall, authentication systems, etc.



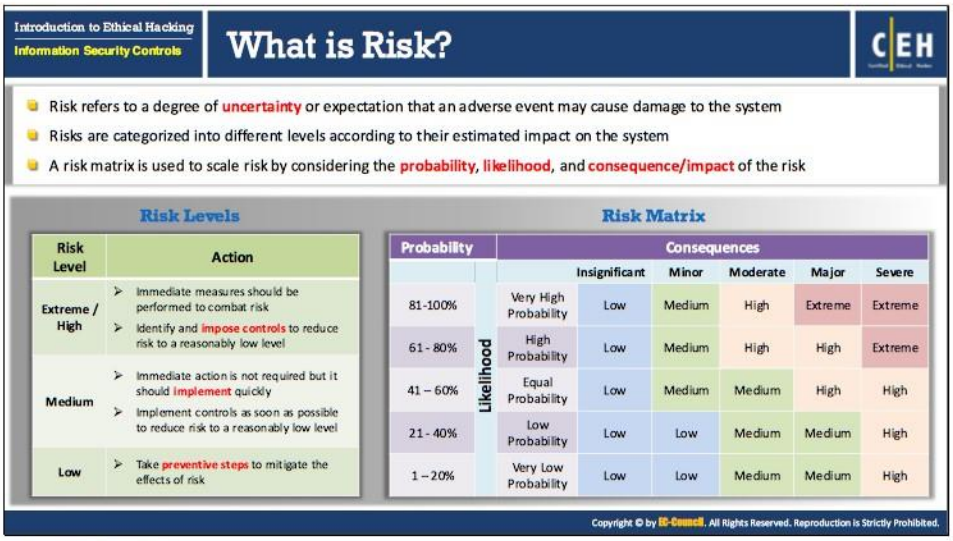
Physical Security Controls

Threat is any event that can cause damage to an asset. The purpose of physical security control is to ensure the confidentiality, integrity, and availability of assets, including the safety of all personnel.

Listed below are some of the physical security control measures:

- **Premises and company surroundings:** Use 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, and 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, mantraps, 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, and never leave any wire exposed.
- **Environmental control:** Keep check on humidity and air conditioning, HVAC, fire suppression, EMI shielding, as well as hot and cold aisles.



What is Risk?

Risk refers to a degree of uncertainty or expectation of potential damage that an adverse event may cause to the system or resources, under specified conditions. Alternatively, risk can also be defined as:

- A probability of the occurrence of a threat or an event that may damage, or cause loss or have other negative impact either from internal or external liabilities.
- A possibility of a threat, acting upon an internal or external vulnerability and causing harm to a resource.
- The product of the likelihood that an event would occur and the impact that event would have on an information technology asset.

The relation between Risk, Threats, Vulnerabilities and Impact is as follows:

RISK = Threats x Vulnerabilities x Impact

The impact of an event on an information asset is the product of vulnerability in the asset and the asset's value to its stakeholders. IT risk can be expanded to

RISK = Threat × Vulnerability × Asset Value

In fact, risk is the combination of the following two factors:

- Probability of the occurrence of an adverse event
- Consequence of the adverse event.

Risk Level

The risk level is an assessment of the resulted impact on the network. Various methods exist to differentiate risk levels depending on the risk frequency and severity. One of the common methods used to classify risks is to develop a two-dimensional matrix.

To analyze risks, you need to work out the frequency or probability of an incident happening (likelihood) and the consequences it would have. This is referred to as the level of risk. Risk can be represented and calculated using the following formula:

Level of Risk = Consequence x Likelihood

Risks are categorized into different levels according to their estimated impact on the system. Majorly, there are four risk levels, which include extreme, high, medium and low levels. Remember that control measures decrease the level of risk, but do not always eliminate them.

Risk Level	Consequence	Action
Extreme / High	Serious or Imminent danger	➢ Immediate measures should be performed to combat risk ➢ Controls should be identified and imposed to reduce risk to a reasonably low level
Medium	Moderate danger	➢ Immediate action is not required but it should implement quickly ➢ Controls should be implemented as soon as possible to reduce risk to a reasonably low level
Low	Negligible danger	➢ Take preventive steps to mitigate the effects of risk

TABLE 1.1: Risk Levels

Risk Matrix

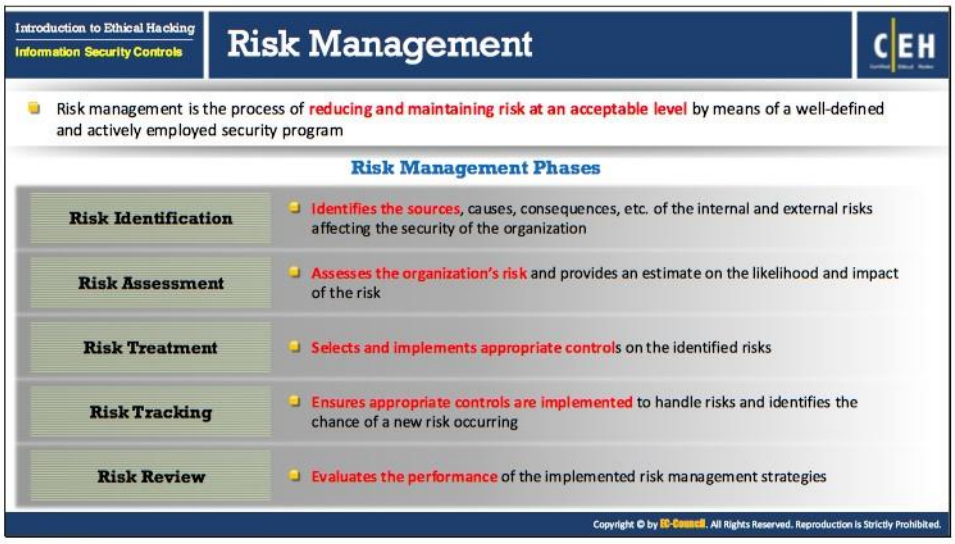
The risk matrix scales the risk occurrence/likelihood probability along with its consequences or impact. It is the graphical representation of risk severity and the extent to which the controls can/will mitigate it. The Risk matrix is one of the simplest processes to use for increased visibility of risk and contributes to the management's decision-making capability. The risk matrix defines various levels of risk and categorizes them as the product of negative probability and negative severity categories. Although there are many standard risk matrices, individual organizations need to create their own.

Probability	Likelihood	Consequences				
		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

TABLE 1.2: Risk Matrix

The above table is the graphical representation of the risk matrix, which is displayed for visualizing the risk and comparing risks. It is a simple way for analyzing risks and differentiates the two levels of risk.

- Likelihood: The chance of the risk occurring
- Consequence: The severity of the risk event that occurred



Risk Management

Risk management is the process of identifying, assessing, response and implementing the activities, which control how the organization manages the potential effects. It has a prominent place throughout the security life cycle and is a continuous and ever-increasing complex process. The types of risks vary from organization to organization but preparing a risk management plan will be common between all organizations.

Risk Management Objectives:

- To identify the potential risks is the main objective of risk management.
- To identify the impact of risks and help the organization develop better risk management strategies and plans.
- To prioritize the risks, depending on the impact/severity of the risk, and use established risk management methods, tools and techniques to assist.
- To understand and analyze the risks and report identified risk events.
- To control the risk and mitigate the risk effect.
- To create awareness among the security staff, develop strategies and plans for risk management strategies that last.

Risk management is a continuous process performed by achieving goals at every phase. It helps reduce and maintain risk at an acceptable level utilizing a well-defined and actively employed security program. This process is applied in all stages of the organization, i.e., strategic and operational contexts, to specific network locations.

The four key steps commonly termed as risk management phases are:

- Risk Identification
- Risk Assessment
- Risk Treatment
- Risk Tracking and Review

Every organization should follow the above steps while performing the risk management process.

- **Risk Identification**

  It is the initial step of the risk management plan. The main aim is to identify the risks - sources, causes, consequences, etc. of the internal and external risks affecting the security of the organization before they cause harm to the organization. The risk identification process depends on the skill set of the people and it differs from one organization to the other.

- **Risk Assessment**

  This phase assesses the organization's risks and estimates the likelihood and impact of those risks. Risk assessment is an ongoing iterative process and assigns priorities for risk mitigation and implementation plans, which help to determine the quantitative and qualitative value of risk. Every organization should adopt a risk evaluation process in order to detect, prioritize, and remove risks.

  Risk assessment determines the kind of risks present, the likelihood and severity of risk, as well as the priorities and plans for risk control. Organizations perform a risk assessment when they identify a hazard, but are not able to control it immediately. After performing a risk assessment, an update of all information facilities is needed at regular intervals.

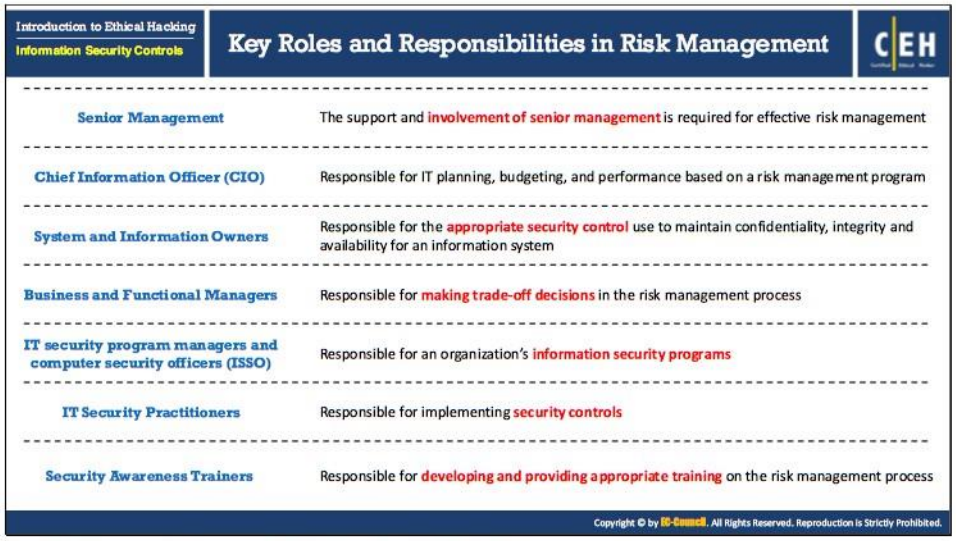
- **Risk Treatment**

  Risk treatment is the process of selecting and implementing appropriate controls on the identified risks in order to modify them. The risk treatment method addresses and treats the risks, according to their severity level. Decisions made in this phase are based on the results of a risk assessment. The purpose of this step is to identify treatments for the risks that fall outside the department's risk tolerance and provide an understanding of the level of risk with controls and treatments. It identifies the priority order in which individual risks should be treated, monitored and reviewed. Before treating the risk, you need to gather information about:

  - The appropriate method of treatment
  - People responsible for treatment
  - Costs involved
  - Benefits of treatment
  - Likelihood of success
  - Ways to measure and assess the treatment

- **Risk Tracking and Review**

  An effective risk management plan requires a tracking and review structure to ensure effective identification and assessment of the risks as well as the use of appropriate controls and responses. The tracking and review process should determine the measures adopted, the procedures adopted, and ensure that information gathered for undertaking the assessment was appropriate. The review phase evaluates the performance of the implemented risk management strategies. Performing regular inspections of policies and standards, as well as reviewing them regularly helps to identify the opportunities for improvement. Further, the monitoring process assures there are appropriate controls in place for the organization's activities and that the procedures are understood and followed.



Key Roles and Responsibilities in Risk Management

Risk management team member roles and responsibilities are:

- **Senior Management**

  The support and involvement of senior management is required for effective risk management. It is the responsibility of the senior management to supervise the risk management plans carried out in an organization. They develop policies and techniques required to handle the commonly occurring risks. Senior managers, through their expertise can design the steps required for handling future risk.

- **Chief Information Officer (CIO)**

  The person entitled with the position "Chief Information Officer" is responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization. The main responsibility of a CIO is to train employees and other executive management regarding the possible risks in IT and its effect on business. The officer is also responsible for IT planning, budgeting, and performance based on a risk management program and plays a vital role in the formation of basic plans and policies for risk management.

- **System and Information Owners**

  System and information owners mainly monitor the plans and policies developed for information systems. They are responsible for the appropriate security control used to maintain confidentiality, integrity and availability for an information system. Their responsibilities would be to:

  - Take part in all discussions regarding the configuration management process.

- Keep a record of the information system's components.
- Conduct an investigation on all the changes in the information systems and its impact.
- Prepare a security status report for all information systems.
- Update the security controls required for protecting the information systems.
- Update the security related documents on a regular basis.
- Examine and evaluate the existing security controls in order to confirm their efficiency in protecting the system.

- **Business and Functional Managers**

  They are responsible for maintaining all management processes in an organization and making trade-off decisions in the risk management process. They are empowered with an authority to manage almost all the processes in an organization. The roles defining functional managers are:

  - Development Team Manager
  - Sales Manager
  - Accounts Receivable Manager
  - Customer Service Manager

- **IT Security Program Managers and Computer Security Officers (ISSO)**

  ISSOs are responsible for an organization's information security programs. An ISSO provides the required support to the information system owners with the selection of the security controls for protecting the system. They also play an important role in the selection and the amendment of the security controls in an organization.

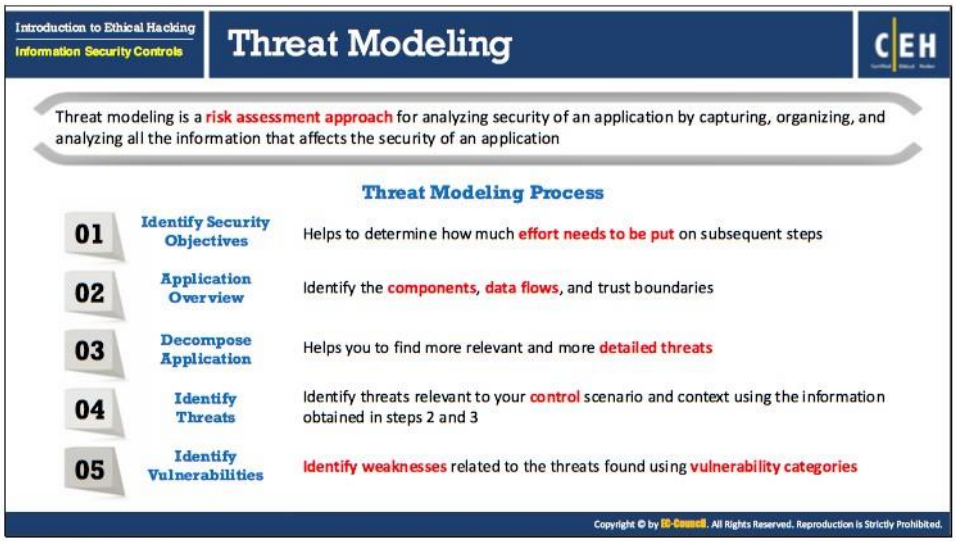
- **IT Security Practitioners**

  The IT security practitioners protect the personnel, the physical and information security in an organization. They are responsible for implementing security controls. The main responsibilities include:

  - Framing better security methods in the organization.
  - Developing methods that fulfill the company's standards.
  - Examining the company's security approach to risk management and business planning.
  - Handling and recording security incidents.
  - Assigning roles and responsibilities for security in an organization.
  - Supervising the overall security measures taken in an organization.

- **Security Awareness Trainers**

  Security awareness trainers are responsible for developing and providing appropriate training programs on the risk management process and IT security awareness in an organization. People responsible for this role will be subject matter experts and validate that only proper content is included in the program.



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. The threat model consists of three major building blocks: understanding the adversary's view, characterizing the security of the system, and determining threats. Every application should have a threat model developed and documented, and should be revisited as the application evolves and development progresses.

Threat modeling helps to:

- Identify relevant threats to a particular application scenario
- Identify key vulnerabilities in application design
- Improve security design

When using this approach, an administrator should keep the following in mind:

- Try not to be rigid on specific steps or implementations; focus on the approach. If any step becomes impassable, go right to threat modeling process step 4 and identify the problem.
- Use scenarios to scope the modeling activity.
- Use existing design documents. Make use of items like documented use cases, or use stories, architecture diagrams, data flow diagrams, or other design documentation.
- Start with a whiteboard before capturing information in documents or getting lost in details. It may be helpful to use a digital camera with printing capabilities to document and distribute the information from the whiteboard.

- Use an iterative approach. Add more details and improve the threat model as the design and development continue. This will help to become familiar with the modeling process and develop the threat model to better examine more possible scenarios.
- Obtain input about host and network constraints from system and network administrators. To better understand the end-to-end deployment diagram, obtain as much as information as possible about host configurations, firewall policies, allowed protocols and ports, and so on.

The threat modeling process involves five steps:

1. **Identify Security Objectives**

   Security objectives are the goals and constraints related to the application's confidentiality, integrity, and availability. Security-specific objectives guide the threat modeling efforts and helps to determine how much effort need to put on subsequent steps. To identify security objectives, administrators should ask the following questions:

   - What data should be protected?
   - Are there any compliance requirements?
   - Are there specific quality-of-service requirements?
   - Are there intangible assets to protect?

2. **Application Overview**

   Identify the components, data flows, and trust boundaries. To draw the end-to-end deployment scenario, the administrator should use a whiteboard. First, he/she should draw a rough diagram that explains the working and structure of the application, its subsystems, and its deployment characteristics. The deployment diagram should contain the following:

   - End-to-end deployment topology
   - Logical layers
   - Key components
   - Key services
   - Communication ports and protocols
   - Identities
   - External dependencies

   Identify Roles

   The administrator should identify people and the roles they can perform within the application, as well as what users can do. For example, are there higher-privileged groups of users? Who can read data? Who can update data? Who can delete data?

Identify Key Usage Scenarios

The administrator should use the application's use cases to determine the application's objective. Use cases explain how the application is used and misused.

Identify Technologies

The administrator should list the technologies and key features of the software, as well as the following technologies in use:

- Operating systems
- Web server software
- Database server software
- Technologies for presentation, business, and data access layers
- Development languages

Identifying these technologies helps to focus on technology-specific threats.

Identify Application Security Mechanisms

The administrator should identify some key points regarding the following:

- Input and data validation
- Authorization and authentication
- Sensitive data
- Configuration management
- Session management
- Parameter manipulation
- Cryptography
- Exception management
- Auditing and logging

The aim of these efforts is to identify relevant details and be able to add details where required, or to identify areas in which more research is required.

3. **Decompose Application**

In this step, the administrator breaks down the application to identify trust boundaries, data flows, entry points, and exit points. This makes it considerably easier to find more relevant and more detailed threats and vulnerabilities.

Identify trust boundaries

Identifying the application's trust boundaries helps the administrator focus on the relevant areas of the application. It indicates where trust levels change.

