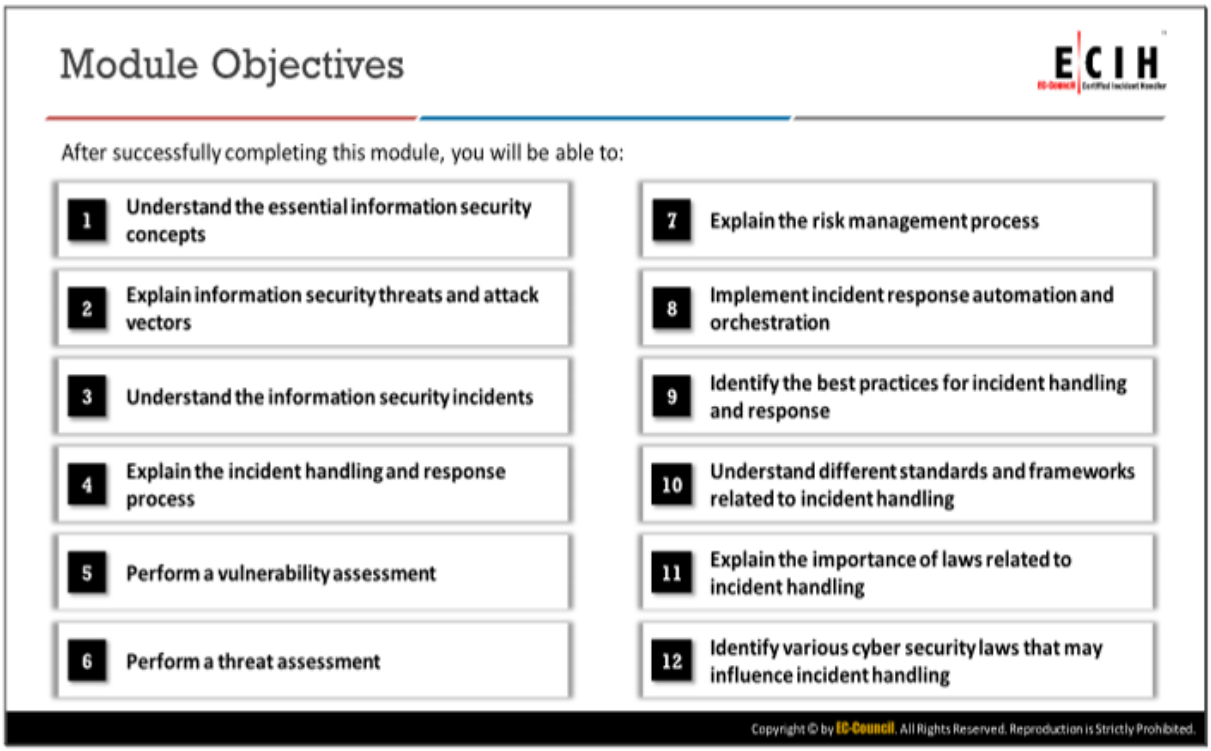
Module 01

Introduction to Incident Handling and Response

This page is intentionally left blank.



Module Objectives

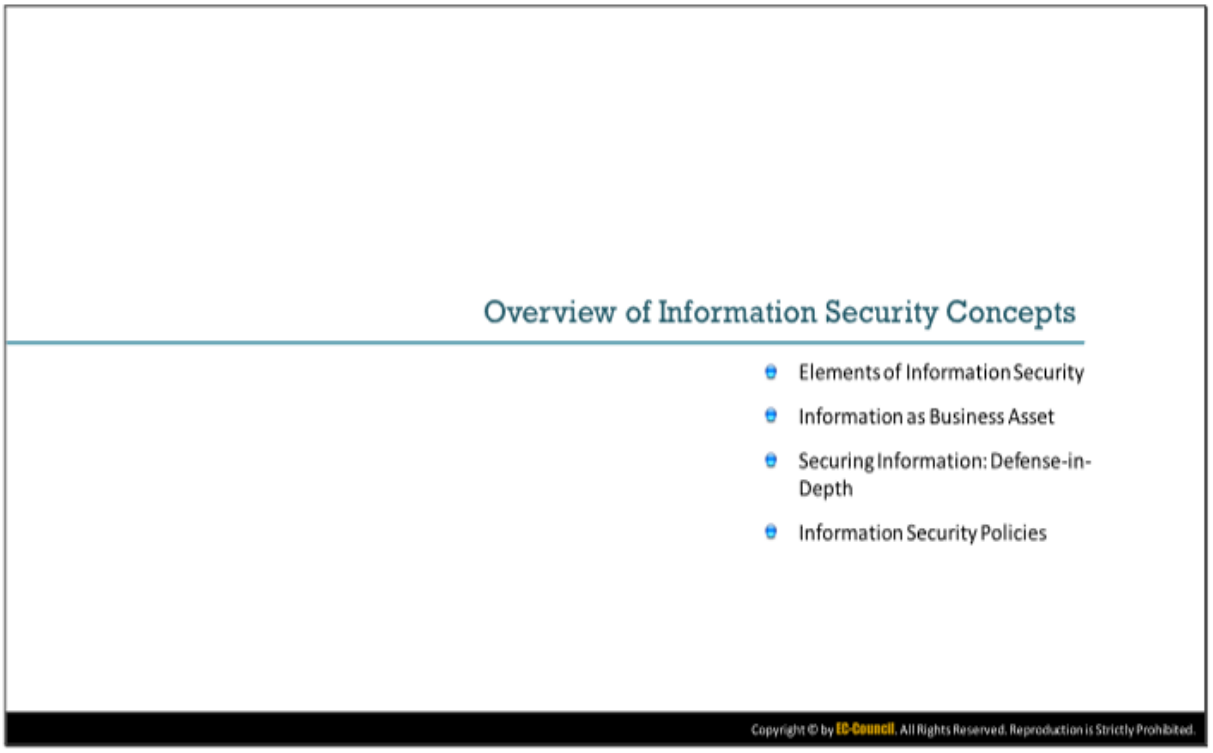
The ever-evolving, complex cyber threat landscape, security breaches, and data theft have led organizations to recognize the importance of properly handling and responding to security incidents. Handling these incidents efficiently and effectively, in a planned manner, helps organizations minimize the impact caused, mitigate the exploited vulnerabilities, restore the affected services and processes, reduce the risk of future threats, and enhance their cyber defense strategy. Further, planning incident response keeps organizations prepared for various known and unknown threats and establishes a reliable method of identifying security incidents in a timely way.

This module starts with an overview and discussion of essential information security concepts. It explains in detail the various information security threats and attack vectors. Besides discussing information security incidents, signs of an incident, and costs of incidents, it gives an overview of the incident management process and the vulnerability management process, along with the classification of vulnerabilities. In addition, it explains the threat assessment process, threat intelligence, threat contextualization, threat correlation, and threat attribution, as well as discussing the risk management process and the steps involved in risk assessment. Next, it gives an overview of incident response automation and orchestration as well as introduces best practices for incident handling and response (IH&R) and the various standards and frameworks related to incident handling. In conclusion, it explains the importance of laws in incident handling and the various laws that may influence the incident handling process.

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

- Understand the essential information security concepts
- Explain information security threats and attack vectors

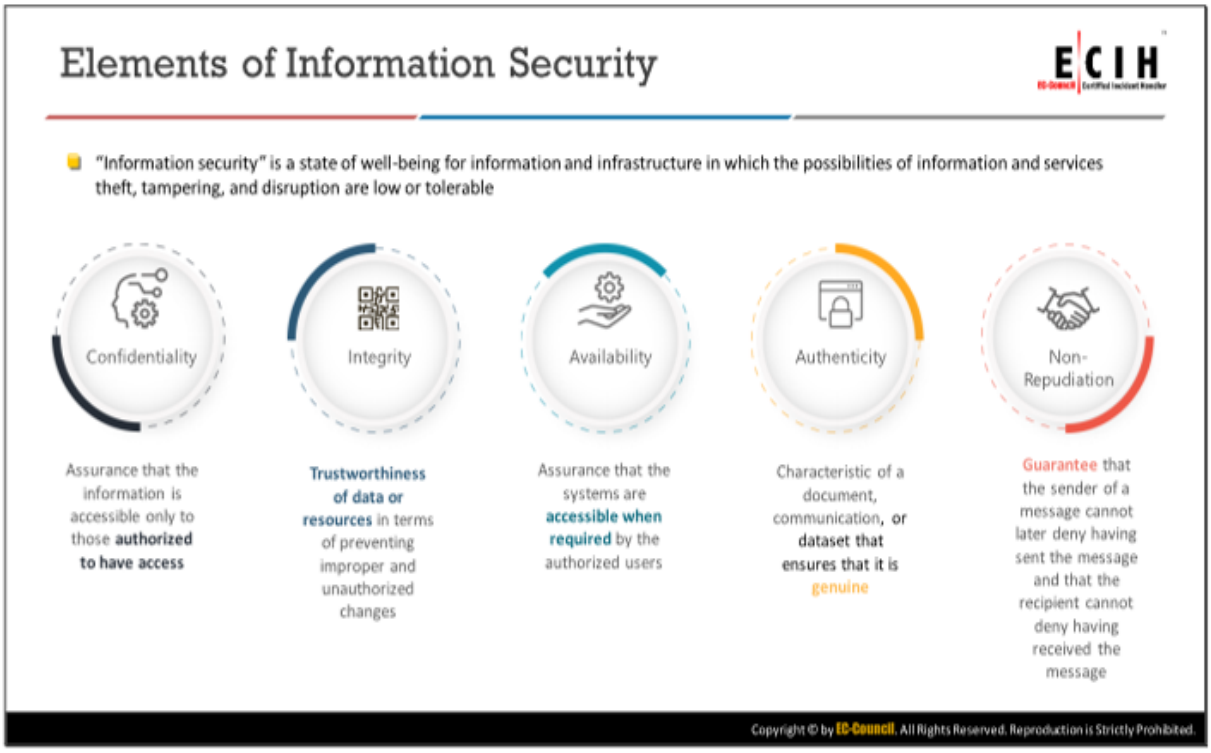
- Understand information security incidents along with their signs and cost
- Explain the IH&R process
- Perform vulnerability assessment
- Perform threat assessment
- Explain the risk management process
- Implement incident response automation and orchestration
- Identify the best practices for incident handling and response
- Understand different standards and frameworks related to incident handling
- Explain the importance of laws in incident handling
- Identify various cybersecurity laws that may influence incident handling



Overview of Information Security Concepts

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

This section discusses the elements of information security and how information is considered as a business asset. It also gives an overview of defense-in-depth and information security policies.