- Identify outer system boundaries

- Identify access control points, or key places where access requires extra privileges or role membership
- Identify trust boundaries from a data flow perspective

Identify Data Flows

The administrator should list the application's data input from entry to exit. This helps her/him understand how the application communicates with outside systems and clients, and how the internal components interact. He/she should pay particular attention to the data flow across the trust boundaries and data validation at the trust boundary entry point. A good approach is to start at the highest level and then deconstruct the application by testing the data flow between different subsystems.

Identify Entry Points

The application's entry point can also serve as an entry point for attacks. All users interact with the application at these entry points. Other internal entry points uncovered by subcomponents over the layers of the application may be present only to support internal communication with other components. The administrator should identify these entry points to determine the methods used by an intruder to get in through them. He/she should focus on the entry points that allow access to critical functionalities and provide adequate defense for them.

Identify Exit Points

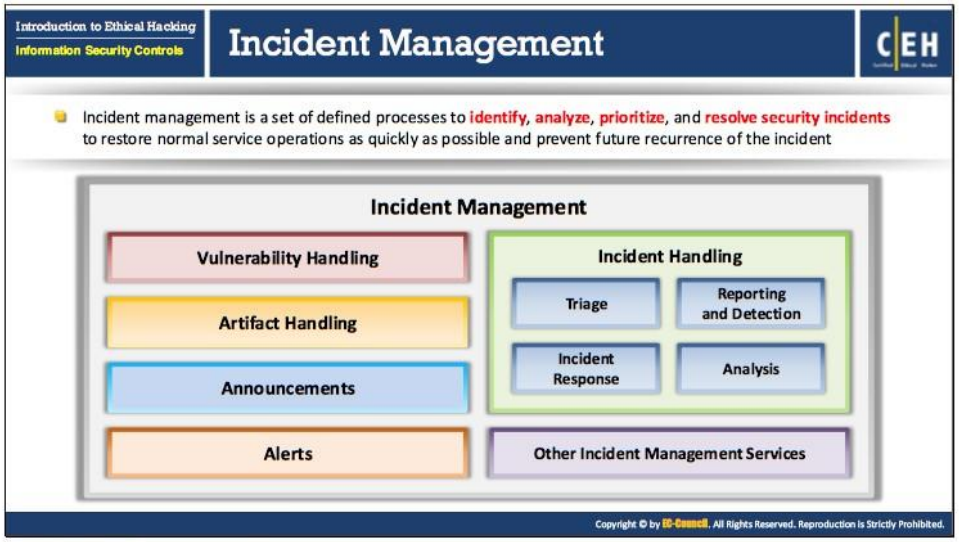
The administrator should also identify the points where the application transfers data to the client or external systems. He/she should prioritize exit points at which the application writes data containing client input or data from untrusted sources, such as a shared database.

4. **Identify Threats**

   The administrator should identify threats relevant to the control scenario and context using the information obtained in application overview and decompose application steps. He/she should bring members of the development and test teams together to identify potential threats. The team should start with a list of common threats grouped by application vulnerability categories. This step uses a question-driven approach to help identify threats.

5. **Identify Vulnerabilities**

   Vulnerability is a weakness in an application (deployed in an information system) that allows an attacker to exploit it, thereby leading to security breaches. Security administrators should identify weaknesses related to the threats found using vulnerability categories as identifying vulnerabilities and fixing them beforehand keeps intruders away.



Incident Management

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible, and prevent further recurrence of the incident. It involves not only responding to incidents, but also triggering alerts to prevent potential risks and threats. Security administrator must identify software that is open to attacks before someone takes advantage of the vulnerabilities.

Incident management includes the following:

- Vulnerability analysis
- Artifact analysis
- Security awareness training
- Intrusion detection
- Public or technology monitoring

The purpose of the incident management process:

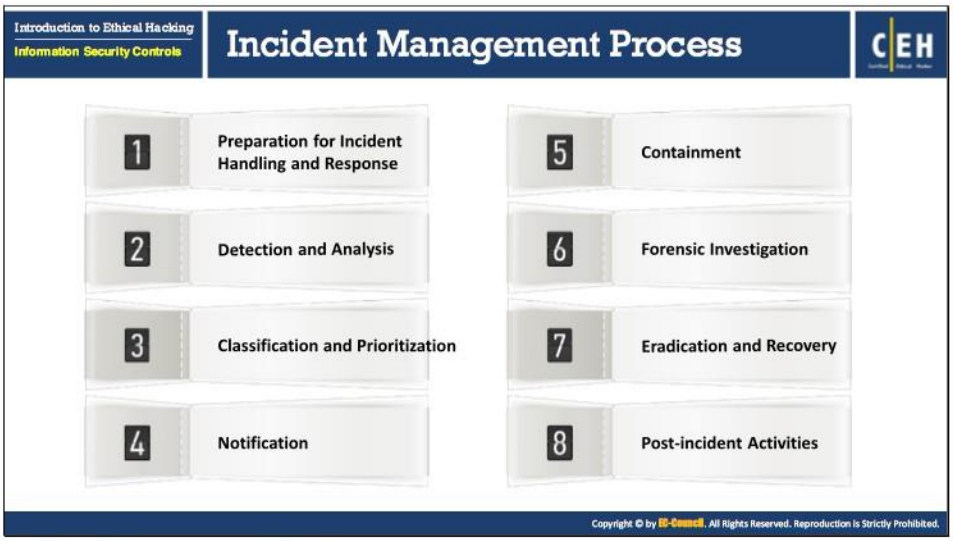
- Improves service quality
- Resolves problem proactively
- Reduces impact of incidents on business/organization
- Meets service availability requirements
- Increases staff efficiency and productivity
- Improves user/customer satisfaction
- Assists in handling future incidents

Conducting training sessions to spread awareness among users is an important part of incident management. They help end users better recognize suspicious events or incidents with ease, and be able to report an attacker's behavior to the appropriate authority.

The following people perform incident management activities:

- Human resources personnel can take steps to fire employees suspected in harmful computer activities.
- Legal counsel sets the rules and regulations in an organization. These rules can influence the internal security policies and practices of the organization in case an insider or an attacker uses the organization's system for harmful or malicious activities.
- The firewall manager keeps filters in place where denial-of-service attacks are made frequently.
- An outsourced service provider repairs system infected by viruses and malware.

Incident response is one of the functions performed in incident handling. Incident handling is one of the services provided as part of incident management. The diagram in the slide illustrates the relationship between incident response, incident handling, and incident management.



Incident Management Process

Incident management is the process of logging, recording, and resolving incidents that take place in the organization. The incident may occur due to fault, service degradation, error, and so on. The users, technical staff, and/or event monitoring tools identify the incidents. The main objective of the incident management process is to restore the service to a normal state as quickly as possible for customers, while maintaining availability and quality of service.

Steps involved in the incident management process:

- **Preparation for Incident Handling and Response**

  All the actions are pre-planned and detailed guidelines are provided to the employees at this step. Various policies and procedures are established to stay well equipped. Right people with appropriate skills are trained by providing tools to ensure effective response actions.

- **Detection and Analysis**

  In this step, security events are monitored and carefully analyzed using firewalls, intrusion detection and prevention systems, etc. Detection and analysis of incidents include identifying signatures of an incident, analyzing those signatures, recording the incident, prioritizing various incidents and alerting incidents.

- **Classification and Prioritization**

  Each incident is categorized and sub-categorized to troubleshoot the incident securely. It helps in saving a lot of time. Accurate categorization helps to allocate the management to the right team that has the appropriate knowledge and skills to handle the situation in real time. Moreover, depending on the impact of incident, events are

classified as a low, medium or high priority incident. Prioritization is done based on the severity, urgency, resource requirement, potential cost, etc.

- **Notification**

  After the incident has been identified and classified, suitable people and teams are notified about the problem. People having appropriate knowledge and training against the breach are employed to consider the situation and perform all the required actions at the right time. All the required people, including the third party, the CIO, Head of Information Security and Local Information Security Officer, etc. are provided with regular status updates.

- **Containment**

  Containment is a crucial step in the incident management process that focuses on preventing additional damage. It includes planning of strategies to avoid any further loss from taking place along with being assured that no forensic evidence is destructed or tempered related to the incident. Two important aspects need to be taken care of and they are:

  - Ensuring all the critical and essential computer resources are kept and protected at a safe place
  - Regular check on infected system is done to know their operational status.

- **Forensic Investigation**

  Forensic investigation is performed to find the root cause of the incident to know what exactly happened to the information system. The analysis of past records is performed using various forensic tools to detect the source of the attack and to capture the culprit. The whole process is well documented, as it is required in case of external threats for law enforcement. System logs, real-time memory, network device logs, application logs and all other supporting data are scanned and reviewed during investigation.

- **Eradication and Recovery**

  The eradication and recovery step is the process of recovering the system or network to its original state. This process is done only after the completion of all internal and external actions. The two important aspects of this step are cleanup and notification. Cleanup is performed using various antivirus softwares, uninstalling infected software, reloading the operating system, and also sometimes replacing the entire hard disk and rebuilding the network. All the professionals working with the incident response team are notified about the actions taken to recover the system or network.

- **Post-incident Activities**

  Once the process is complete, the security incident requires additional review and analysis before closing the process. Conducting the final review is an important step in the incident management process due to the following reasons:

  - It enhances public relations
  - It includes legal action

- It requires review by higher level management
- It needs to be documented for auditing purpose

This step includes post incident review and generating a post incident report. Security incident review includes preparing a set of questions on the incident and sending it to a group of end users, who have knowledge on it. This review helps to gather information about incident handling from various sources. Once the review is completed, the post incident report is automatically generated.

Responsibilities of an Incident Response Team

Cybercriminals use sophisticated attacking techniques to breach the security of an organization in order to steal or damage its critical assets. The loss incurred by the organization can lead to bankruptcy. The Incident Response Team (IRT) can help the organization prevent or mitigate such incidents. The IRT can include individuals, with varied skills and duties, who can perform different tasks.

Incident response team responsibilities include:

- Managing security issues by taking a proactive approach towards the customers' security vulnerabilities and by responding effectively to potential information security incidents.
- Developing or reviewing the processes and procedures that must be followed in response to an incident.
- Managing the response to an incident and ensuring that all procedures are followed correctly in order to minimize and control the damage.
- Identifying and analyzing what has happened during an incident, including the impact and threat.
- Providing a single point of contact for reporting security incidents and issues.
- Reviewing changes in legal and regulatory requirements to ensure that all processes and procedures are valid.
- Reviewing existing controls and recommending steps and technologies to prevent future security incidents.

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

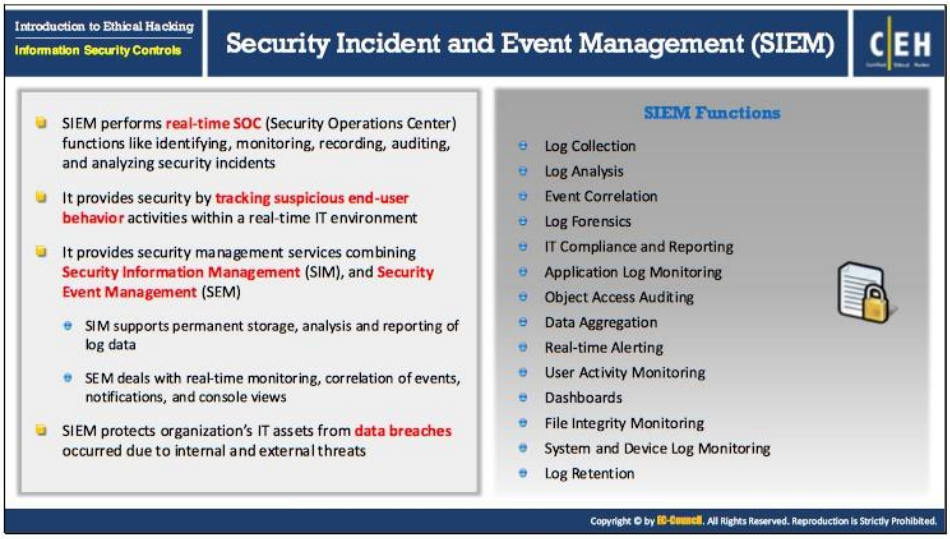
Incident Response Team Members: Roles and Responsibilities

- **Information Security Officer (ISO)**
  - Identifies the nature and scope of the computer security incident
  - Communicates with information security specialists as well as with other team members, and takes their advice, if required
  - Provides incident handling training to members
  - Examines the details of the investigation
  - Makes sure the evidence gathered, chain of custody, and evidence stored are correct
  - Prepares a report of the incident, and takes corrective action
- **Information Technology Officer**
  - Acts as the communication point for various computer security incidents
  - Notifies the information security officer to provide the IRT to carry out necessary operations
  - Ensures the incident management team and other activated teams are supported via available technology
- **Information Privacy Officer**
  - Coordinates activities with the information security officer
  - Prepares documentation for different types of data that may have been breached
  - Helps individuals in discussing investigation issues related to customer privacy and employee personal information
  - Provides guidance for creating communication among the affected agencies
  - Monitors the need for altering practices, privacy policies, and procedures, as a result of the security incident
- **Incident Manager (IM)**
  - Focuses on the incident and analyzes the manner in which to handle it from a management and technical point of view. He/she is responsible for the actions performed by the incident analysts, and reports the information to the incident coordinator. The Incident Manager must be a technical expert with an understanding of security and incident management.
- **Network Administrator**

- Examines the computer network traffic for signs of incidents or attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS), firewall breach, or other malicious code
- Uses tracer tools such as sniffers, transmission control protocol (TCP) port monitors, and event loggers to identify the incidents
- Contacts the ISP and seeks their assistance in handling incidents
- Performs the necessary actions required to block network traffic from the suspected intruder

- **System Administrator**
  - Examines and updates service packages and patches available on critical systems
  - Examines the backups for critical systems
  - Inspects system logs for unusual activity
- **Business Applications and Online Sales Officer**
  - Reviews business applications and services for signs of incident
  - Checks the audit logs of critical servers that are vulnerable to attacks
  - Gathers information related to the security incident, according to the request of the information security officer
- **Internal Auditor**
  - Checks whether the information systems are in compliance with security policies and controls
  - Performs an audit test to make sure that patches and service packs are current with mission-critical systems
  - Identifies and reports any security loopholes to the management for necessary actions
- **Incident Coordinator**
  - Acts as a link between various groups affected by the incidents, such as legal, human resources, different business areas, and management. He/she plays a vital role coordinating between the security teams and networking groups. The incident coordinator helps in the communication process and keeps everyone updated. The incident coordinator should possess communication, technical skills, and business understanding of the organization.
- **Incident Analyst**
  - These technical experts in their particular area apply the appropriate technology and try to eradicate and recover from the incident

- **Constituency**
  - The constituency is not part of the incident-response team itself, but rather a stakeholder in the incident. It includes different business areas and technical and management teams.
- **Administration**
  - The administration ensures that the offices start their operations as soon as possible after the occurrence of an incident. It assists in the development of an alternate site, if needed, and helps the staff in transportation and lodging aspect. The administration estimates the loss of property and communicates with insurers and third-party administrators. He/she prepares all paperwork needed to file a claim for insurance.
- **Human Resources**
  - Analyze the human aspects of the disaster and conducting a post-event counseling. He/she is responsible for tracking, recording, reporting, and compensating human resource for all billable hours, for performing duties throughout the event.
  - Keeps track of records of any injuries, along with the investigation results relating to the event.
- **Public Relations**
  - This department serves as a primary contact for the media and informs the media about an event. It updates the website information and monitors media coverage. Public relations also play a major role in communicating with stakeholders and other personnel, including the:
    - Board and foundation personnel
    - Donors
    - Grantees suppliers/vendors and media



Security Incident and Event Management (SIEM)

Today, organizations need to protect their IT assets from data breaches due to internal and external threats. To meet strict compliance requirements and for threat identification and mitigation, organizations need to audit the information that is flowing through their enterprise network. Security Incident and Event Management (SIEM) systems are used to manage and store huge collection of log data from different sources like networks, applications, devices, security, and user activity in real time. SIEM performs real time monitoring and detection of security events, forensic and post incident analysis, auditing, and IT Security and regulatory compliance reporting.

What is SIEM?

Security incident and event management (SIEM) is also known as security information and event management which performs real-time security operations center (SOC) functions like identifying, monitoring, recording, auditing and analyzing security incidents. It performs threat detection and security incident response activities. SIEM provides security by tracking suspicious end-user behavior activities within a real-time IT environment.

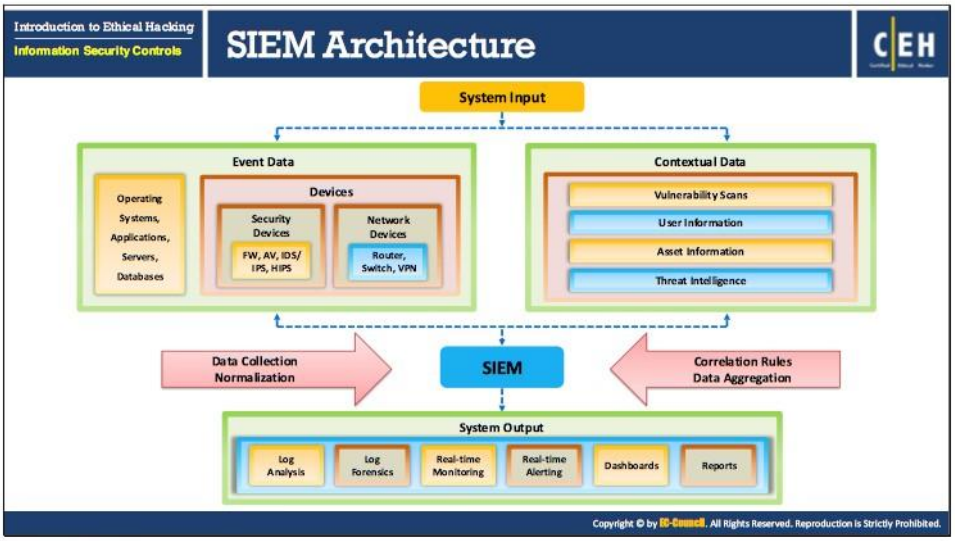
SIEM provides security management services combining Security Information Management (SIM) and Security Event Management (SEM). SIM supports permanent storage, analysis and reporting of log data. SEM deals with real-time monitoring, correlation of events, notifications and console views. SIEM protects organization's IT assets from data breaches occurred due to internal and external threats.