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. It plays a major role in securing sensitive information from unauthorized access. Confidentiality breaches may occur due to improper data handling or a successful hacking attempt. To prevent such breaches organizations need to implement confidentiality controls, such as data classification, data encryption, setting passwords, multifactor authentication, biometric verification, security tokens, and key fobs.

- **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 system disk arrays and clustered machines, antivirus software to stop malware from destroying networks, and distributed-denial-of-service (DDoS) prevention systems.

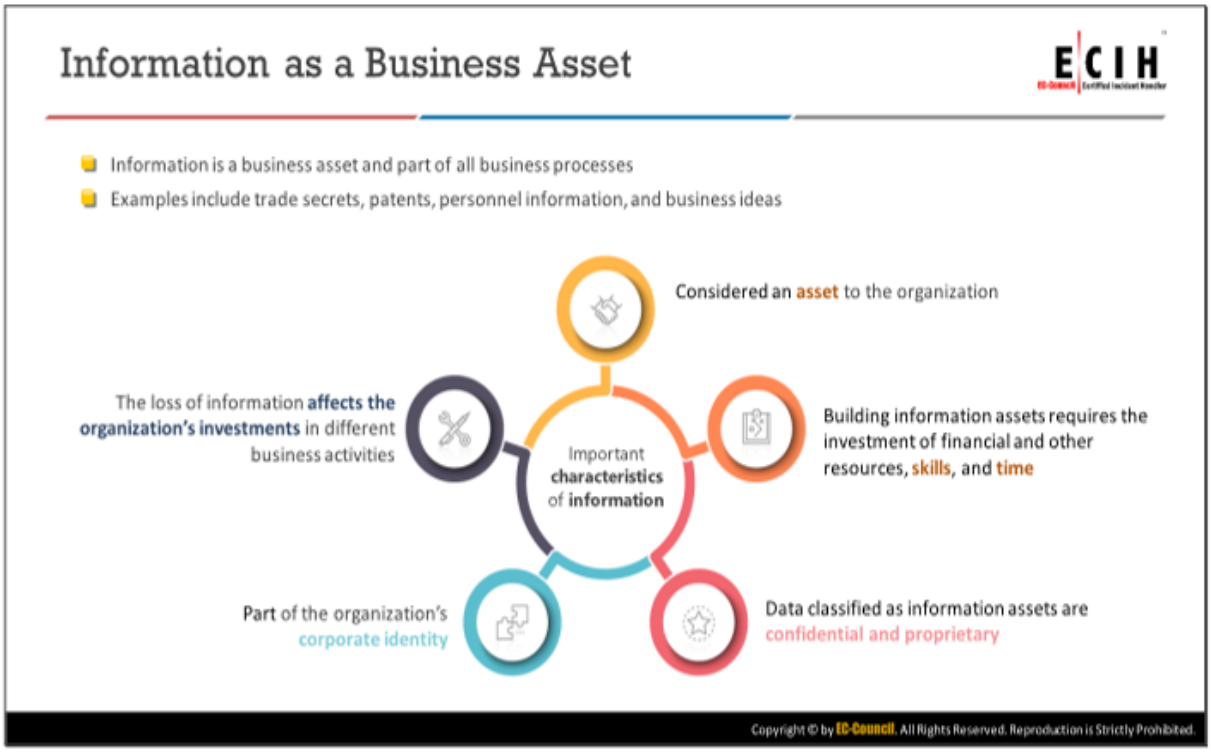
- **Authenticity**

  Authenticity refers to the genuineness or uncorruptedness of any communication, document, or data. The major role of authentication is to confirm that a user is who he or 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 organizations use digital signatures to ensure non-repudiation.

Note: Confidentiality, integrity, and availability are together referred to as the CIA triad.



Information as a Business Asset

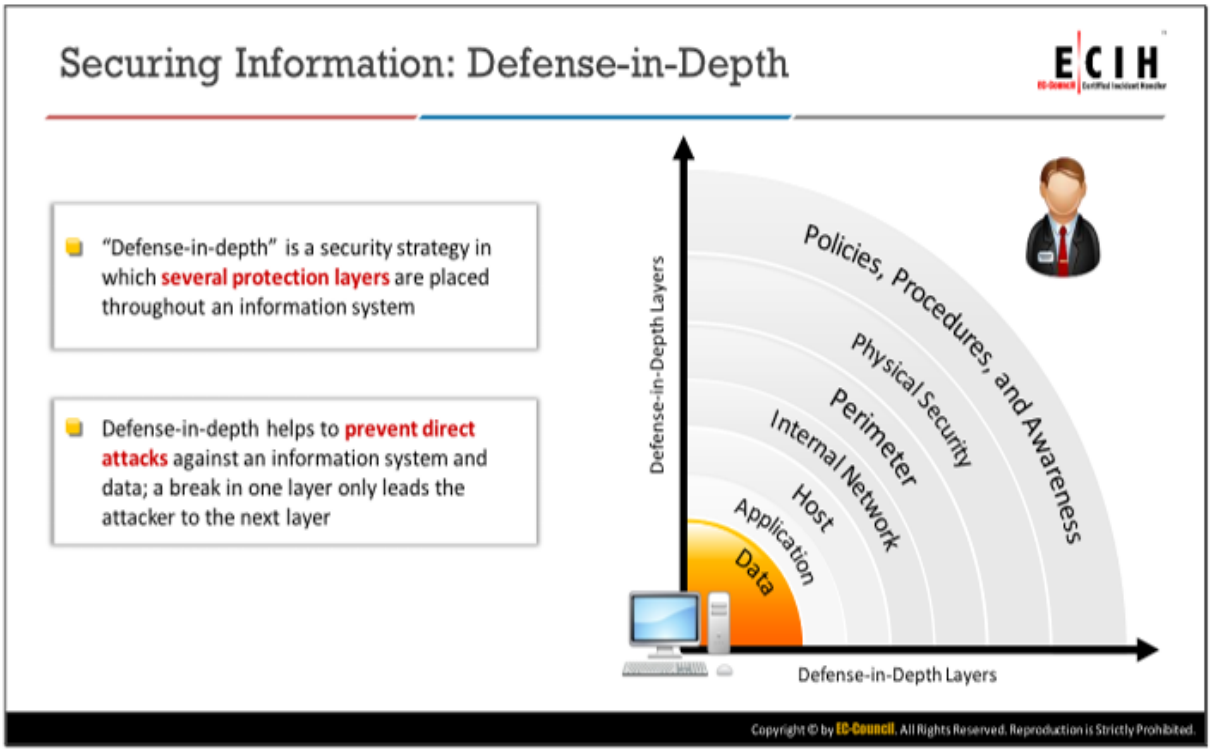
Information is an essential commodity for a business, and an information asset can be defined as a piece of information identified as important to an organization. Information assets or intellectual property are generally accumulated by means of long-term, coordinated efforts, and require significant investment of time and resources. These assets are the backbone of business operations and help the organization to remain business competitive. Secure business-critical information provides businesses with continuity assurance.

Information assets may include trade secrets, patent information, new techniques, management concepts, employee/personnel information, or any other information that if leaked can negatively affect the organization's business environment. Loss of such critical information assets may indeed result in large financial losses and may jeopardize the organization's survival; therefore, organizations must protect their critical information to assure business continuity.

Important characteristics of an information asset of an organization include the following:

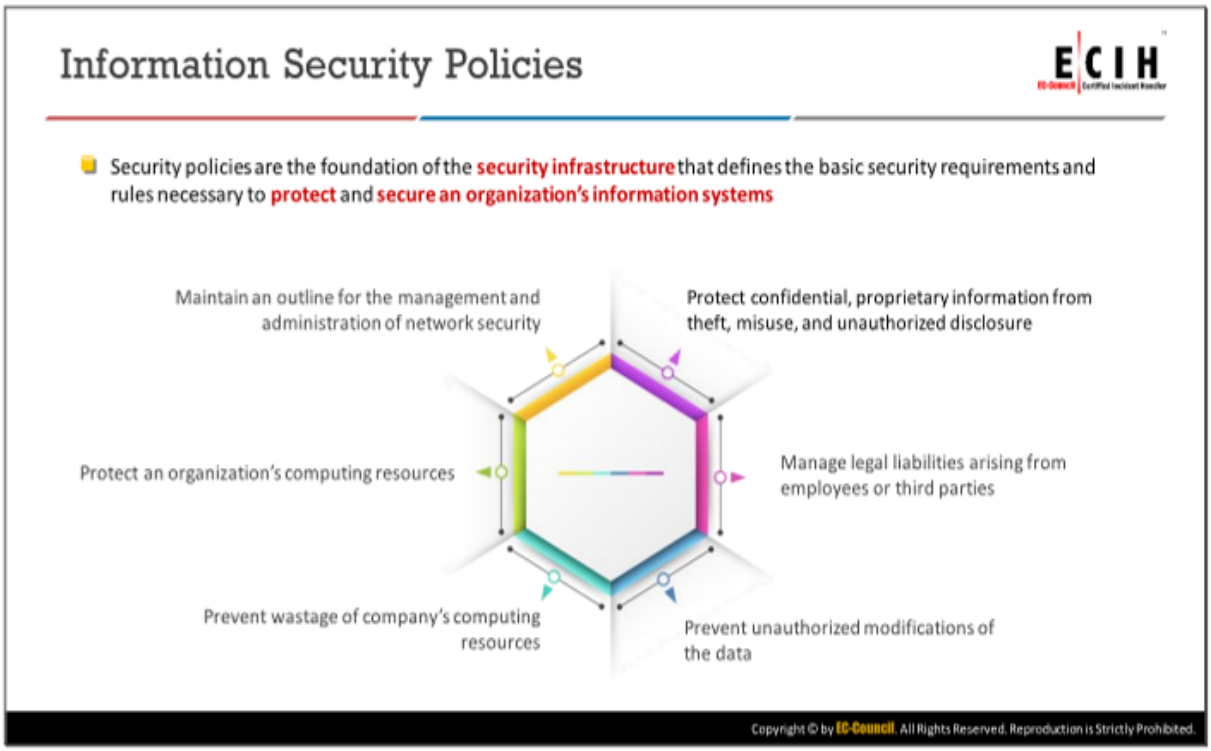
- It is recognized to be of value to the organization.
- It is considered an asset to the organization.
- It is difficult to replace the information without cost, skills, time, and resources.
- It is part of the organization's corporate identity.
- Data classified as an information asset are confidential and proprietary.
- It plays a significant role in the organization's business.
- It is any organized documentation that motivates the organization to achieve its goals.

- It is maintained by people working in a consistent and cooperative manner.
- It can be part of a unique enterprise application or part of one.
- The loss of information affects the organization's investments in different business activities.



Securing Information: 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 multilayered 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 an 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 be implemented 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.