Function performed by SIEM

- **Log Collection:** SIM collects and logs data from different sources like networks, applications, devices, and user activity in real-time into a central repository for analysis and reporting.
- **Log Analysis:** SEM deals with real-time monitoring and analysis of security incidents. SIEM monitors all the security policies, mechanisms (confidentiality, authentication, authorization etc.), devices and applications (IDS/IPS, firewall, etc.) in real-time and detects malicious activities and alerts about security relevant events.
- **Event Correlation:** SIEM performs real-time event correlation and alerts analysts and administrators to secure enterprise network from internal and external threats. SIEM uses rules to correlate events within a time period to understand interrelations between the events and alerts for intrusions and insider threats.
- **Log Forensics:** SIEM collects, logs, and tracks information from different resources in the enterprise network, performs forensic analysis and generates various forensic reports like user activity reports, compliance reports, audit reports, etc.
- **IT Compliance and Reporting:** SIEM ensures compliance in real-time with various industry regulations such as FISMA, PCI/DSS, HIPAA etc., and automatically collects information necessary for compliance with organizational and government policies, and generates compliance reports.
- **Application Log Monitoring:** SIEM monitors log files from various operating systems, servers and web applications and generates analysis reports when security events are detected.
- **Object Access Auditing:** SIEM collects and manages all the object access audit logs at the central repository effectively. This helps in tracking successful and failure attempts in accessing organizational resources.
- **Data Aggregation:** Using data aggregation, SIEM aggregates all the similar events into one summary report. This report helps security analysts to further investigate on various security related events effectively.
- **Real-time Alerting:** SIEM triggers real-time notifications like intuitive dashboards, email or text messages to alert analyst regarding security events.
- **User Activity Monitoring:** SIEM tracks suspicious user behavior activities and generates user wise activity reports. It provides user activity monitoring, privileged user activity monitoring and audit reports.
- **Dashboards:** SIEM makes use of dashboards to inform security analysts and administrators to take defensive actions quickly and make right decision during security events.
- **File Integrity Monitoring:** In SIEM, file integrity monitoring ensures real-time monitoring and integrity of confidential data, meeting compliance requirements. It supports security analysts and administrators to record, access, and changes to the system files and folders like operating system files, system configuration files, installed software,

running processes, etc. It generates reports on all changes done to the system files and folders, and triggers real-time alerts when an unauthorized user tries to access any confidential files and folders.

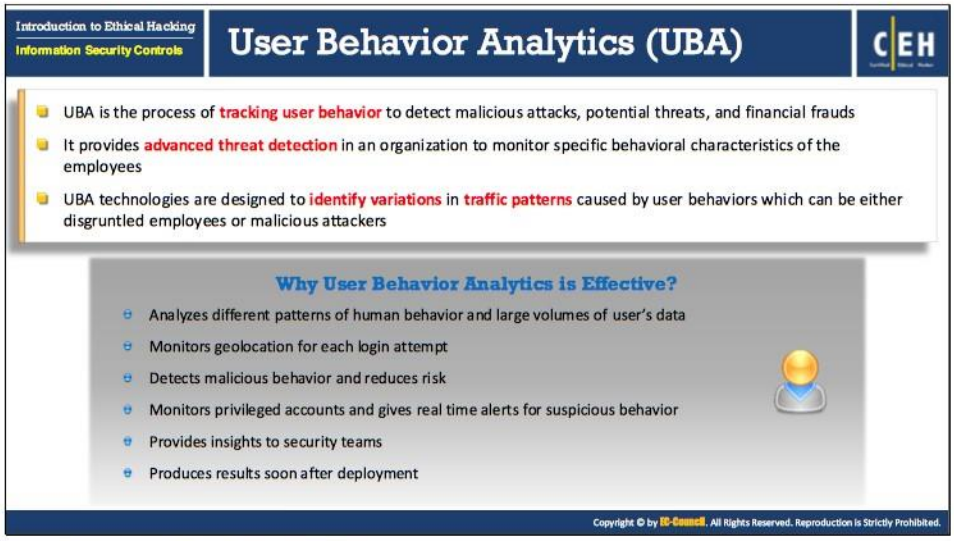
- **System and Device Log Monitoring:** SIEM provides both static and dynamic monitoring of enterprise systems and networks. It analyzes log data to identify suspected activities related to system compromise. It dynamically collects, correlates, and evaluates data from heterogeneous systems and devices in the network to detect attacks as early as possible before any significant damage to enterprise resources.
- **Log Retention:** SIEM stores logged data in a central repository for long periods to meet compliance and regulatory requirements and for conducting forensic analysis, investigation, and internal audits. The log data stored in the central repository is generally encrypted and time stamped, to protect it from tampering.



SIEM Architecture

SIEM technology provides Security Event Management (SEM) and Security Information Management (SIM) services. SEM supports threat management and security incident handling by collecting and analyzing event information from different data sources in real time. SIM supports log management and analysis, compliance monitoring and forensic investigation of logged data.

SIEM applies normalization and aggregation to event data and contextual data collected from different internal and external sources such as business applications, operating systems, network devices, endpoint, access management, malware, vulnerability and identity information. Correlation rules are applied to the normalized data to detect security incidents. SIEM monitors access to servers and databases, performs user activity monitoring across multiple systems and applications in real time as well as provides protection from various internal and external threats.



User Behavior Analytics (UBA)

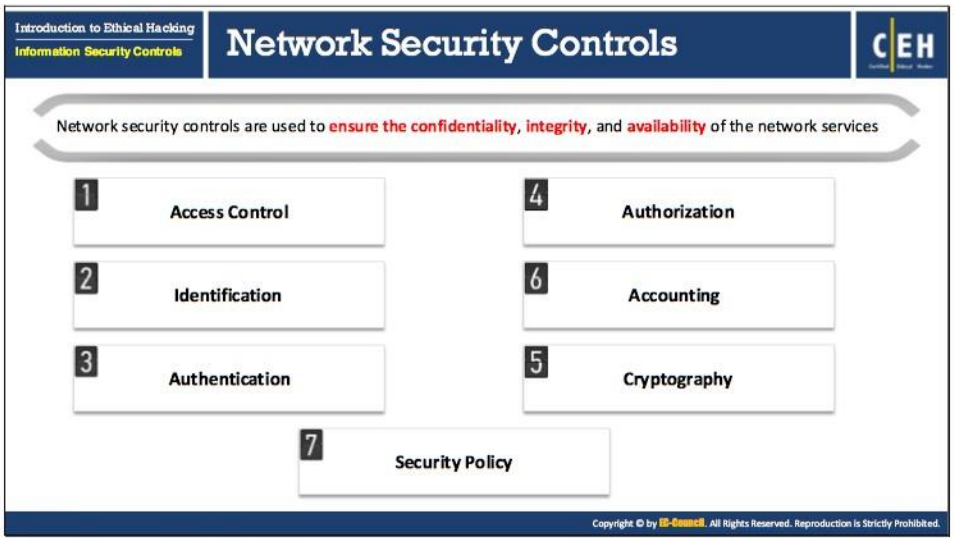
User Behavior Analytics (UBA) is the process of tracking user behavior to detect malicious attacks, potential threats, and financial frauds. It provides advanced threat detection in an organization to monitor specific behavioral characteristics of the employees. UBA technologies are designed to identify any unusual variations in traffic patterns, caused by user behaviors, which can be either disgruntled employees or malicious attackers. It is used as a defense mechanism to address anomalous user behavior in the field of Information to overcome the most complicated issues faced by security professionals today.

The employees working in a company access different websites, tools and applications. All their activities are logged and monitored. While these applications are running, there is a possibility of an intruder getting into the IT system and stealing the credentials without the knowledge of the user. When an intruder (external attacker or an insider) stays on the company's network as a legitimate user, UBA distinguishes this unusual behavior of the account by comparing the behavior baselines of both the user and the attacker, and raises an alert on its database and highlights the risk scores. When an alert is raised, a notification is sent out to the user's personal device for confirmation. In case the user does not confirm this activity, it is considered a major security breach. Through UBA the user's account can be disabled by the security teams depending on the severity of the incident and the risk level.

Why User Behavior Analytics is effective?

- Detects malicious insiders and outsiders at an early stage
- Identifies possible risk events in the IT infrastructure
- Analyzes different patterns of human behavior and large volumes of user's data
- Monitors geo-location for each login attempt

- Detects malicious behavior and reduces risk
- Monitors privileged accounts and provides real time alerts for suspicious behavior insights to security teams
- Provides insights to security teams
- Produces results soon after deployment

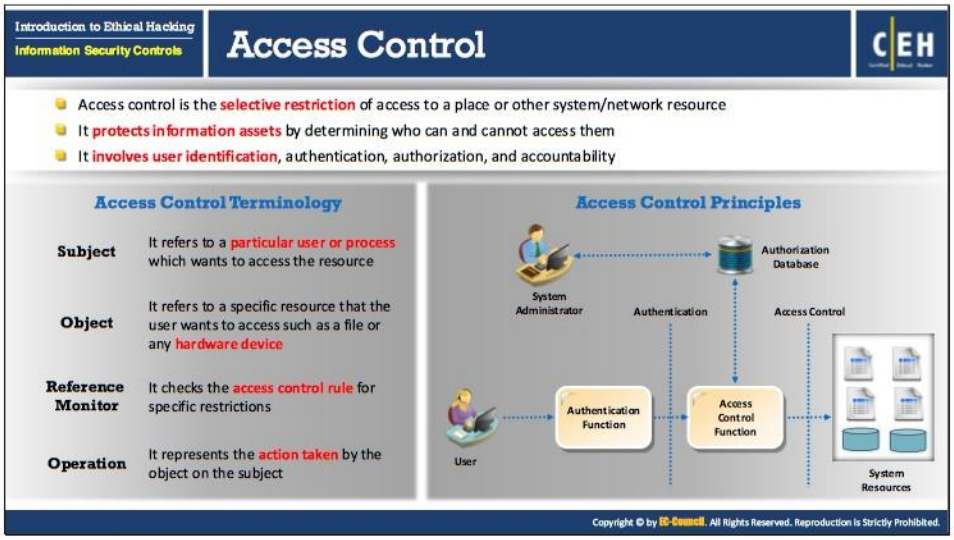


Network Security Controls

Network security controls are used to ensure the confidentiality, integrity, and availability of the network services. These security controls are either technical or administrative safeguards implemented to minimize the security risk. To reduce the risk of a network being compromised, an adequate network security requires implementing a proper combination of network security controls. These network security controls include:

- Access Control
- Identification
- Authentication
- Authorization
- Accounting
- Cryptography
- Security Policy

These controls help organizations with implementing strategies for addressing network security concerns. The multiple layers of network security controls along with the network should be used to minimize the risks of attack or compromise. The overlapping use of these controls ensures defense in depth network security.



Access Control

Access control is a method for reducing the risk of data from being affected and to save the organization's crucial data by providing limited access of computer resources to users. The mechanism grants access to system resources to read, write, or execute to the user based on the access permissions and their associated roles. The crucial aspect of implementing access control is to maintain the integrity, confidentiality, and availability of the information.

An access control system includes:

- File permissions such as create, read, edit or delete
- Program permissions such as the right to execute a program
- Data rights such as the right to retrieve or update information in a database

There are two types of access controls: physical and logical. The physical access controls the access to buildings, physical IT assets, etc. The logical access controls the access to networks and data.

In general, access control provides essential services like authorization, identification, authentication, access permissions and accountability.

- Authorization determines the action a user can perform
- Identification and authentication identify and permit only authorized users to access the systems
- The access permissions determine approvals or permissions provided to a user to access a system and other resources
- Accountability categorizes the actions performed by a user

Access Control Terminology

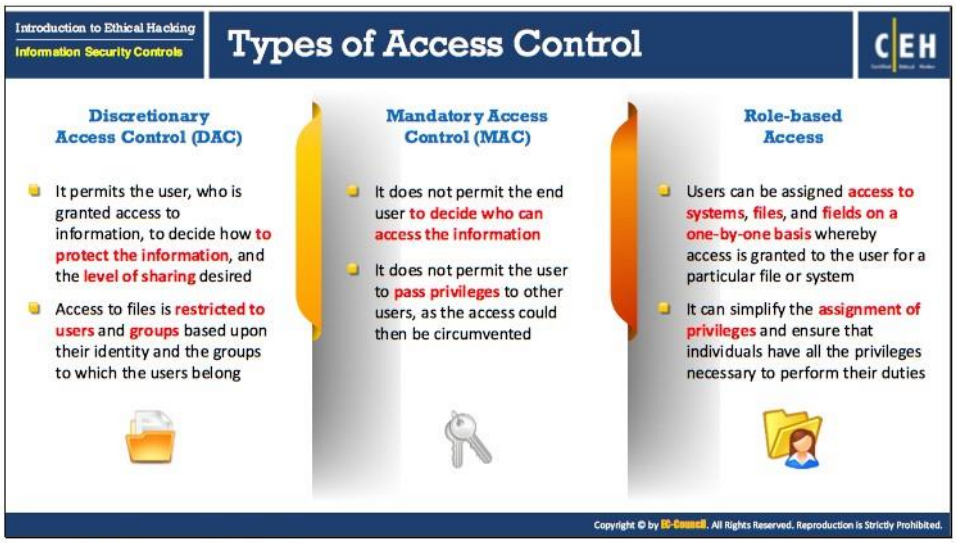
The following terminologies are used to define access control on specific resources:

- **Subject:** A subject may be defined as a user or a process, which attempts to access the objects. Further, subjects are those entities that perform certain actions on the system.
- **Object:** An object is an explicit resource on which access restriction is imposed. The access controls implemented on the objects further control the actions performed by the user. For example, files or hardware devices.
- **Reference Monitor:** It monitors the restrictions imposed according to certain access control rules. Reference monitor implements a set of rules on the ability of the subject to perform certain actions on the object.
- **Operation:** An operation is an action performed by the subject on the object. A user trying to delete a file is an example of an operation. Here, the user is the subject, delete refers to the operation and file is the object.

Access Control Principles

Access control principles deal with restricting or allowing the access controls to users or processes. The principle includes the server receiving a request from the user and authenticating the user with the help of an Access Control Instruction (ACI). The server can either allow or deny the user to perform any actions like read, write, access files, etc.

Access controls enable users to gain access to the entire directory, subtree of the directory and other specific set of entries and attribute values in the directory. It is possible to set permission values to a single user or a group of users. The directory and attribute values contain the access control instructions. Access control function uses an authorization database, maintained by the security admin, to check the authorization details of the requesting user.



Types of Access Control

Types of access control determine how a subject can access an object. The policy for determining the mechanism uses access control technologies and security.

The types of access control include:

- **Discretionary Access Control (DAC)**

  Discretionary access controls determine the access controls taken by any possessor of an object in order to decide the access controls of the subjects on those objects. The other name for DAC is a need-to-know access model. It permits the user, who is granted access to information, to decide how to protect the information and the level of sharing desired. Access to files is restricted to users and groups based upon their identity and the groups to which the users belong.

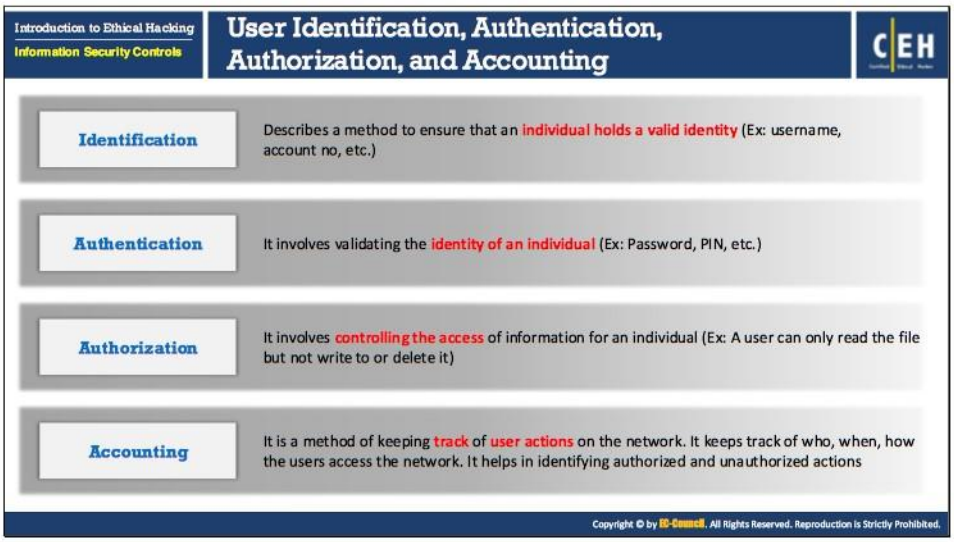
- **Mandatory Access Control (MAC)**

  The mandatory access controls determine the usage and access policies of the users. Users can access a resource only if that particular user has the access rights to that resource. MAC finds its application in the data marked as highly confidential. The network administrators impose MAC, depending on the operating system and security kernel. It does not permit the end user to decide who can access the information, and does not permit the user to pass privileges to other users as the access could then be circumvented.

- **Role Based Access Control (RBAC)**

  In role based access control, the access permissions are available based on the access policies determined by the system. The access permissions are out of user control, which means that users cannot amend the access policies created by the system. Users

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



User Identification, Authentication, Authorization and Accounting

- **Identification:** Identification deals with confirming the identity of a user, process, or device accessing the network. User identification is the most common technique used in authenticating the users in the network and applications. Users have a unique User ID, which helps in identifying them.

  The authentication process includes verifying a user ID and a password. Users need to provide both the credentials in order to gain access to the network. The network administrators provide access controls and permissions to various other services depending on the user ID's.

  Example: Username, Account Number, etc.

- **Authentication:** Authentication refers to verifying the credentials provided by the user while attempting to connect to a network. Both wired and wireless networks perform authentication of users before allowing them to access the resources in the network. A typical user authentication consists of a user ID and a password. The other forms of authentication are authenticating a website using a digital certificate, comparing the product and the label associated with it.

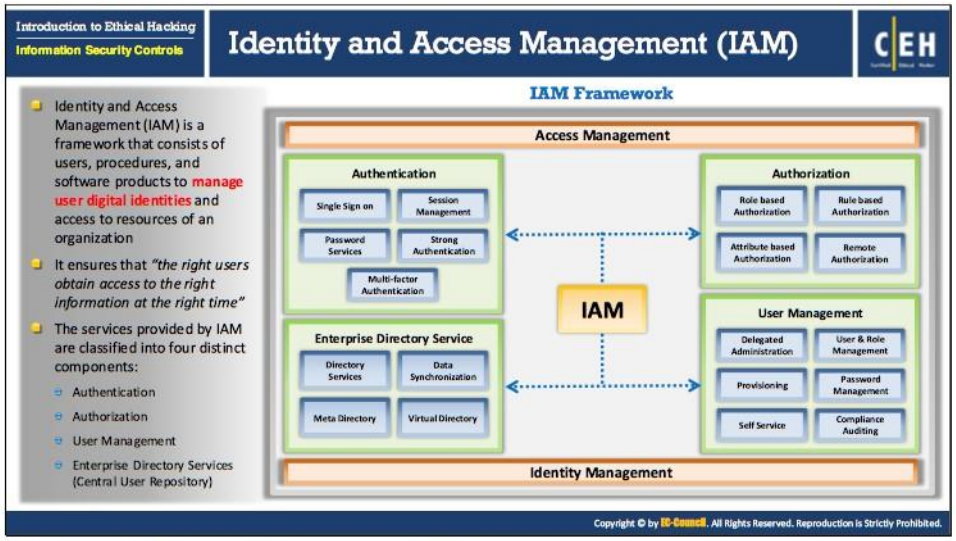
  Example: Password, PIN, etc.