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; that is, management should take into consideration the areas in which security is most important and prioritize its actions accordingly, but it is also very important to look into each individual department for possible security breaches and ways to protect against them. The following information security systems in an organization might require particular attention in terms of security:

- Encryption mechanisms

- Access control devices
- Authentication systems
- Firewalls
- Antivirus systems
- Websites
- Gateways
- Routers and switches

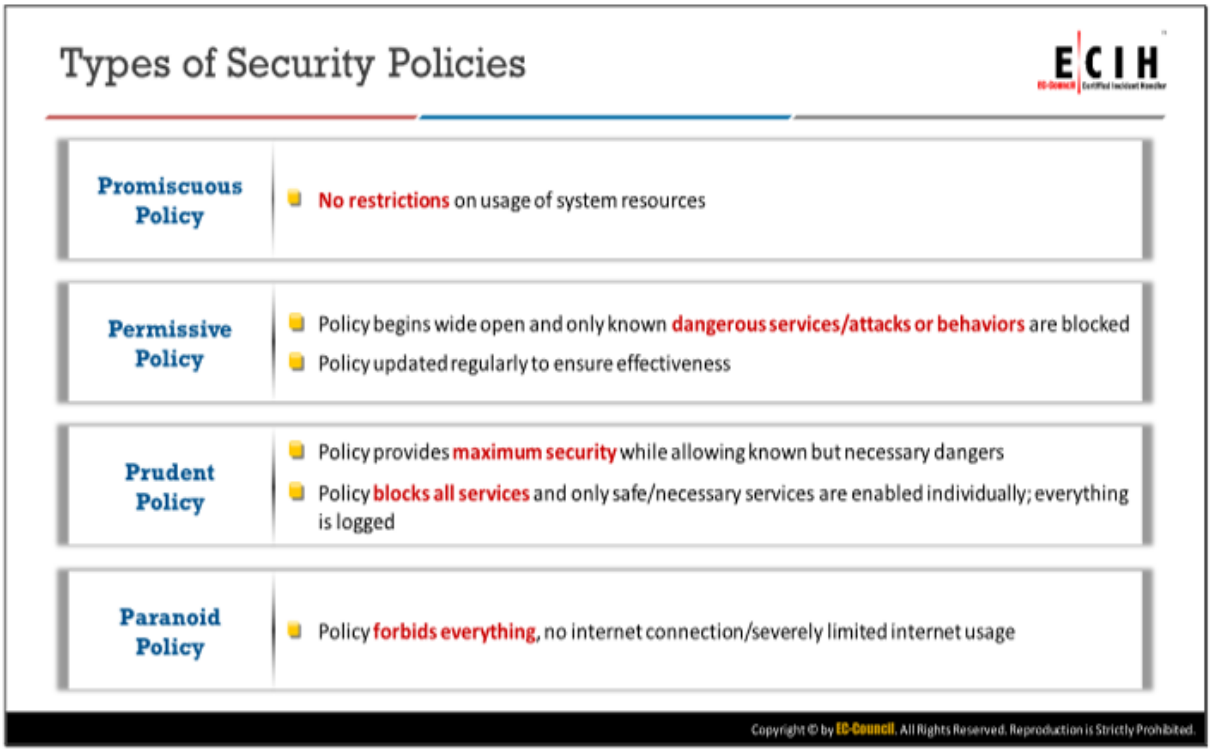
There are two types of security policies: technical security and administrative security policies. Technical security policies describe the configuration of the technology for convenient use; administrative security policies address how all persons should behave. All employees must be required to agree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

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

- Director of Information Security
- Chief Security Officer

The following are the usual 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 the 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 company's 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 company computer or 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 organizational networks, many malware, virus, and Trojan threats are present on the internet, and with 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**

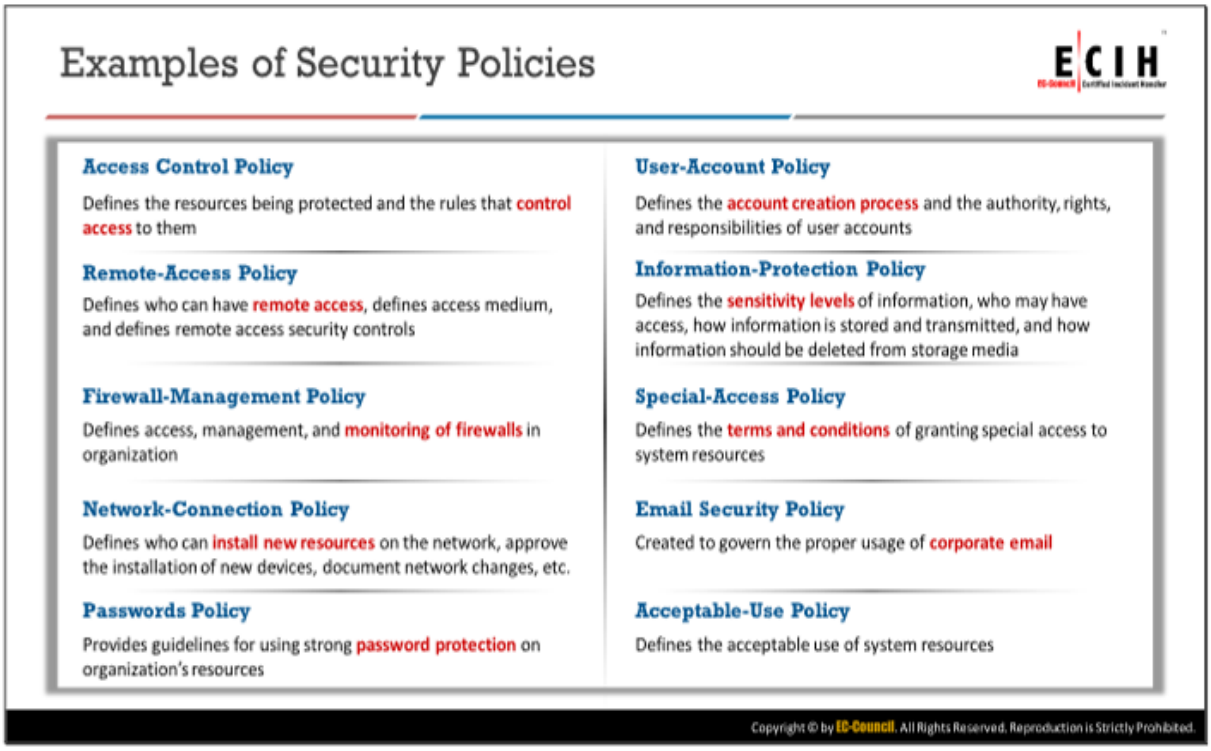
  This policy starts from a wide-open base, and the majority of internet traffic is accepted, but known dangerous services and cyberattacks are blocked. Because only known attacks and exploits are blocked, it is impossible for administrators to keep up with current exploits; they are always playing catch-up with new attacks and exploits. This policy should thus be updated regularly to be effective.

- **Prudent Policy**

  A prudent policy starts with all services blocked, and the administrator enables safe and necessary services individually. Under such a policy, the system logs everything like system and network activities. It provides maximum security, 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. When faced with these overly severe restrictions, users often try to find ways around them.



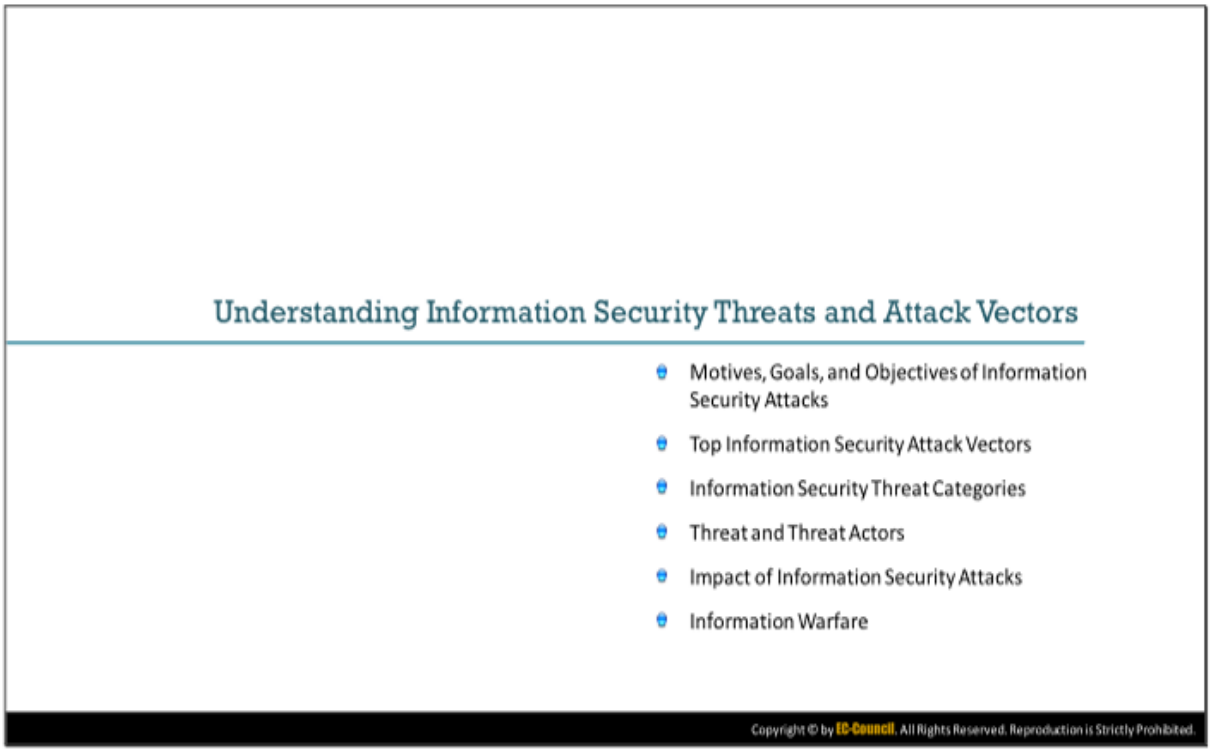
Examples of Security Policies

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

- **Access Control Policy:** An access control policy outlines procedures that help in protecting organizational resources and the rules that control access to them. It enables organizations to better track their assets.
- **Remote-Access Policy:** A remote-access policy contains a set of rules that defines 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 out and in 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 email traffic. This policy describes how to manage, monitor, protect, and update firewalls in the organization. It identifies network applications and the 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 and approve the installation of new devices, document network changes, and so on.