- **Authorization:** Authorization refers to the process of providing permission to access the resources or perform an action on the network. Network administrators can decide the access permissions of users on a multi-user system. They even decide the user privileges. The mechanism of authorization can allow the network administrator to create access permissions for users as well as verify the access permissions created for each user. In logical terms, authorization succeeds authentication. But, the type of

authentication required for authorization varies. However, there are cases that do not require any authorization of the users requesting for a service.

Example: A user can only read the file but not write to or delete it.

- **Accounting:** User accounting refers to tracking the actions performed by the user on a network. This includes verifying the files accessed by the user, functions like alteration or modification of the files or data. It keeps track of who, when, how the users access the network. It helps in identifying authorized and unauthorized actions.



Identity and Access Management (IAM)

Modern enterprises currently need fast, easy and secure access to IT resources, from anywhere and at any time, provided with effective security controls on IT assets that protect from both internal and external threats. Advancement in technologies like IoT (Internet of Things), M2M Communication, Bring Your Own Device (BYOD) pose a variety of internal and external threats and vulnerabilities to the organizations. Identity and Access Management solutions have become an important part of IT strategic planning and organizations need to use IAM solutions to prevent and protect their IT assets from various malicious attacks.

What is IAM?

Identity and Access Management (IAM) is a framework for business practices that consists of users, procedures, and software products to manage user digital identities and access to resources of an organization. It ensures that the right users obtain access to the right information at the right time.

IAM systems are used for automated creation, recording, and management of user identities and their access privileges. It is linked to the policies, procedures, protocols and processes of an organization. It provides identity management functions such as controlling user access to organizational secure systems and ensures that all users and services are properly authenticated, authorized and audited.

IAM Framework

IAM comprises of two modules, namely, access management module and identity management module.

- **Access Management Module**

  It covers authentication and authorization components of IAM. It provides organization wide authentication of resources by verifying access privileges of the users at the time of access.

- **Identity Management Module**

  It covers user management and enterprise directory service components of IAM. It provides capabilities like monitoring, recording, and logging of user behavioral activities.

The services provided by IAM are classified into four distinct components:

- **Authentication:** This component provides authentication management and session management. Through this component, the users provide their login credentials to access the applications and resources of the organization. It provides services such as single sign on, session management, password services, strong authentication and multifactor-authentication.
- **Authorization:** Authorization provides access control to various organizational resources. Access control includes role-based, rule-based, and attribute-based authorization services. Once the user is authenticated authorization component verifies whether that user is allowed to access a particular service or not. The user access request (generally in the form of URL for Web-based applications) is validated based on authorization policies stored in IAM policy store. To provide this service authorization makes use of complex access control mechanisms based on organizational security policies such as user groups, user roles, action performed, channels accessed, types of resources, time, external data and business rules.
- **User Management:** It provides administrative services such as delegated administration, user and role management, user provisioning and de-provisioning, password management, self-service, and compliance audit. Delegated administration improves accuracy of the system data within an IAM by distributing workload among different user departments. Many of the user management functions are centralized and some of these functions are delegated to end users. User and role management provides administrative services such as user identity creation, propagation and maintaining user identity and rights. It also performs user life cycle management that helps an organization to manage the lifetime of user accounts, from the initial phase of provisioning to the final phase of de-provisioning. An organization can maintain update and accurate user identity information using self-service, which provides user profile management functions including user's self-registration and automated password reset. Compliance audit service logs and tracks user behavioral activities.
- **Enterprise Directory Services:** The directory service provides central user repository that stores user identity information and enables other components and services of IAM

to retrieve and verify user credentials submitted by various client systems. This component provides the logical structure of all the user identities of an organization. It provides single point of administration and services such as data synchronization, meta directory and virtual directory, which are used to synchronize and manage user identity data from databases, applications, networks, and systems in real time. IAM directory services implement standards such as Lightweight Directory Access Protocol (LDAP) and Simple Cloud Identity Management (SCIM).

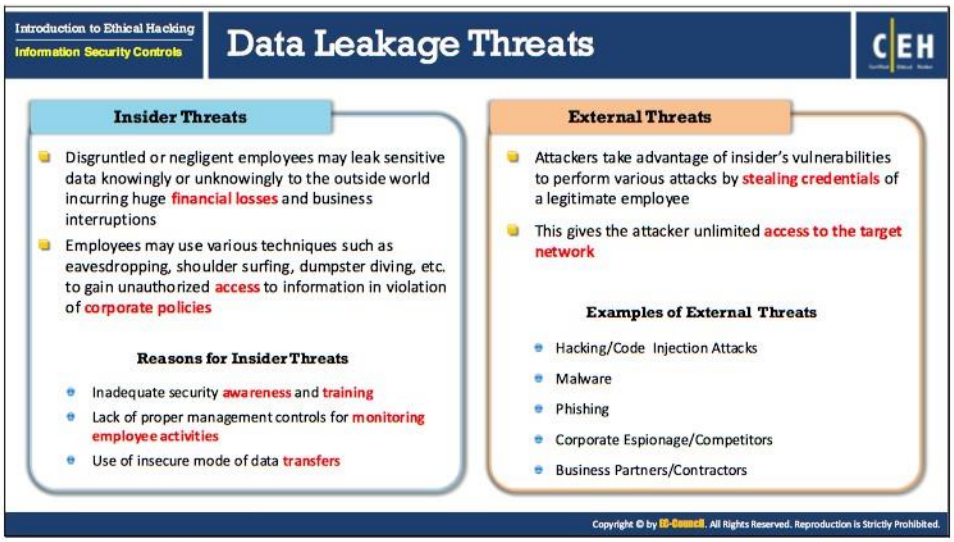
Data Leakage

Data leakage refers to unauthorized access or disclosure of sensitive or confidential data. Advancement in information technology has made data vulnerable to various malware attacks leading to the leakage of sensitive and confidential data to the attacker. Data leakage may happen electronically through an email or malicious link or via some physical method such as device theft, hacker break-ins, etc.

Major Risks to Organizations

The following are major risks that are encountered by organizations due to data leakage:

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



Data Leakage Threats

Insider Threats

Most of the data attacks come from the insiders only making it much more difficult to prevent or detect them. Disgruntled or negligent employees may leak sensitive data knowingly or unknowingly to the outside world incurring huge financial losses and business interruptions. Employees may use various techniques such as eavesdropping, shoulder surfing, dumpster diving, etc. to gain unauthorized access to information in violation of corporate policies. System misconfiguration and technology failures also enable insiders to steal sensitive information. Insider threats are difficult to thwart because insiders are mostly aware of the security loopholes of the organization and they exploit them to steal confidential information.

Reasons for insider threats:

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

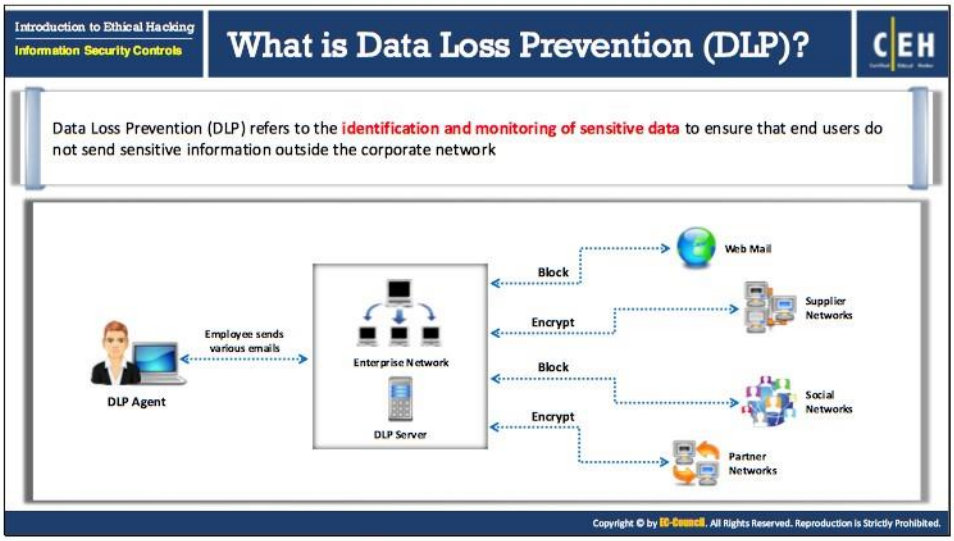
External Threats

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

Listed below are some of the examples of external threats:

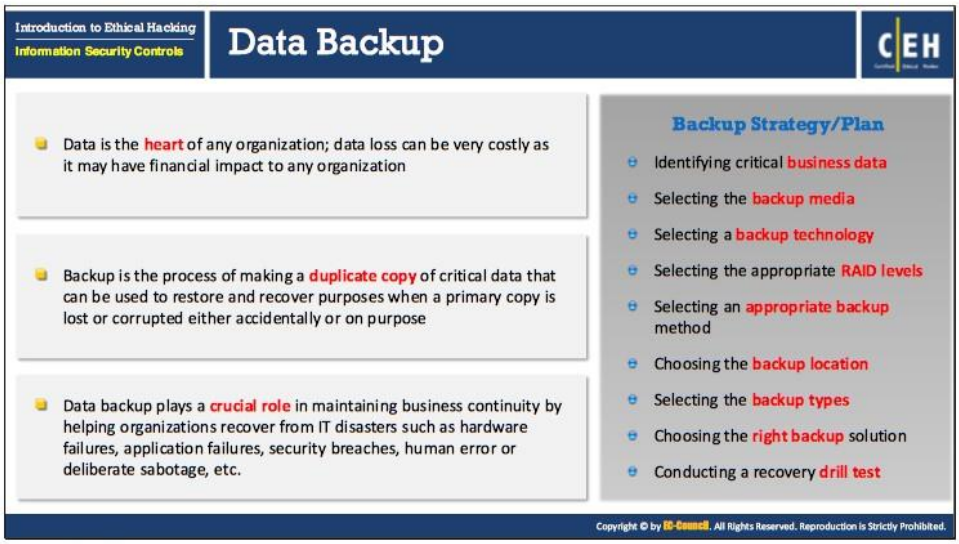
- **Hacking/Code Injection Attacks:** Attackers exploit vulnerabilities in operating systems, applications and databases, which provide them access to confidential information.

- **Malware:** Malicious software such as key loggers, spyware, Trojans, backdoors, etc. installed in a system enable the attacker to gain access to the system and steal all the information.
- **Phishing:** An illegitimate email or pop-up falsely claiming to be from a legitimate site attempts to acquire the user's personal or account information.
- **Corporate espionage/Competitors:** Nefarious competitors use different tactics to gain information such as corporate and marketing strategies, product plans, source code, trade secrets, etc. from the organization.
- **Business Partners/Contractors:** Outsourcing some capabilities to partners pose a significant risk as they have access to sensitive data and even sell them locally without the knowledge of the organization.



What is Data Loss Prevention (DLP)?

Data Loss/Leakage Prevention (DLP) refers to the identification and monitoring of sensitive data to ensure that end users do not send sensitive information outside the corporate network. It is a combination of various techniques and tools that help administrators to control data access. It provides a more secure environment for the transmission of data between different parties. DLP recognizes private data and tracks all its movement through the network access points and protects it from any unauthorized entity in the network. It detects potential threats to data transmissions and prevents data breaches by monitoring, detecting, and blocking access to confidential data.



Data Backup

Data is the heart of any organization; data loss can be very costly as it may have financial impact on any organization. Backup is the process of making a duplicate copy of critical data that can be used to restore and serve towards the recovery purpose when a primary copy is lost or corrupted either accidentally or on purpose. Data backup plays a crucial role in maintaining business continuity by helping organizations recover from IT disasters such as hardware failures, application failures, security breaches, human error or deliberate sabotage, etc. All regulatory compliance such as COBIT, SSAE SOCII, PCI-DSS, HIPPA, SOX, FINRA, FISMA, EU General Data Protection Regulation (GDPR), etc. require businesses to maintain data backups of critical data for a specified duration.

Data backup is mainly used for two purposes: To reinstate a system to its normal working state after damage or to recover data and information after a data loss or data corruption. Data loss in an organization affects the financial, customer relationship, and company data. Data loss in personal computers may lead to a loss of personal files, images and other important documents saved in the system.

Backup Strategy/Plan

An ideal backup strategy includes steps ranging from selecting the right data to conducting a drill test data restoration.

1. **Identifying the critical business data**

   Every organization has an abundance of data. The criticality of the data is based on the importance it serves to the organization. It requires analyzing and deciding which information is more important to the organization's proper functioning. The critical data may consist of revenue, emerging trends, market plans, database, files including

documents, spreadsheet, e-mails, etc. and loss of such critical data can affect the organization immensely. Therefore, an organization should identify critical data or files that require backup.

2. **Selecting the backup media**

   Choosing the best backup media is a common concern within most organizations. Backup media selection depends on the type and amount of data the backup will consist of. With a better and well thought out plan, selecting the proper media enables a better level of data backup. Whereas the selection of the wrong media device leads to the segregation of data to many different media devices. At times, data backup also consumes a large amount of space and therefore, attention is required while selecting the best backup media for the situation and fulfillment of the needs of the organization.

3. **Selecting a backup technology**

   Choosing proper backup technology plays a major role in backup strategy planning. Organizations need to select proper backup technology that acquires the ability to restore, recover and maintain the availability of its services whenever needed.

4. **Selecting the appropriate RAID levels**

   Many organizations depend on RAID technology for handling their critical backup needs, especially with the increases in data flow and data volume. Organizations are expanding their networks in order to improve their productivity in the market. However, this additional increase can cause network bottlenecks. The probability of losing data due to a disaster, threats, mistakes and hardware failure hamper an organization's ability to grow. RAID technology overcomes these situations providing an option for data availability, high performance, efficient, and accessible recovery options without a loss of data. Selection of any RAID level should be based on the needs of the organization and the features offered by each level.

5. **Selecting an appropriate backup method**

   Organizations can choose any backup method depending on their budget and IT infrastructure. The different types of data backup methods are:

   - **Hot backup**

     A hot backup is a popular type of backup method. It is also called as dynamic backup or active backup. In a hot backup, the system continues to perform the backup process even if the user is accessing the system. Implementation of a hot backup in an organization, avoids downtime.

   - **Cold backup**

     A cold backup is also called an offline backup. The cold backup takes place when the system is not working or is not accessible by users. A cold backup is the safest method of backup as it avoids the risk of copying the data. A cold backup involves downtime, as the users cannot use the machine until the process is back online.

- **Warm backup**

  A warm backup, also called a nearline backup, will have connectivity to the network. In a warm backup, the system updates are turned on to receive periodic updates. It is beneficial when mirroring or duplicating the data.

6. **Choosing a backup location**

   Organizations can choose any backup location depending on their budget and IT infrastructure. The different types of data backup locations are:

   - **Onsite data backup**

     This type of backup is performed within the organization. Onsite backup uses external devices such as a tape drive, DVD, hard disk, etc. The choice of external storage will depend on the amount of data to be backed up.

   - **Offsite data backup**

     In an offsite backup, the backup is done at a remote location. It either stores the data on physical drives, online or third party backup service. Storing the data online helps have an updated data backup available.

   - **Cloud data backup**

     A cloud backup is also known as online backup. It involves storing the backup on a public network or on a proprietary server. Usually a third party service provider hosts the proprietary server. The backup process in a cloud data backup works according to the requirements of the organization. If the organization needs the backup on a daily basis, the proprietary server will run a daily backup. Usually any non-critical data is archived using a cloud data backup.

7. **Selecting the backup types**

   An appropriate backup type is the one that does not add a major impact to the bandwidth, cost, time required and the resources of the organization. The three most common backup types are full, differential and incremental.

   - **Full backup**

     It is also called a normal backup. The full backup occurs automatically according to a set schedule. It copies all the files and compresses them to save space. A full backup provides efficient data protection to the copied data.

   - **Incremental backup**

     Backups only the data that has changed since the last backup. The last backup can be any type of backup. Before an incremental backup can be performed, the system should be backed up using a full or normal backup.

   - **Differential backup**

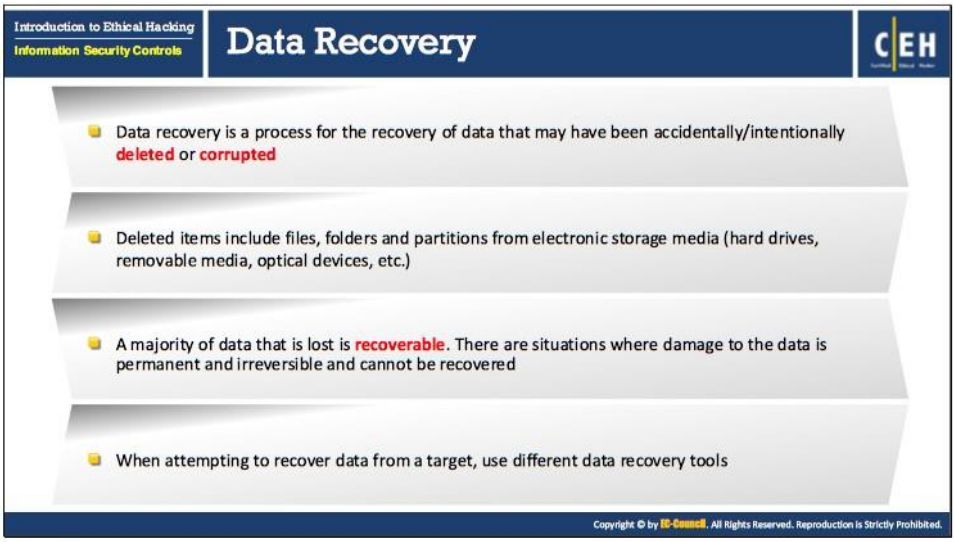
     Differential backup is the combination of a full backup and an incremental backup. A differential backup backs up all the changes made since the last full backup.

8. **Choosing the right backup solution**

   Choosing an appropriate backup solution is essential for efficient and effective backups. Data loss is avoidable to an extent with excellent backup solutions.

9. **Conducting a recovery drill test**

   An organization performs a drill test to validate it has a foolproof and updated DR plan. Having chosen the appropriate backup solution, it is advised to perform a recovery drill test at least once or twice a year, depending on the size of the organization.



Data Recovery

Data loss is a primary concern for any organization. Data recovery (DR) is a process for the recovery of data that may have been accidentally/intentionally deleted or corrupted. Deleted items include files, folders, and partitions from electronic storage media (hard drives, removable media, optical devices, etc.). The process of data recovery varies depending on how the data was lost, the data recovery software used and the device where the data will be restored. Data recovery software can assist with retrieving the data, usually with great results and most of the data that is lost is recoverable. However, there are situations where the damage to the data is permanent and irreversible. When attempting to recover data from a target, use different data recovery tools.