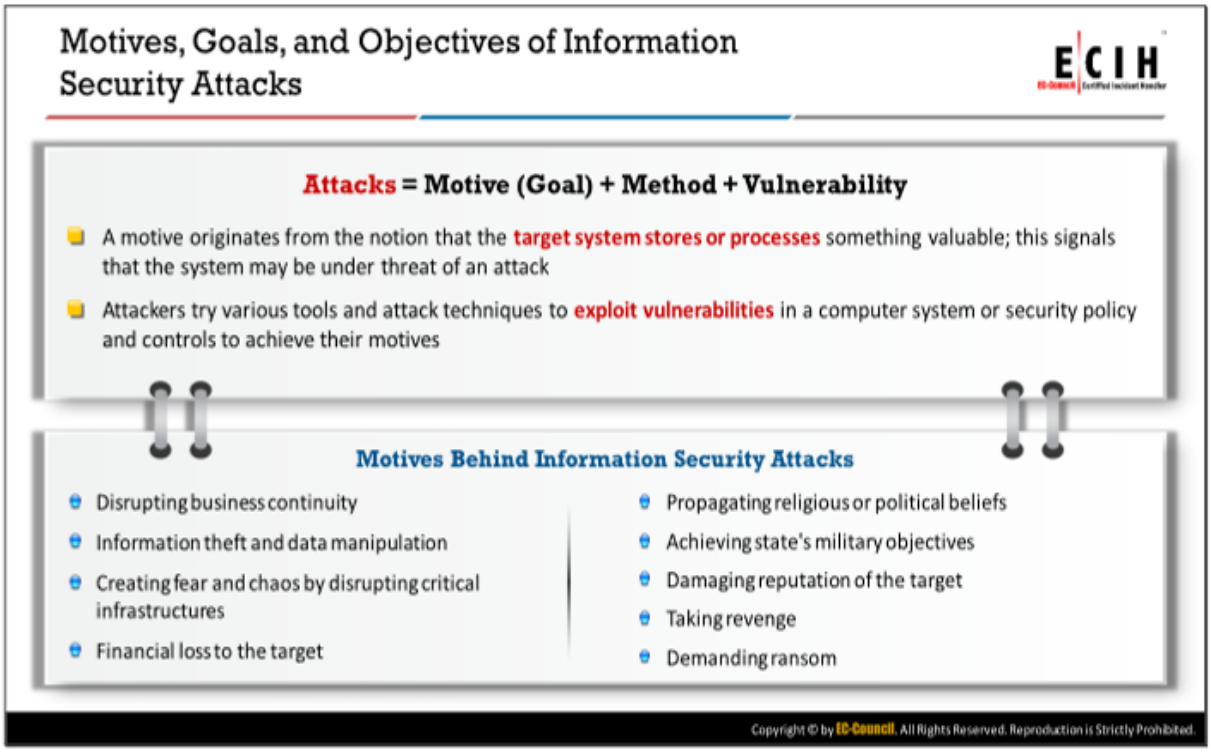
- **Password Policy:** A password policy is a set of rules framed to increase system security by encouraging users to employ strong passwords to access an organization's resources and to keep them secure.
- **User Account Policy:** A user account policy provide guidelines to secure access to a system. It defines the account creation process and the authority, rights, and responsibilities of user accounts. It outlines the requirements for accessing and maintaining accounts on a system. This is especially important for large websites for which users may have accounts on many systems. Users (user account owners) have to read and sign an account policy.
- **Information-Protection Policy:** An information-protection policy defines standards to reduce the danger of misuse, destruction, and/or loss of confidential information. It defines the sensitivity level(s) of information, who may have access, how it is stored and transmitted, and how it should be deleted from storage media. It gives guidelines on the processing, storage, and transfer of 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 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 (often by asking employees to report when unknown or offensive emails are received), to minimize company liability for employees' actions, and to most effectively educate employees in email etiquette.
- **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 users' responsibility to protect the information available in their accounts.



Understanding 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, and botnets, that might affect an organization's information security.

This section introduces the motives, goals, and objectives of information security attacks, top information security attack vectors, information security threat categories, threat and threat actors, and information warfare.



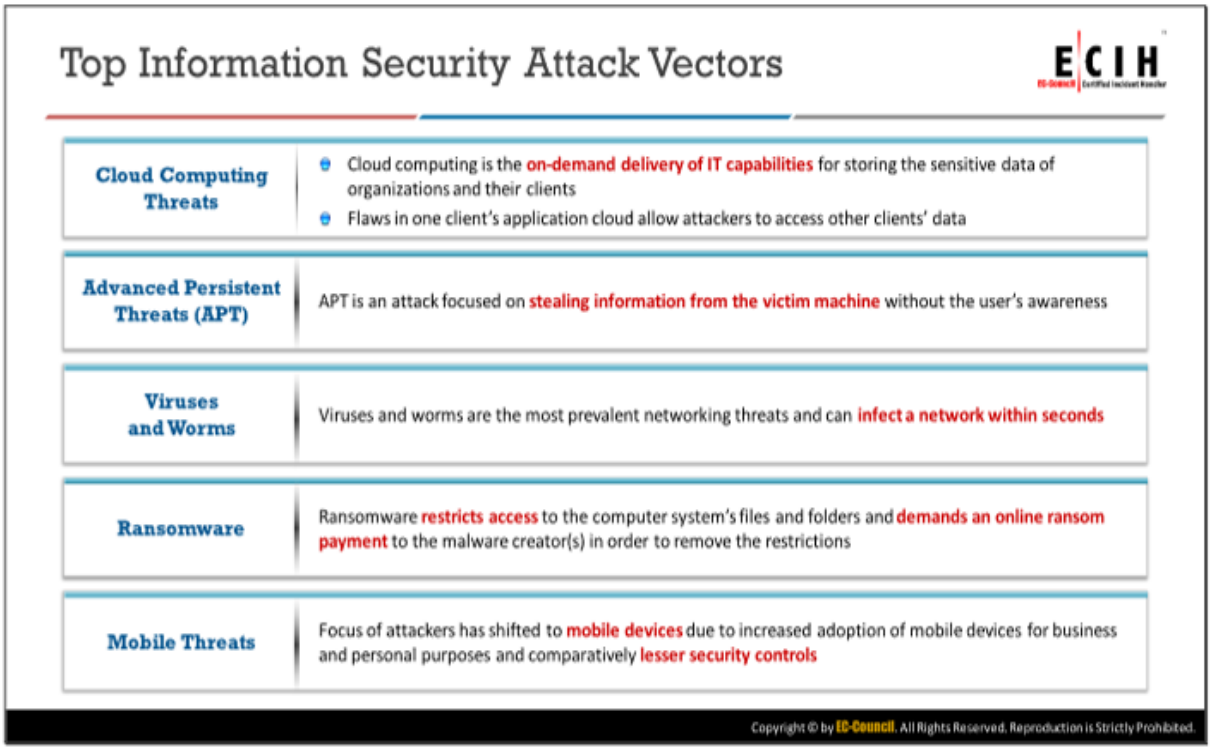
Motives, Goals, and Objectives of Information Security Attacks