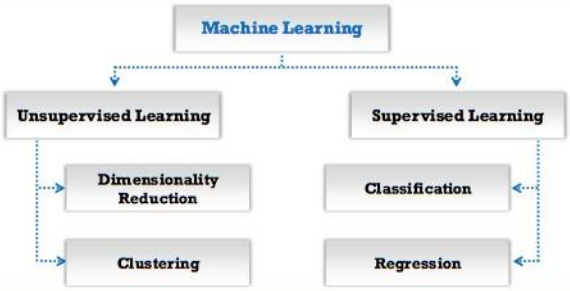
Information stored on storage devices such as a flash drive, a hard disk, DVD, etc. can be recovered. Users should not write or save over any data stored on the affected media. In an organization the disaster recovery plan should mention the individual/team responsible for recovery of data. And, improperly trained users should not perform data recovery.

Introduction to Ethical Hacking
Information Security Controls

Role of AI/ML in Cyber Security

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

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

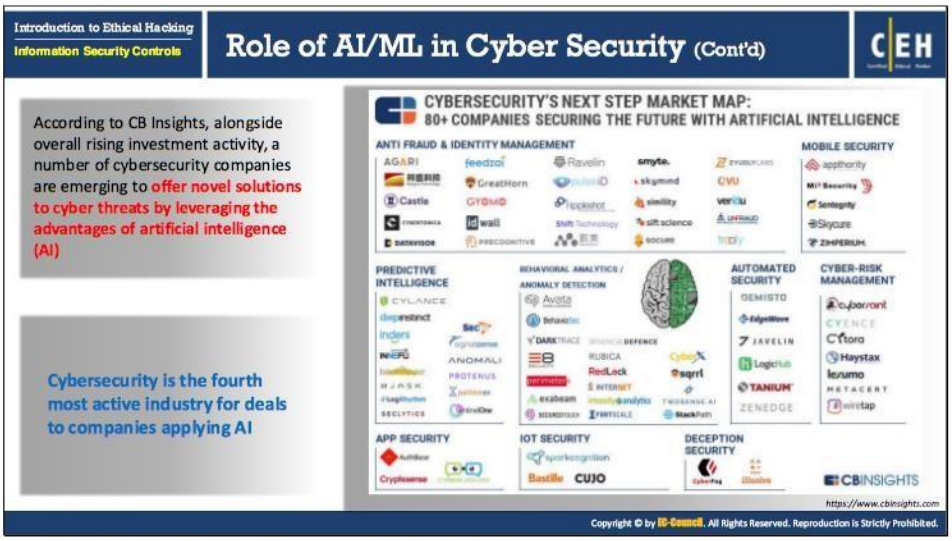


Introduction to Ethical Hacking
Information Security Controls

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

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

https://www.gartner.com



Role of Artificial Intelligence and Machine Learning in Cyber Security

Machine learning (ML) and Artificial Intelligence (AI) are now vastly used across various industries and applications due to the increase in the computing power, data collection and storage capabilities.

Along with technological advancements in AI such as self-driving cars, language translators and big data there is also rise in threats such as ransomware, botnets, malware, phishing, etc. Using AI and ML in cyber security helps in identifying new exploits and weaknesses, which can be easily analyzed to mitigate further attacks. It reduces the pressure of security professionals and alerts them whenever an action needs to be performed.

What is AI/ML?

Artificial Intelligence is the only solution to defend networks against various attacks that an antivirus scan cannot detect. The huge amount of collected data is fed into the AI, which is processed and analyzed to understand its details and trends.

ML is a branch of artificial intelligence (AI) that gives the systems the ability to self-learn without any explicit programs. It is a self-learning system that is used to define what the normal network looks like along with its devices and then uses this to backtrack and report any deviations and anomalies in real time.

There are two types of ML classification techniques:

- **Supervised Learning**

  Supervised learning makes use of algorithms that inputs a set of labeled training data, with the aim of learning the differences between the labels. Supervised learning is further divided into two subcategories, namely, classification and regression.

Classification includes completely divided classes and its main task is defining the test sample to identify the class it belongs to. Regression is used when data classes are not separated i.e. when data is continuous.

- **Unsupervised Learning**

  Unsupervised learning makes use of algorithms that input unlabeled training data, with the aim of deducing all categories by itself. Unsupervised learning is further divided into two subcategories namely, clustering and dimensionality reduction. Clustering divides the data into clusters based on the similarities between the input data regardless of class information. Dimensionality reduction is the process that involves reducing the dimensions (attributes) of data.

Why AI/ML?

Source: *https://www.gartner.com*

The security threat landscape continues to evolve not just in scale, but, more importantly, in sophistication. Despite a range of advancements in the industry to safeguard against increasingly bold and intricate threats, organizations have struggled to keep pace with the technologies and techniques employed by those responsible for such attacks.

As companies continue to increase their digital footprints, "identify and diagnose" capabilities are not enough to remediate against a growing fundamental business challenge for organizations of all shapes and sizes. The development of advanced security analytics is an important consideration for organizations looking to implement machine learning to defend against an array of internal and external security threats.

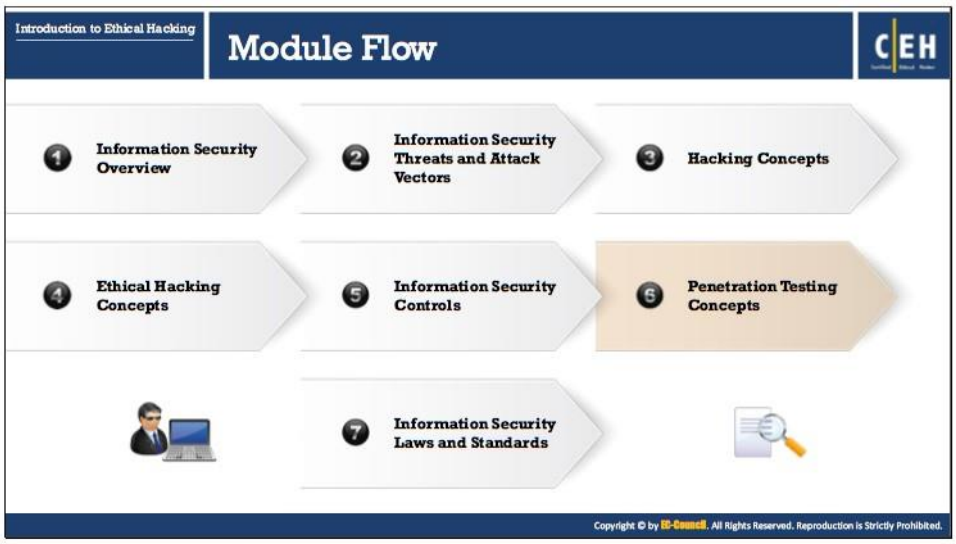
AI/ML Applications Areas

Source: *https://www.cbinsights.com*

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

According to CB Insights' AI Deals Tracker, cybersecurity is the fourth most active industry for deals to companies applying AI. As per CB Insights data, there are over 80 private companies in cybersecurity that are using AI and they categorized them into the nine main areas in which they operate.

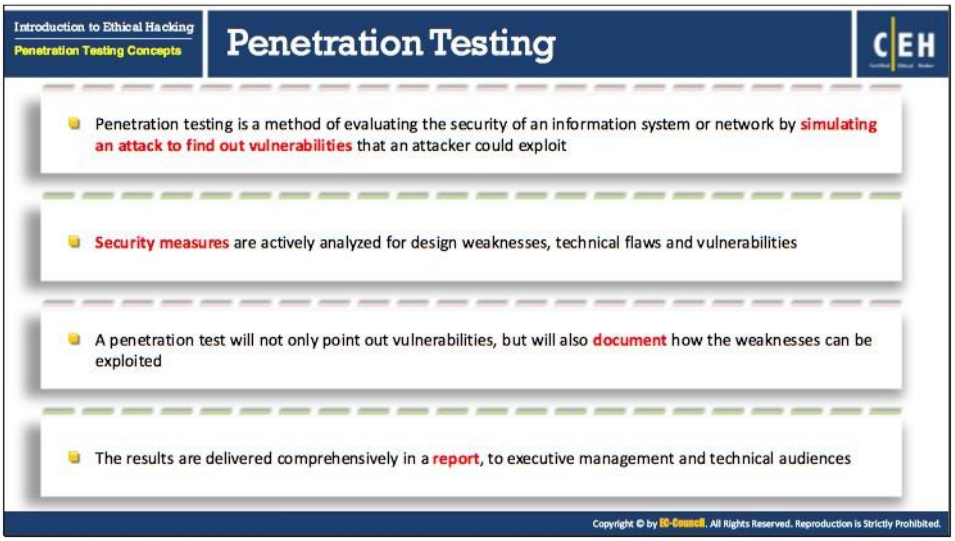
- Anti-fraud and identity management
- Mobile security
- Predictive intelligence
- Behavioral analytics / anomaly detection
- Automated security
- Cyber-risk management
- App security
- IoT security
- Deception security



Penetration Testing Concepts

Hacking is the ability to invent previously unknown ways of doing things. In this context, advocating a specific methodology to simulate a real-world hack might come across as a contradiction. The reason behind advocating a methodology in penetration testing arises from the fact that most hackers follow a common underlying approach when it comes to penetrating a system.

This section provides an overview of penetration testing, why penetration testing is necessary, the types of penetration testing, and the phases of penetration testing.



Penetration Testing

Penetration testing is a method of evaluating the security of an information system or network by simulating an attack to find out vulnerabilities that an attacker could exploit. Penetration test (or "pen-testing") exposes the gaps in the security model of an organization and helps organizations reach a balance between technical prowess and business functionality from the perspective of potential security breaches. This can help in disaster recovery and business continuity planning. It simulates methods used by intruders to gain unauthorized access to an organization's networked systems and then compromise them and involves using proprietary and open-source tools to conduct the test. Apart from automated techniques, penetration testing involves manual techniques for conducting targeted testing on specific systems to ensure that there are no security flaws that previously might have gone undetected. In the context of penetration testing, the tester is limited by resources: namely, time, skilled resources, and access to equipment as outlined in the penetration testing agreement.

Penetration testing involves an active analysis of system configurations, design weaknesses, network architecture, technical flaws, and vulnerabilities. A penetration test will not only point out vulnerabilities, but will also document how the weaknesses can be exploited. On completion of the penetration testing process, pen-testers deliver a comprehensive report with details of vulnerabilities discovered and suite of recommended countermeasures to the executive, management, and technical audiences.

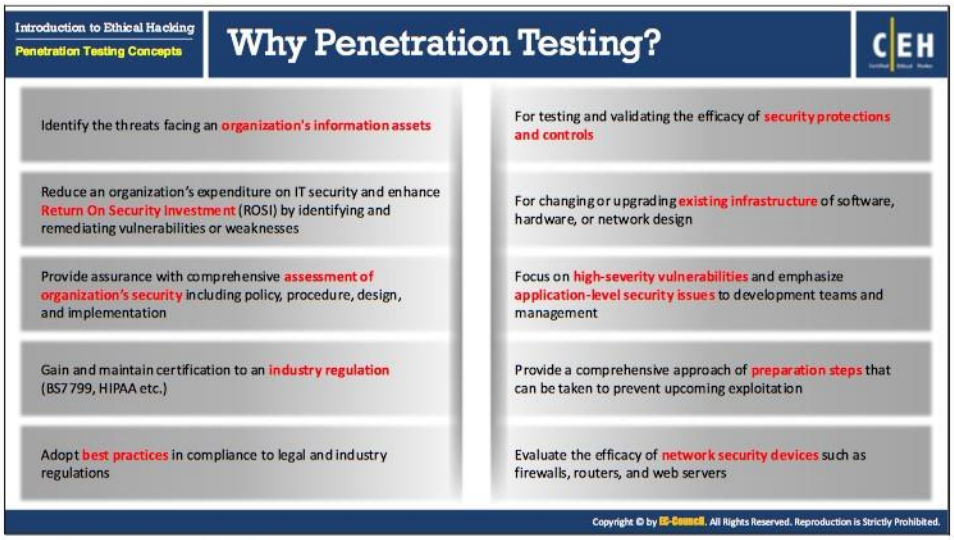
A penetration tester is different from an attacker only by intent, lack of malice, and authorization. Incomplete and unprofessional penetration testing can result in a loss of services and disruption of business continuity. Therefore, employees or external experts must not conduct pen-tests without proper authorization.

The management of the client organization should provide clear written permission to perform penetration testing. This approval should include a clear scope, a description of what to test, and when the testing will take place. Because of the nature of pen-testing, a failure to obtain this approval might result in committing a computer crime, despite one's best intentions.

What Makes a Good Penetration Test?

The following activities will ensure a good penetration test:

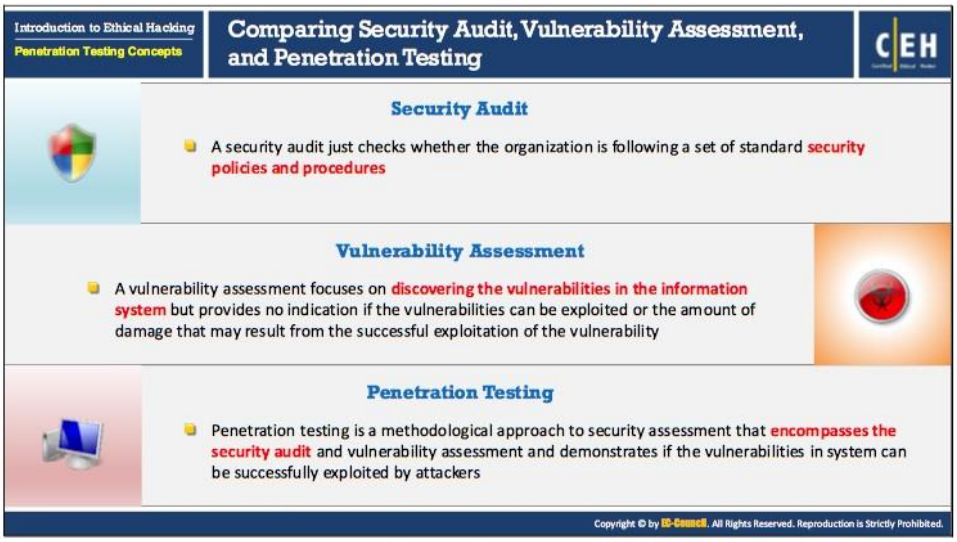
- Establishing the parameters for the penetration test, such as objectives, limitations, and justifications of the procedures
- Hiring highly skilled and experienced professionals to perform the pen-test
- Appointing a legal penetration tester, who follows the rules in the nondisclosure agreement
- Choosing a suitable set of tests that balance costs and benefits
- Following a methodology with proper planning and documentation
- Documenting the results carefully and making them comprehensible to the client. The penetration tester must be available to answer any queries whenever there is a need.
- Clearly stating findings and recommendations in the final report



Why Penetration Testing

Penetration testing is important to the organizations for the following reasons:

- Identifying the threats facing an organization's information assets
- Reducing an organization's expenditure on IT security and enhancing Return on Security Investment (ROSI) by identifying and remediating vulnerabilities or weaknesses
- Providing assurance with comprehensive assessment of organization's security including policy, procedure, design, and implementation
- Gaining and maintaining certification to an industry regulation (BS7799, HIPAA etc.)
- Adopting best practices in compliance to legal and industry regulations
- Testing and validating the efficacy of security protections and controls
- Changing or upgrading existing infrastructure of software, hardware, or network design
- Focusing on high-severity vulnerabilities and emphasize application-level security issues to development teams and management
- Providing a comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation
- Evaluating the efficacy of network security devices such as firewalls, routers, and web servers



Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

Although many people use the term security audit, vulnerability assessment, and penetration testing interchangeably to mean security assessment, there are considerable differences, as discussed below.

- **Security Audit**

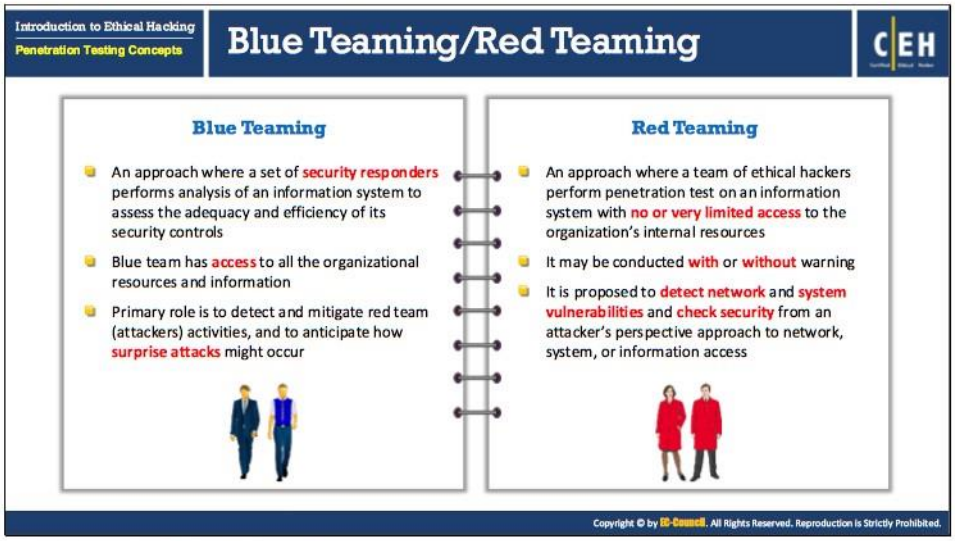
  A security audit just checks whether the organization is following a set of standard security policies and procedures. It is systematic method of technical assessment of an organization's system that includes conducting manual interviews with staff, performing security scans, reviewing security of various access controls, and analyzing physical access to the organizational resources.

- **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 of the amount of damage that may result from the successful exploitation of the vulnerability.

- **Penetration Testing**

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



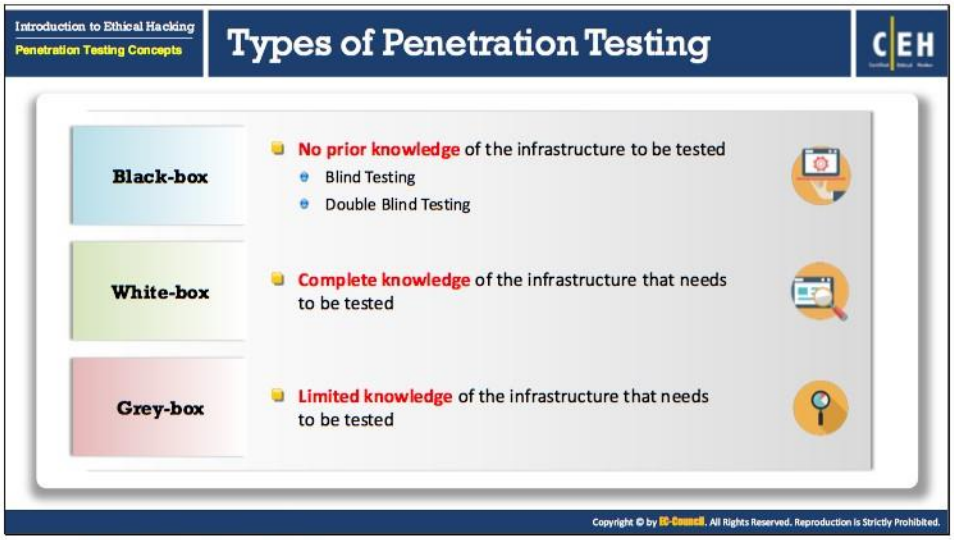
Blue Teaming/Red Teaming

- **Blue Teaming**

  A blue team (also known as defender team) is a group of highly skilled individuals, who undertake assessment of information security or products to identify security deficits, to determine the adequacy of security measures, to foresee efficacy of proposed security solutions, and so on, to defend against various attacks. Blue team The blue team may include system administrators and general IT staff and has access to all the organizational resources and information. Blue teaming is the least expensive and the most frequently used security assessment approach. Its primary role is to detect and mitigate red team (attackers) activities, and to anticipate the surprise attacks that might occur.

- **Red Teaming**

  A red team (also known as aggressor team) is a group of white-hat hackers (ethical hackers) who attempt to launch attacks against an organization's digital infrastructure, as would a malicious attacker, to test the organization's security posture. It is proposed to detect network and system vulnerabilities and check security from an attacker's perspective approach to network, system, or information access and it may be conducted with or without warning. Red teaming may include system administrators from various departments in an organization and they perform penetration test on an information system with no or a very limited access to the organization's internal resources.



Types of Penetration Testing

The types of penetration testing depend on the amount of information the pen-testing team is given about the organization, prior to the test. One can conduct any of the pen testing types either externally (conducted against Internet-facing hosts) or internally (conducted against hosts inside the organization's internal network). If we want a complete test, then testing both externally and internally is a must.

The three types of penetration testing are as follows:

- **Black-box Testing (Zero-Knowledge Testing)**

  In order to simulate real-world attacks, pen-testers can choose to undertake black-box testing (or zero knowledge testing, with no information or assistance from the client), and map the network while enumerating services, shared file systems, and operating systems discreetly. Additionally, the pen-tester can perform "war dialing" (scanning and dialing a list of phone numbers) to detect listening modems, and "war driving" (physically driving around an area to find wireless networks) to discover vulnerable access points, provided these activities are legal and within the scope of the project.

  In black-box testing, the pen-testers have only the company name. The tester thereafter uses fingerprinting methods to acquire information about the inputs and the expected outputs but is not aware of the internal workings of a system. Testers carry out this test after extensive research of the target organization. Black-box testing simulates an external attacker. Designing test cases are difficult without clear and concise specifications, but it is done once the specifications are complete.

  This test simulates the process of a real hacker. Black-box testing (also known as "functional testing") is time-consuming and expensive.

There are two types of black-box penetration testing:

- **Blind Testing**

  In the blind testing, the pen-tester has limited information or knows nothing about the target, but the target is informed of an audit scope (what, how, and when the pen-tester will be testing) prior to performing the test.

  Blind testing simulates the actions and procedures of a real hacker. The pen-testing team attempts to gather as much information as possible about the target organization from the Internet (company's website, domain name registry, online discussion board, USENET, etc.) and other publicly accessible sources. Pen testers start audit of the target organization's security based on the collected information. Tough, blind testing provides a lot of inside information (such as Internet access points, directly accessible networks, publicly available confidential /proprietary information, etc.) about the organization that may have been otherwise not known, but it is more time consuming and expensive, as a lot of effort is involved to research the target.

  Example: Ethical hacking, war-gaming, etc.

- **Double-Blind Testing**

  In double-blind testing (also known as "zero-knowledge testing"), neither the pen-tester knows about the target nor the target is informed of an audit scope (what, how, and when the pen-tester will test) prior to test execution. In other words, both parties are blind to the test. Most of the security assessments today are based on double-blind testing strategy, as it validates the presence of vulnerabilities that can be exploited and the ability of the target's individuals, processes, and tools to recognize and react appropriately to the penetration attempts made.

  Example: Black-box auditing, penetration testing, etc.

- **White-Box Testing (Complete-Knowledge Testing)**

  The organization may give complete information about its network to the pen-testers if it wants to assess its security against a specific kind of attack or a specific target. The information provided can include network-topology documents, asset inventory, and valuation information. Typically, an organization would opt for this when it wants a complete audit of its security. It is critical to note that despite all this, information security is an ongoing process and penetration testing gives a snapshot of the security posture of an organization at any given point in time. Security professionals may perform white-box testing with or without the knowledge of IT staff. The top management must approve the test if it does not involve the organization's IT staff.

  Organizations generally provide the following information for white-box testing:

  - **Company infrastructure:** This includes information related to the different departments of an organization. Penetration testers have the Information related to hardware, software, and controls in an organization.

- **Network type:** The network-type information could be regarding the organization's LAN and the topology used to connect the systems. It could also be information regarding access to remote networks or the Internet.
- **Current security implementations:** Current security implementations are the various security measures adopted by an organization to safeguard vital information against any kind of damage or theft.
- **IP address/firewall/IDS details:** This information includes details of the IP addresses an organization uses, the firewalls used to protect data from unauthorized users, and other important technical details about the network. Organizations generally provide the firewall and IDS policies to the penetration tester.
- **Company policies:** An organization may provide business continuity and IT security policies to the pen testers, depending on the nature of the test. Security policies, legal policies, and labor policies can all be useful to the penetration tester.

- **Grey-Box Testing (Partial-Knowledge Testing)**

  Grey-box testing combines the methodologies of both black-box and white-box testing. It is the most common approach to test the vulnerabilities that an attacker can find and exploit. In certain cases, organizations would prefer to provide the pen-testers with partial knowledge or information that hackers could find, such as the domain-name server. This information can also include an organization's publicly perceived asset and vulnerabilities. The pen-testers may also interact with system and network administrators.

  Grey-box pen testing provides a full system inspection, from both the developer's and a malicious attacker's perspectives. It is a simulation of a systematic attack by outside intruders or malicious insiders with limited access privileges.

There are two ways to perform the above mentioned penetration tests:

- **Announced Testing**

  Announced testing is an attempt to compromise systems on the client's network with the full cooperation and knowledge of the IT staff. This type of testing examines the existing security infrastructure for possible vulnerabilities.

  Announced penetration testing helps a penetration tester in the following ways:

  - A penetration tester can easily acquire a complete overview of the infrastructure of the organization.
  - A penetration tester may be given the kind of physical access provided to different employees in the organization.
  - A penetration tester may get a clearer picture of measures applied to information and system security of the organization.

The security staff usually joins the penetration testing teams to conduct these audits. This type of penetration testing is quite effective for the physical security of the penetration testing.

Advantages:

- More efficient
- Team-oriented

Disadvantages:

- Lack of security
- Less-reliable results

- **Unannounced Testing**

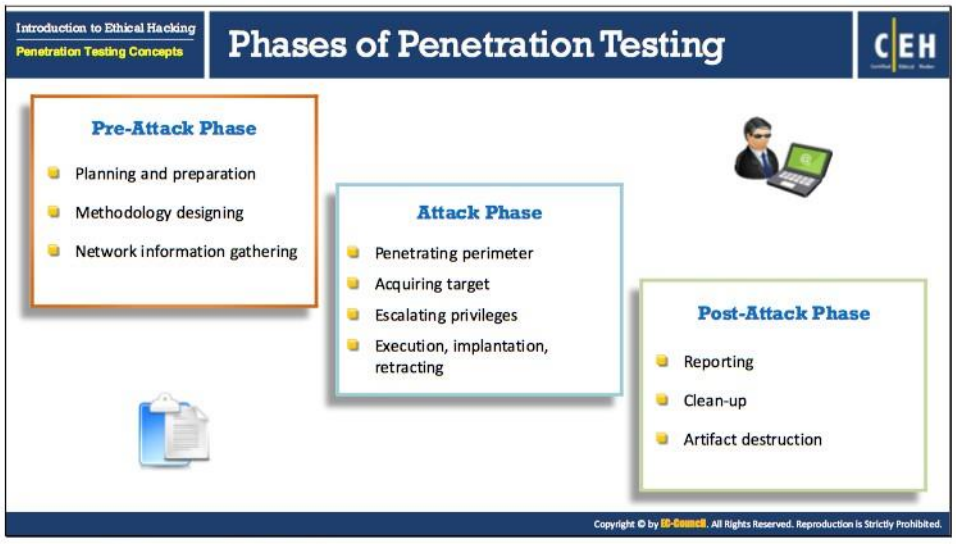
  Unannounced testing is an attempt to compromise systems on the client's network without the knowledge of IT security personnel. This approach is quite effective for testing the security of an organization against social-engineering attempts. In unannounced pen testing, only the top management is aware of these tests. It helps the organization to check for organizational security threats that may arise because of human error and/or ignorance. Unannounced testing examines the agility of the security infrastructure and the responsiveness of IT staff and how much they are aware of the sensitivities of the organization's information security.

  Advantages:

  - Strong security
  - Highly reliable

  Disadvantages:

  - Less efficient
  - Requires a strict process



Phases of Penetration Testing

The three phases of penetration testing include pre-attack phase, attack phase and post-attack phase.

Pre-Attack Phase

The pre-attack phase includes planning, preparation and methodology designing to perform pen testing. This phase focuses on gathering as much information as possible about the target. It can be invasive, such as gathering information through scanning, or it can be noninvasive, such as reviewing public records.

Rules of Engagement (ROE)

Rules of Engagement (ROE) are the formal permissions to conduct a penetration test. They provide certain rights and restrictions to the test team for performing the test, and help testers to overcome legal, federal, and policy-related restrictions to use different penetration testing tools and techniques.

ROE may allow the testers to conduct some technical and nontechnical activities such as port scanning, social engineering, and network sniffing, and may restrict the conducting of certain activities, such as password cracking or SQL-injection attacks, which an organization might think are detrimental to the normal function of the organization or are too intrusive. The ROE explicitly defines these activities. Penetration testers might be allowed to conduct certain activities that may otherwise be considered illegal or against the established legal, federal, and policy guidelines.

Scope of ROE

The ROE acts as a guideline for penetration testers and therefore should clearly explain the allowed and restricted activities during a test.

The ROE includes:

- Specific IP addresses/ranges to be tested
- Any restricted hosts (i.e., hosts, systems, or subnets not to be tested)
- A list of acceptable testing techniques (e.g., social engineering, DoS, etc.) and tools (password crackers, network sniffers, etc.)
- Times when testing is to be conducted (e.g., during business hours, after business hours, etc.)
- Identification of a finite period for testing
- IP addresses of the machines from which penetration testing will be conducted, so that administrators can differentiate legitimate penetration testing attacks from actual malicious attacks
- Points of contact for the penetration testing team, the targeted systems, and the networks
- Measures to prevent law enforcement being called with false alarms (created by the testing)
- Handling of information collected by the penetration testing team

Understand Customer Requirements

Before proceeding with the penetration testing, it is important to fully understand the customer's requirements to ensure that the penetration test addresses them completely.

- Identify what needs to be tested:

FIGURE 1.7: Checklist of the Items that need to be tested

- Select the specific sectors to be tested, and prepare users and administrators
- Create a checklist of testing requirements
- Identify the time frame and testing hours
- Develop an emergency plan

- Ensure all information is securely backed up before beginning anything
- Decide on the format for reporting
- Identify who will be involved in the reporting and document delivery

Create a Checklist of the Testing Requirements

The following is an example checklist of penetration-testing requirements:

- Do you have any security-related policies and standards? If yes, do you want them to be reviewed?
- What is the network layout (segments, DMZs, IDS, IPS, etc.)?
- Does the client organization require analysis of its Internet presence?
- Do you want a review of the physical security of your servers and network infrastructure?
- What is the IP address configuration for internal and external network connections?
- Does your organization require pen testing of networking devices such as routers and switches? If yes, how many routers and switches exist on your network?
- Does the organization require pen testing of individual hosts?
- How many networking devices exist on the client's network?
- Do you want mapping of your Internet presence? Otherwise, can you provide us with a detailed diagram of your Internet presence; including addresses, host OS types, and software in use on the hosts? We will also need addresses in use on both sides of the hosts if they connect to both the Internet and the internal network.
- What security controls are deployed across the organization?
- Do you want a security review of the workstations on the network? If so, what operating systems are the workstations running? In addition, how many workstations would you like to be tested?
- Pen test will include five or fewer servers of each type (NT, UNIX, and Novell); do you want review of more servers? If so, how many of each?
- Does the organization require assessment of wireless networks?
- Does the organization require assessment of analog devices in the network?
- Does the organization deploy a mobile workforce? If so, is the mobile security assessment required?
- What are the web application and services offered by the client?
- Does the organization require an assessment of web infrastructure?
- Do you want the test team to conduct denial-of-service testing? This testing can have adverse effects on the systems tested. We can arrange to perform this testing during nonproduction hours.

- Do you want the test team to conduct a modem scan of your analog phone lines?
- What kind of RAS server are you using and how many modems are used?
- Do you want visits to other sites to perform assessments on systems?

Define the Pen-Testing Scope

The scope of the penetration test specifies the areas to be tested. It ensures that the team covers all the systems that require assessment.

The project scope considers the requirements of all the stakeholders. The organization and the testing team should clearly define all the objectives before creating the scope of the project. The following objectives require a higher priority:

- **Deliverables:** A list of the reports that are to be made available after the completion of the project.
- **Functionality:** Verification of whether the system works as expected.
- **Data definition:** A definition of the form that the results of testing will take.
- **Technical structure:** The design of the project in the form of flow diagrams.

The changes incorporated during project development influence the scope of the pen test. Usually, the client does not understand the impact of the changes. The more changes the project is subject to, the more time and resources it uses. The engagement lead should explain the effects of changes in requirements to the client. Often, a person from the client's company continually updates on the progress of the project.

The engagement lead should balance the time and project costs with respect to the scope of the project. The team should discard all the changes in the requirement that are beyond the scope. Other factors to consider while defining the project scope are:

- Business process changes
- Technology changes
- Location changes
- Application changes

The testing team should test all the features that the project will exhibit as a part of the design specification. The features that are to be tested include the following areas:

- **Network Security:** The testing team should test all the network components for security and configuration.
- **System Software Security:** The penetration test should identify system-software vulnerabilities.
- **Client-Side Application Security:** The testing team should check client-side applications for security and compliance with system requirements.
- **Client-Side to Server-side Application Communication Security:** The testing team should check data transmission for security.

- **Server-Side Application Security:** The testing team should check applications on the Web servers and application servers for flaws.
- **Document Security:** The testing team should advise the organization to enhance security. Employees should destroy the documents that are no longer used, but contain important details of the organization. The testing team should emphasize upon the use of shredders.
- **Social Engineering:** Implement social engineering techniques to trick individuals into divulging sensitive information such as passwords, project details, etc.
- **Application Communication Security:** Assess application communication security for any unauthorized interceptions.
- **Physical Security:** The organization should restrict physical access to relevant departments only.
- **Dumpster Diving:** Look for treasure (sensitive information) in the target's trash.
- **Inside Accomplices:** The team should check for disgruntled employees, who might release confidential data to the company's competitors.
- **Sabotage Intruder Confusion:** Organizations generally implement various strategies such as honeypots to confuse or misguide intruders. Intruders will attack the system thinking it as genuine, but that system will be a decoy system monitored by administrators. As a pen tester, you have to test and bypass various intruder confusion strategies.
- **Intrusion Detection:** The team should test any IDS or IPS.
- **Intrusion Response:** Determine the appropriate response to each incident.

Sign Penetration Testing Contract

A contract for penetration testing should include all needed clauses and other information and conditions for both parties involved in the penetration test. It should clearly state the rights and responsibilities of both the parties. The penetration testing contract must be drafted by a lawyer and signed by the penetration tester and the organization. A well-constructed contract must clearly state all points, such as:

- **Non-disclosure clause:** The target organization drafts this clause to safeguard its confidential information.
- **Objective of the penetration test:** This section of the pen testing contract states the reasons for performing the penetration test and the goals of the test.
- **Fees and project schedule:** These are the payment and pricing options of the pen-testing service.
- **Sensitive information:** This includes information related to the target organization's electronic assets, developing applications, network security parameters, or other sensitive information that is required by the penetration testing team.

- **Confidential information:** Confidential information includes trade-secret information, network information, telephone system information, customer data, business materials, etc. This information is provided to the pen tester, in confidence, for the purpose of tests on the condition that the confidential information will not be divulged or copied to any other third person, firm, or a company unless mentioned in written authorization by the confiding party.
- **Indemnification clause:** This clause protects the penetration tester/agency from any legal or financial liabilities, in case the penetration test results in loss or damage to the assets of the organization.
- **Reporting and responsibilities:** Contract guidelines state the methodology for performing the test and reporting procedures and scheduling period for the task assigned.

Sign Confidentiality Agreement and Non-Disclosure Agreement (NDA)

Two important documents to complete before any penetration testing begins are a confidentiality agreement and a nondisclosure agreement (NDA). A confidentiality agreement states that the information provided by the target organization is confidential and proprietary. This agreement also covers key aspects of negligence and liability for many potential issues. The target organization should be careful in wording the agreement, because many testing firms would try to avoid liability even in the case of negligence. Ensure that the service-providing firm has insurance coverage for damages.

A nondisclosure agreement (NDA) protects an organization's confidential information during business dealings with customers, suppliers, employees, and the press. A written NDA is a powerful legal tool, which states that no party will disclose any trade secrets, patents, or other proprietary information to anyone outside the company. A party can initiate legal action against the other party for any violation of the documented agreement whereas the organization can sue for damages and compensation. Many documents and other information regarding penetration testing contain critical information that could damage one or both parties if improperly disclosed.

Both parties bear the responsibility of protecting tools, techniques, vulnerabilities, and information from disclosure beyond the terms specified by a written agreement. Specific areas to consider include:

- Ownership of the information flowing on the network (internally and in the DMZ)
- Use of the evaluation reports
- Use of the testing methodology in customer documentation

The points to consider when drafting an NDA

- Identify truly valuable information and information that is critical to the company.
- Clearly specify that the person signing the agreement should not disclose the things mentioned in it.

- Clearly identify all parties in the agreement.
- Specifically include the starting date and length of the nondisclosure period.

All the parties involved in the NDA agreement should have it reviewed by their respective legal advisors.

Pre-Attack Phase: Information Gathering

During the pre-attack phase, the testing team will gather as much information as possible about the target company. Most leaked information relates to the network topology and the types of services running within the organization. The team can use this information to provisionally map out the network for planning a more coordinated attack strategy later.

This phase can include information retrieval such as the following:

- **Physical and logical location of the organization:** Map this phase to the tools and techniques discussed in the footprinting chapter. Examples include using the WHOIS database or search engines like Google, and finding the network block using the RIRs or the company website. This technique analyzes data returned during normal interaction with the organization, such as the banners and other system messages returned when connecting to the Web or mail server.
- **Analog connections:** These include phone lines, fax lines, dial-up lines, and other out-of-band connectivity types. Testers note these details for later use with war dialers. The important point here is to bypass the conventional security provided by firewalls, DMZs, and the like by taking advantage of an unprotected modem.
- **Contact information:** Testers obtain any contact information online, in phone books, or elsewhere. The tester can scout sources such as print media to get personal information and use social engineering techniques to extract information. This can include breaching physical security (tailgating), dumpster diving, and impersonation.
- **Information about other organizations:** Information about organizations connected to the target organization is an important security gap. As security is only as good as the weakest link, it is possible to breach the security by taking advantage of a weak link. Examples include third-party merchant sites or partners using default installations of Web application components known to have vulnerabilities.
- **Other information:** Information that has the potential for exploitation can include job postings, message group postings, press releases, and even casual conversations.

Passive Reconnaissance

Passive reconnaissance is a hacker's attempt to scout for our survey potential targets and then investigate the target using publicly available information. Access to this information is independent of the organization's resources, and anyone can freely access this information. This kind of reconnaissance is, consequently, difficult to detect.

Indicated passive reconnaissance steps include (but are not limited to) the following:

- Identifying the directory structure of the Web servers and FTP servers.

- Gathering competitive intelligence over newsgroups, bulletin boards, and industry feedback sites for references to and submissions from the organization. Testers can also obtain related information from job postings that include numbers of personnel required, and resumes and responsibilities. This can also include estimating the cost of support infrastructure.
- Determining the worth of the infrastructure that is interfacing with the Web—Testers may carry out asset classification as described under ISO 17799. This helps in quantifying acceptable risk to the business.
- Retrieving network registration information from WHOIS databases, using financial Web sites to identify critical assets, and searching for business services related to the registered party.
- Determining the product range and service offerings of the target company that are available online or can be requested online—estimate the threat level posed to these by checking for available documentation, associated third-party product vulnerabilities, cracks, and versions.
- Document sifting—this refers to gathering information solely from published material. This includes skimming through Web page source code, identifying key personnel, and investigating them further by background checks based on published résumés, affiliations, and publicly available information such as personal web pages, personal email addresses, or job databases.
- Social engineering—this refers to tricking individuals into divulging sensitive information. The objective here is to extract sensitive information and catalog it.

Active Reconnaissance

The information gathering process encroaches on the target territory. In this case, the perpetrator may send probes to the target in the form of port scans, network sweeps, enumeration of shares and user accounts, and so on. The hacker may adopt techniques such as social engineering and use tools that automate these tasks, such as scanners and sniffers.

- **Network mapping**

  Map the network by getting the information from the server domain registry numbers unearthed during the passive reconnaissance phase. The IP block forms the backbone of the network. Investigate the network linkages both upstream and downstream. These include the primary and secondary name servers for hosts and subdomains.

  Steps include (but are not limited to):

  - Interpreting broadcast responses from the network
  - Using ICMP to sweep the network, if ICMP is not blocked
  - Using reverse name lookups to verify addresses

- **Perimeter mapping**

  Map the perimeter by tracerouting the gateway to define the outer network layer and routers, and tracing system trails in the Web logs and intrusion logs. The tester may also follow system trails from Web postings and bulletin boards.

  Steps include (but are not limited to):

  - Analyzing the traceroute response and mapping the perimeter using Firewalking techniques
  - Using online sources such as Netcraft to find out more about the information systems (IS) infrastructure and historical performance data. Doing so will give server uptime to determine if the latest patch releases have been applied. Verify them.

- **System and service identification through port scans**

  This will essentially result in the identification of live systems and their IP addresses, port states (open, closed, or filtered), protocols used (routing or tunneled), active services and service types, service application types and patch levels, OS fingerprinting, version identification, internal IP addressing, and so on.

  Steps include (but are not limited to):

  - Deploying a connect scan for all hosts on the network. Use this through port 1024 to enumerate ports.
  - Deploying a stealth SYN scan for ports 20, 21, 22, 23, 25, 80, and 443. Extend this scan to live systems to detect port states.
  - Deploying an ACK scan for ports 3100–3150, 10001–10050, and 33500–33550 using TCP port 80 as the source to get past the firewall.
  - Deploying a fragment scan in reverse order with FIN, NULL, and XMAS flags set for ports 21, 22, 25, 80, and 443. Testers use this for enumerating the subset of ports in the default packet fragment testing ports.
  - Deploying FTP bounce and idle scans for ports 22, 81, 111, 132, 137, and 161 to infiltrate the DMZ.
  - Deploying UDP scans to check for port filtering on a small subset.
  - Cataloging all the protocols. Note any tunneled or encapsulated protocols.
  - Cataloging all services identified for ports discovered—whether filtered or not. Note service remapping and system redirects.
  - Cataloging all applications identified using scanners such as Nmap. Additionally, you can retrieve information such as patch level and version fingerprinting.

- **Web profiling**

  This phase will attempt to profile and map the Internet profile of the organization. The information gleaned will be used for later attack techniques such as SQL injection, Web server and application hacking, session hijacking, denial-of–service, and so on.

Steps include (but are not limited to):

- Cataloging all Web-based forms, types of user input, and form-submission destinations
- Cataloging Web privacy data including cookie types (persistent or session), nature and location of information stored, cookie expiration rules, and encryption used
- Cataloging Web error messages, bugs in services, third-party links, and applications; locate the destination

The information collected during the pre-attack phase includes:

- Competitive intelligence
- Network registration information
- DNS and mail-server information
- Operating-system information
- User information
- Authentication of credential information
- Analog connections
- Contact information
- Website information
- Physical and logical location of the organization
- Product range and service offerings of the target company that are available online
- Any other information that has the potential to result in a possible exploitation

Attack Phase

The information gathered in the pre-attack phase forms the basis of the attack strategy. Before deciding on the attack strategy, the tester may choose to carry out an invasive information-gathering process such as scanning.

The attack phase involves the actual compromise of the target. The attacker may exploit a vulnerability discovered during the pre-attack phase or use security loopholes such as a weak security policy to gain access to the system. The important point here is that while the attacker needs only one port of entry, organizations need to defend several. Once inside, the attacker may escalate privileges and install a backdoor to sustain access to the system and exploit it.

During the attack phase, the pen tester needs to:

- Penetrate perimeter
- Acquire target
- Escalate privileges
- Execute, implant, retract

Activity: Perimeter Testing

Social engineering will be an ongoing activity throughout the testing phase. The tests in this context include, but are not limited to, making impersonating or making phone calls to capture sensitive information, verifying information gathered through activities like dumpster diving, and so on. Other means include email testing, trusted-person acquisition, and attempts to

retrieve legitimate authentication details such as passwords and access privileges. The tester can use information gathered here in Web-application testing as well.

- **Firewall Testing**

  Pen-testing team makes use of the information gained during the pre-attack phase using techniques such as Firewalking. They attempt to bypass the IDS and firewall.

  This includes crafting and sending packets to check firewall rules—for example, sending SYN packets to test stealth detection. This will determine the nature of various packet responses through the firewall. Pen testers can use customized TCP/IP packets with different combination of flags to enumerate the target network. This also gives an indication of source port control of the target.

  Usually, perimeter testing measures the firewall's ability to handle fragmentation, big packet fragments, overlapping fragments, a flood of packets, and so on. Testing methods for perimeter security include, but are not limited to, the following techniques:

  - Evaluating error reporting and error management with ICMP probes
  - Checking access control lists with crafted packets
  - Measuring the threshold for denial of service by attempting persistent TCP connections, evaluating transitory TCP connections, and attempting streaming UDP connections
  - Evaluating protocol filtering rules by attempting connection using various protocols such as SSH, FTP, and Telnet
  - Evaluating the IDS capability by passing malicious content (such as malformed URLs) and scanning the target variously in response to abnormal traffic
  - Examining the perimeter security system's response to Web server scans using multiple methods such as POST, DELETE, and COPY

Enumerating Devices

A device inventory is a catalog of network devices with descriptions of each device. During the initial stages of the pen-test, the test team can refer the devices by their identification in the network (such as IP address, MAC address, etc.). They can use device enumeration tools and "ping" all the devices on the network to create an inventory of all the devices.

Later, when there is a physical security check, devices may be cross-checked to verify their location and identity. This step can help identify unauthorized devices on the network. Another method is to perform ping sweeps to detect responses from devices and later correlate the results with the actual inventory.

The following are the likely parameters in an inventory sheet:

- Device ID
- Descriptions
- Hostnames

- Physical locations
- IP addresses and MAC addresses
- Network accessibility

Activity: Acquiring Target

Usually, target acquisition refers to all the activities to unearth as much information as possible about a particular machine or system. Acquiring a target refers to the set of activities in which the tester subjects the target machine to more-intrusive challenges such as vulnerability scans and security assessments. This helps in gaining more information about the target and exploiting it in the exploitation phase.

Examples of such activities include subjecting the machine to the following procedures:

- **Active probing assaults**: This can use results of network scans to gather further information that can lead to a compromise.
- **Running vulnerability scans**: Vulnerability scans are completed in this phase.
- **Trusted systems and trusted process assessment**: This involves attempting to access the machine's resources using legitimate information obtained through social engineering or other means.

Activity: Escalating Privileges

Attacker takes an advantage of bugs, design flaws, or misconfigurations in an operating system or an application to gain elevated access to the normally protected resources from an application or user. Privilege escalation is usually performed by attackers to carry out various malicious activities such as delete files, view sensitive information, or install malicious programs such as Trojans and viruses. Therefore, once the pen tester manages to intrude in to the target system, he or she must attempt to exploit the system and gain further access to protected resources.

Activities include (but are not limited to) the following techniques:

- The tester may take advantage of poor security policies, e-mails, or unsafe Web code to gather information that can lead to escalation of privileges.
- Use of techniques such as brute force to achieve privileged status. Tools for this purpose include GetAdmin and password crackers.
- Use of Trojans and protocol analyzers.
- Use of information gleaned through techniques such as social engineering to gain unauthorized access to privileged resources.

Activity: Execute, Implant, and Retract

In this phase, the tester effectively compromises the acquired system by executing arbitrary code. The objective here is to explore the extent to which security fails. The tester will attempt to execute arbitrary code, hide files in the compromised system, and leave the system without

raising alarms. The tester will then attempt to reenter the system stealthily. Activities include the following processes:

- Executing exploits already available or specially crafted to take advantage of the vulnerabilities identified in the target system.
- Subjecting the system to denial-of-service attacks. This can be carried out in the previous phase as well.
- Exploiting buffer overflows in order to trick the system into running arbitrary code. The tester may spawn a remote shell, and attempt to upload files and conceal them within the system.
- The tester may also use viruses, Trojans, and rootkits that take advantage of vulnerabilities to exploit the system. Establishing a rootkit or a Trojan that can lead to access more critical systems can also be part of the testing process.
- Erasing logs files or camouflaging modifications to escape legal ramifications. Activities in the retract phase include manipulation of audit log files to remove traces of the activities. Examples include use of tools such as Auditpol. The tester may also change system settings to remain inconspicuous during a reentry, change of log settings, and so on.
- Reentering the system by using the backdoor implanted by the tester.

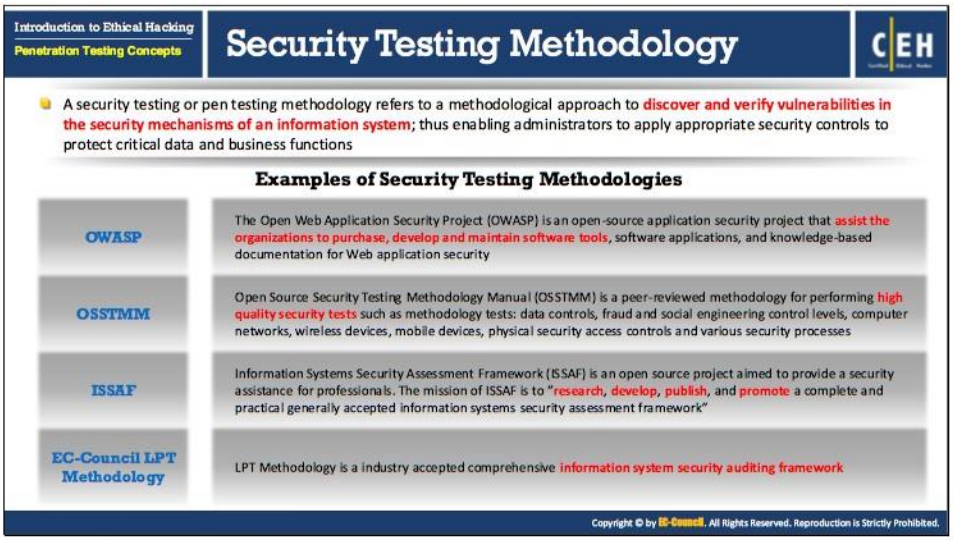
Post-Attack Phase

The post-attack phase includes reporting, cleaning and artifact destruction. This phase is critical to any penetration test, as it is the responsibility of the tester to restore the systems to the pretest state. The objective of the test is to show where security fails, and unless there is a scaling of the penetration test agreement, whereby the tester is assigned the responsibility of correcting the security posture of the systems, this phase must be completed.

Activities in this phase include (but are not restricted to) the following:

- Removing all files uploaded onto the system
- Cleaning all registry entries and removing vulnerabilities created
- Reversing all files and setting manipulations done during the test
- Reversing all changes in privileges and user settings
- Removing all tools and exploits from the tested systems
- Restoring the network to the pretest stage by removing shares and connections
- Mapping the network state
- Documenting and capturing all logs registered during the test
- Analyzing all results and presenting them in the form of reports to the organization

It is important that the penetration tester document all activities and record all observations and results, so that the test can be repeated and verified for the given security posture of the organization. For the organization to quantify the security risk in business terms, it is essential that the tester identifies critical systems and critical resources, and maps the threats to both.



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.

The cornerstone of a successful penetration test is the methodology involved in devising it. The underlying methodology should help the tester by providing a systematic approach to the testing pattern. The consistency, accuracy, and efficiency of the test must be met and should be up to the mark of the testing methodology. This does not mean that the entire framework should be restrictive, however.

The following are two important types of penetration testing methodologies:

Proprietary Methodologies

There are many organizations that work on penetration testing and who offer services and certifications. These network-security organizations have their own methodologies that are kept confidential.

Examples of some proprietary methodologies are:

- **IBM:** Express penetration testing services from IBM Security Services help mid-market organizations quickly assess the security posture of their networks by safely identifying network vulnerabilities before they are exploited.
- **McAfee Foundstone:** McAfee Foundstone guides enterprises on the best ways to protect assets and maximize business goals through maintaining a strong security posture.

- **EC-Council LPT:** LPT methodology is an industry accepted comprehensive information system security auditing framework.

Open-Source and Public Methodologies

There is a wide range of methodologies that are publicly available. Anyone can use these methodologies. The following methodologies can be accessed online:

- **OWASP**

  OWASP is the Open Web Application Security Project, which 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. It provides a set of tools and a knowledge base, which help in protecting Web applications and services. It is beneficial for system architects, developers, vendors, consumers, and security professionals who might work on designing, developing, deploying, and testing the security of Web applications and Web services.

- **OSSTMM**

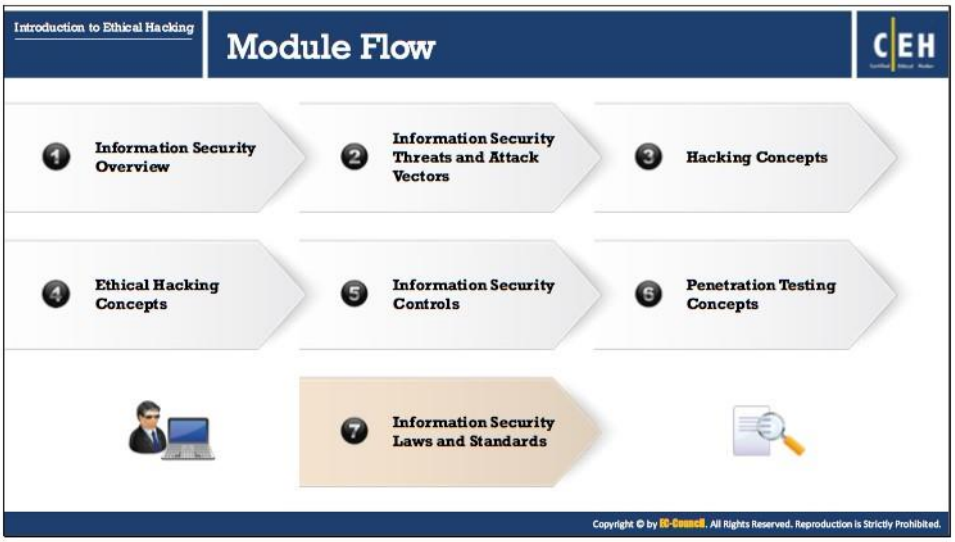
  OSSTMM is the Open-Source Security Testing Methodology Manual, compiled by Pete Herzog. It is a peer-reviewed methodology for performing high quality security tests such as methodology tests: data controls, fraud and social engineering control levels, computer networks, wireless devices, mobile devices, physical security access controls and various security processes. OSSTMM is a standard set of penetration tests to achieve security metrics. It is considered to be a de facto standard for the highest level of testing, and it ensures high consistency and remarkable accuracy.

- **ISSAF**

  Information Systems Security Assessment Framework (ISSAF) is an open source project aimed to provide in-depth information about how to conduct a penetration test. It is supported by the Open Information Systems Security Group (OISSG). The mission of ISSAF is to "research, develop, publish, and promote a complete and practical generally accepted information systems security assessment framework."

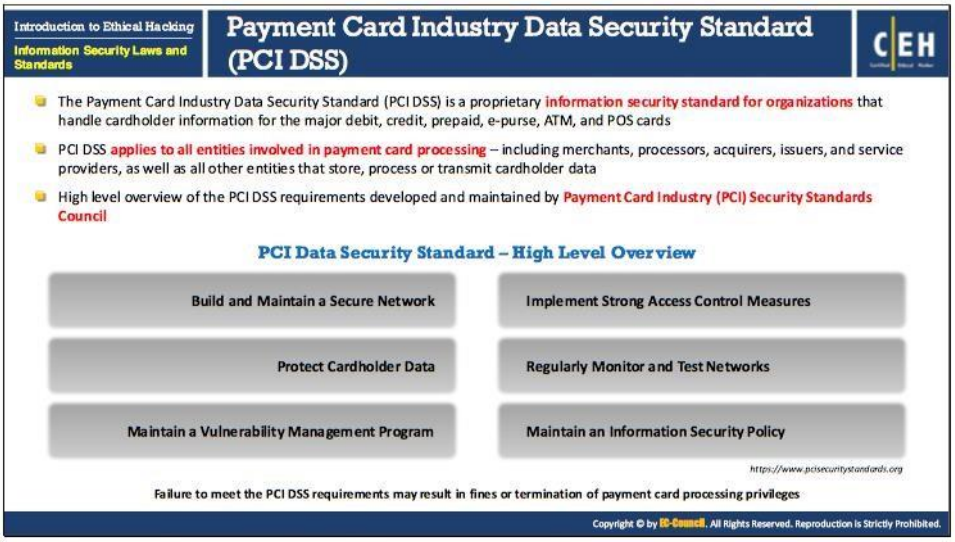
- **NIST**

  The National Institute of Standards and Technology (NIST) is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.



Information Security Laws and Standards

Laws function as a system of rules and guidelines enforced by a particular country or community to govern behavior. A Standard is a "document established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. This section deals with various laws and standards pertaining to information security in different countries.



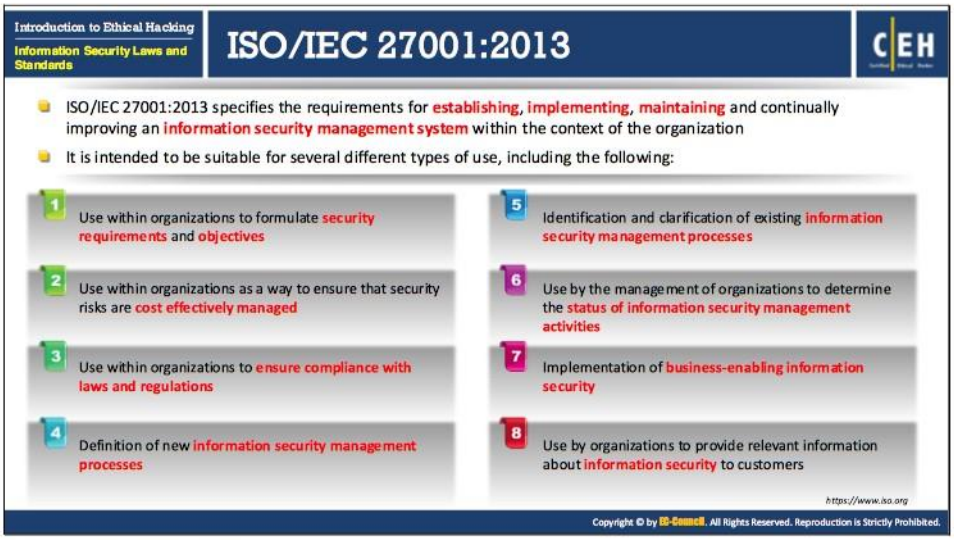
Payment Card Industry Data Security Standard (PCI DSS)

Source: *https://www.pcisecuritystandards.org*

The 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. This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. 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 DSS comprises a minimum set of requirements for protecting cardholder data. High-level overview of the PCI DSS requirements developed and maintained by the PCI Security Standards Council.

Build and Maintain a Secure Network	▪ Install and maintain a firewall configuration to protect cardholder data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	▪ Protect stored cardholder data ▪ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	▪ Use and regularly update anti-virus software or programs ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ Restrict access to cardholder data by business need to know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain a policy that addresses information security for all personnel

TABLE 1.3: Table Showing the PCI Data Security Standard - High Level Overview



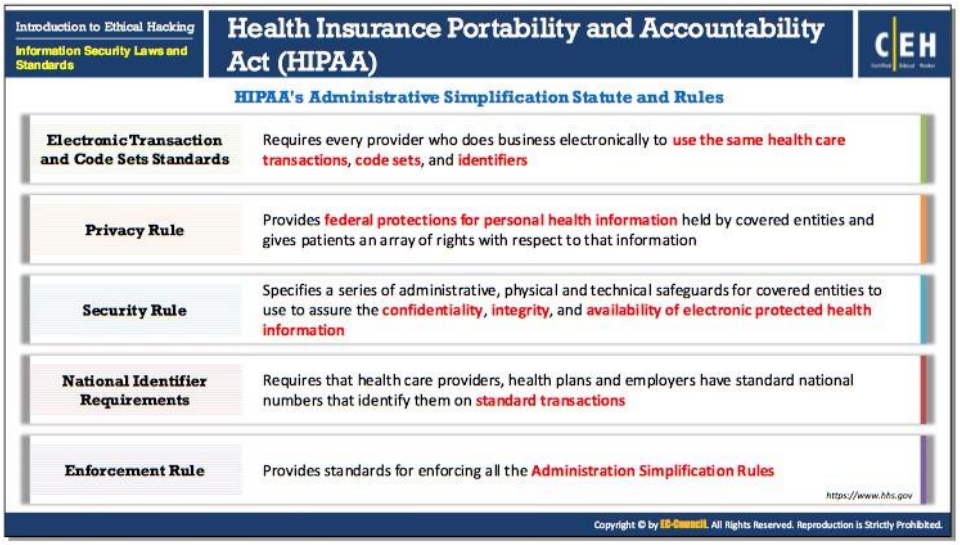
ISO/IEC 27001:2013

Source: *https://www.iso.org*

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



Health Insurance Portability and Accountability Act (HIPAA)

Source: *https://www.hhs.gov*

The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other important purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

The office of civil rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below:

- **Electronic Transaction and Code Sets Standards**

  Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) named certain types of organizations as covered entities, including health plans, health care clearinghouses, and certain health care providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for Electronic Data Interchange (EDI) of health care data. These transactions are claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits and premium payment. Under HIPAA, if a covered entity conducts one of the adopted transactions electronically, they must use the adopted standard—either from ASC X12N or NCPDP (for certain pharmacy transactions). Covered

entities must adhere to the content and format requirements of each transaction. It requires every provider, who does business electronically, to use the same health care transactions, code sets and identifiers.

- **Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses and those health care providers who conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

- **Security Rule**

  The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

- **Employer Identifier Standard**

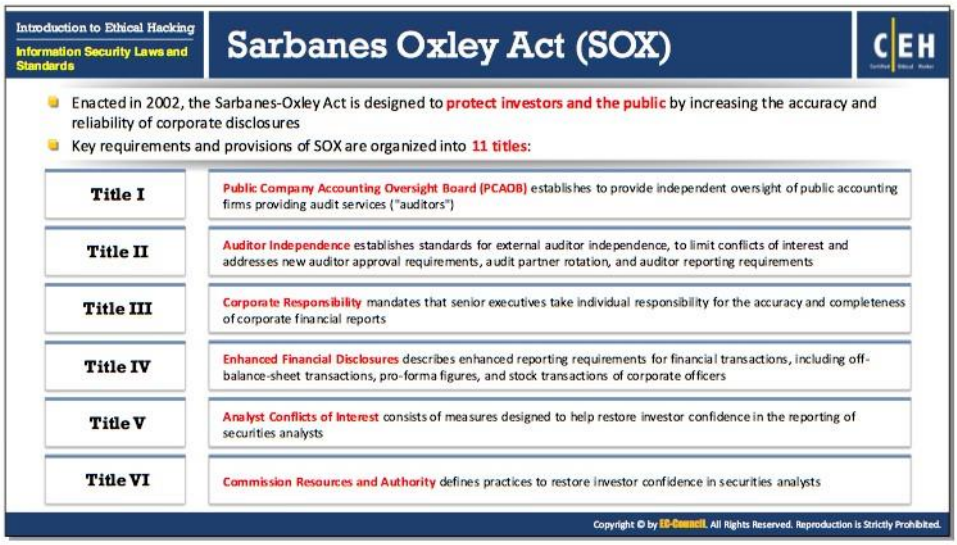
  The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that employers have standard national numbers that identify them on standard transactions.

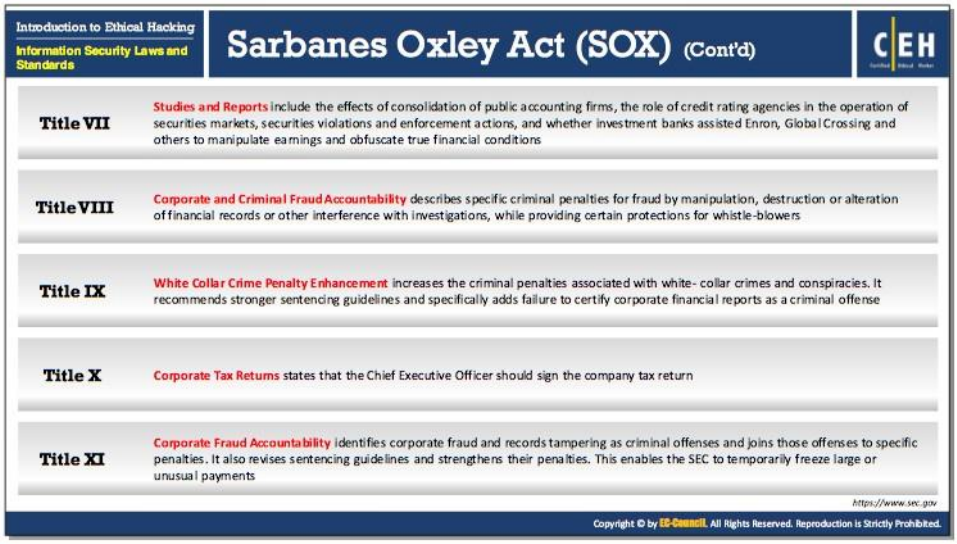
- **National Provider Identifier Standard (NPI)**

  The National Provider Identifier (NPI) is a Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard. The NPI is a unique identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

- **Enforcement Rule**

  The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.





Sarbanes Oxley Act (SOX)

Source: *https://www.sec.gov*

Enacted in 2002, the Sarbanes-Oxley Act aims to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. This act does not explain how an organization needs to store records, but describes records that organizations need to store and

the duration of the storage. The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud.

Key requirements and provisions of SOX are organized into 11 titles:

- **Title I: Public Company Accounting Oversight Board (PCAOB)**

  Title I consists of nine sections and establishes the Public Company Accounting Oversight Board, to provide independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

- **Title II: Auditor Independence**

  Title II consists of nine sections and establishes standards for external auditor independence, to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (e.g., consulting) for the same clients.

- **Title III: Corporate Responsibility**

  Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

- **Title IV: Enhanced Financial Disclosures**

  Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports.

- **Title V: Analyst Conflicts of Interest**

  Title V consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

  Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities

professionals from practice and defines conditions to bar a person from practicing as a broker, advisor, or dealer.

- **Title VII: Studies and Reports**

  Title VII consists of five sections and requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and report their findings. 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**

  Title VIII, also known as the "Corporate and Criminal Fraud Accountability Act of 2002," consists of seven sections. It describes specific criminal penalties for 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**

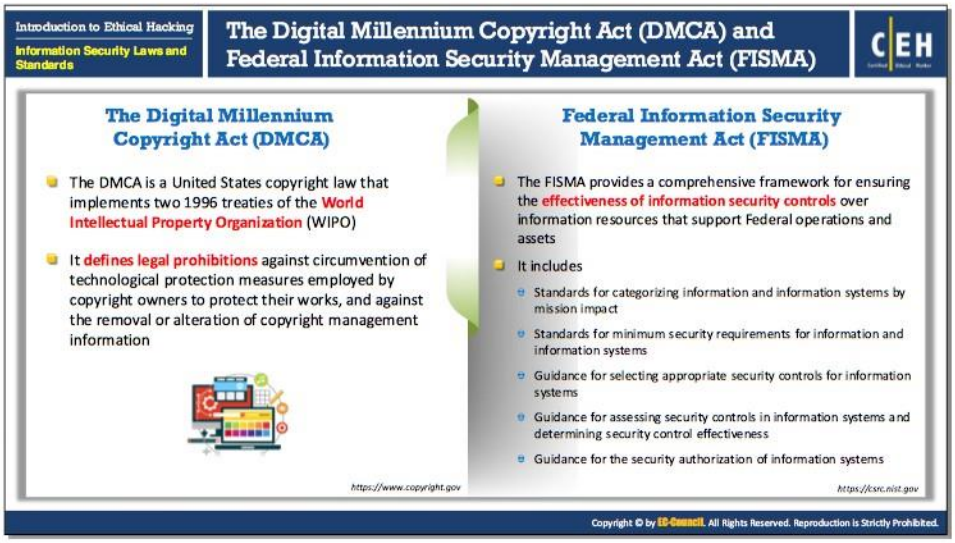
  Title IX, also known as the "**White Collar Crime Penalty Enhancement Act of 2002**," consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

- **Title X: Corporate Tax Returns**

  Title X consists of one section and states that the Chief Executive Officer should sign the company tax return.

- **Title XI: Corporate Fraud Accountability**

  Title XI consists of seven sections. Section 1101 recommends the following name for this title: "**Corporate Fraud Accountability Act of 2002**." It 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 resort to temporarily freezing "large" or "unusual" transactions or payments.



The Digital Millennium Copyright Act (DMCA)

Source: *https://www.copyright.gov*

The DMCA is a United States of America's copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. 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 in order to implement US treaty obligations. The DMCA contains five titles:

- **Title I: WIPO TREATY IMPLEMENTATION**

  Title I implements the WIPO treaties. First, it makes certain technical amendments to US law, in order to provide appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

- **Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

  Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. A service provider bases the limitations on the following four categories of conduct:

  - Transitory communications
  - System caching
  - Storage of information on systems or networks at direction of users

- Information location tools

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

- **Title III: COMPUTER MAINTENANCE OR REPAIR**

Title III of the DMCA allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

- **Title IV: MISCELLANEOUS PROVISIONS**

Title IV contains six miscellaneous provisions, where the first provision provides Clarification of the Authority of the Copyright Office; the second provision grants exemption for the making of "ephemeral recordings"; the third provision promotes distance education study; the fourth provision provides exemption for Nonprofit Libraries and Archives; the fifth provision allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and the sixth provision addresses concerns about the ability of writers, directors and screen actors to obtain residual payments for the exploitation of motion pictures in situations where the producer is no longer able to make these payments.

- **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

Title V of the DMCA, entitles the Vessel Hull Design Protection Act (VHDPA). It creates a new system for protecting original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, "useful articles" are limited to the hulls (including the decks) of vessels no longer than 200 feet.

Federal Information Security Management Act (FISMA)

Source: *https://csrc.nist.gov*

FISMA is the Federal Information Security Management Act of 2002 to produce several key security standards and guidelines required by Congressional legislation. The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The FISMA framework 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

Introduction to Ethical Hacking
Information Security Laws and Standards

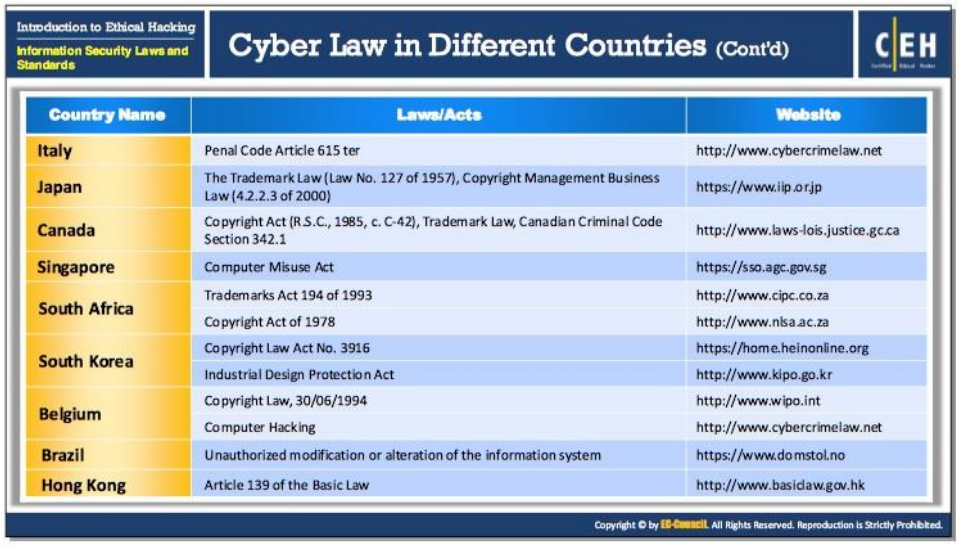
Cyber Law in Different Countries

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

Introduction to Ethical Hacking
Information Security Laws and Standards

Cyber Law in Different Countries (Cont'd)

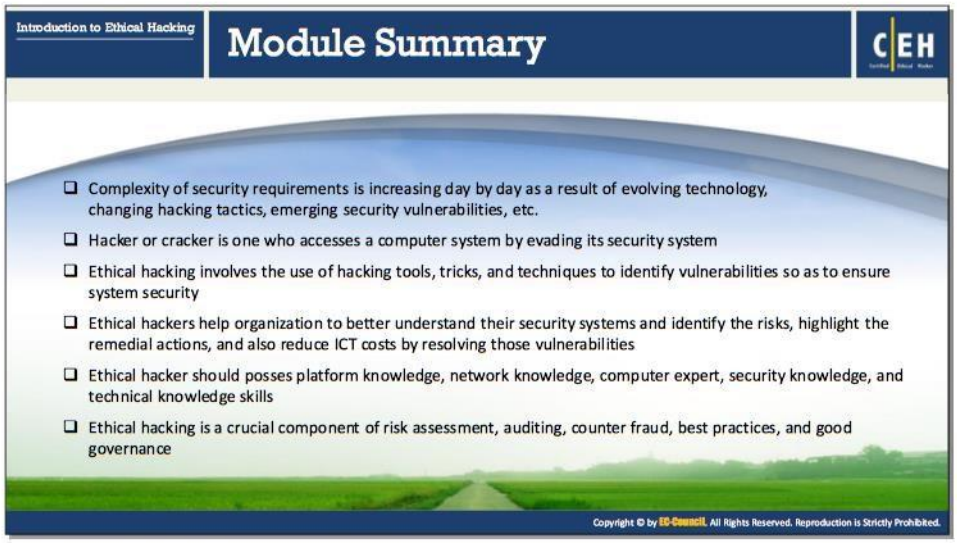
Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994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



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)	https://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	https://sso.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	https://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	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	http://www.basiclaw.gov.hk

Cyber Law in Different Countries

Cyber law or Internet law refers to any laws that deal with protecting the Internet and other online communication technologies. Cyber law covers topics such as Internet access and usage, privacy, freedom of expression, and jurisdiction. Cyber laws provide the assurance of the integrity, security, privacy, and confidentiality of information in both government and private organizations. These laws have become prominent due to increase in the Internet use all over the world. Cyber laws vary by jurisdiction and country, so implementing these laws is quite challenging. Violating these laws result in punishments ranging from fines to imprisonment.



Module Summary

This module ends with an overview discussion of fundamental information security concepts. The next module will include a discussion on how attackers, ethical hackers, and pen-testers perform reconnaissance to collect information about a target of evaluation before an attack or audit.