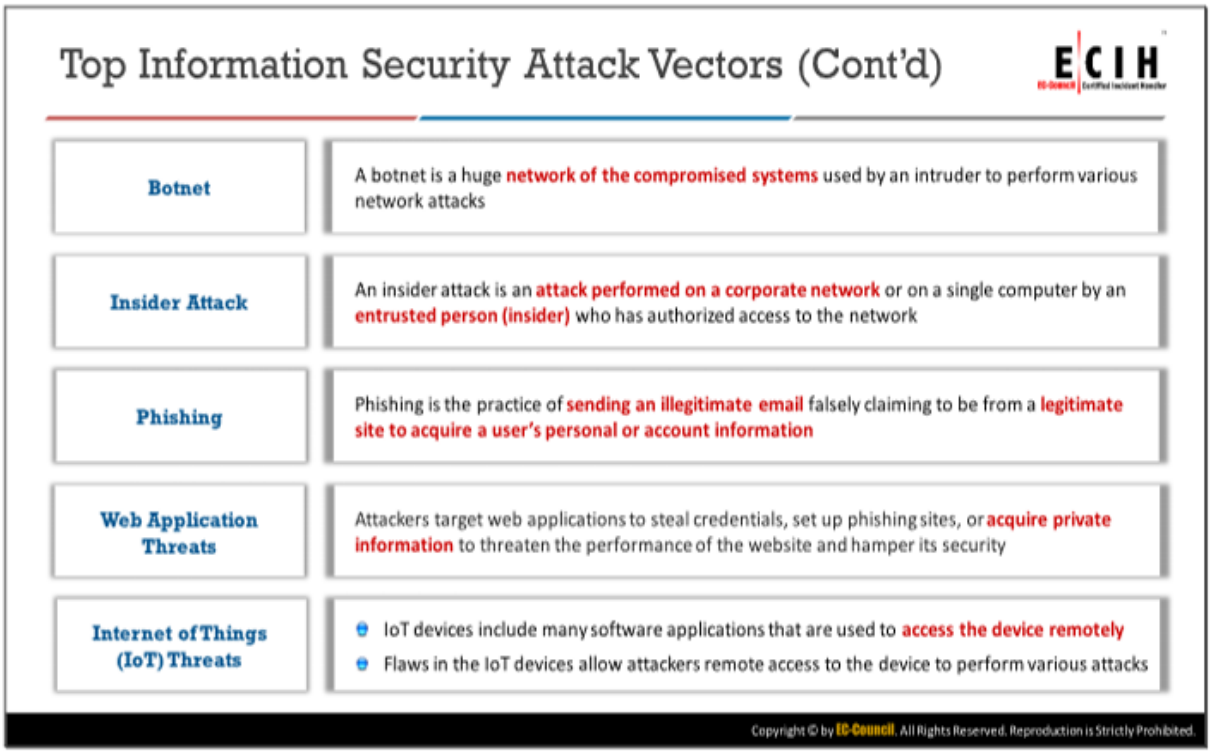
Information security attackers generally have motives (goals) and objectives behind their attacks. A motive may originate out of the notion that a target system stores or processes something valuable, which leads to the threat of an attack on the system. The purpose of the attack may be to disrupt the target organization's business operations, to steal valuable information for the sake of curiosity, or even to exact revenge. Thus, these motives or goals depend on the attacker's state of mind, his or her reason for carrying out such an activity, and their 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 infrastructure
- Bringing financial loss to the target
- Propagating religious or political beliefs
- Achieving the state's military objectives
- Damaging the reputation of the target
- Taking revenge
- Demanding ransom
- Fun/thrills/exploration





Top Information Security Attack Vectors

Below is a list of information security attack vectors through which a cyber-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 in the cloud. Flaw in one client's application cloud could potentially allow attackers to access another client's data.

- **Advanced Persistent Threats**

  An advanced persistent threat (APT) is an attack that focuses on stealing information from the victim's machine without the victim 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/or 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 malicious 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 the virus with the victim through the internet or 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 that 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 smartphones 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. Among other tactics, 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 (DoS) 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**

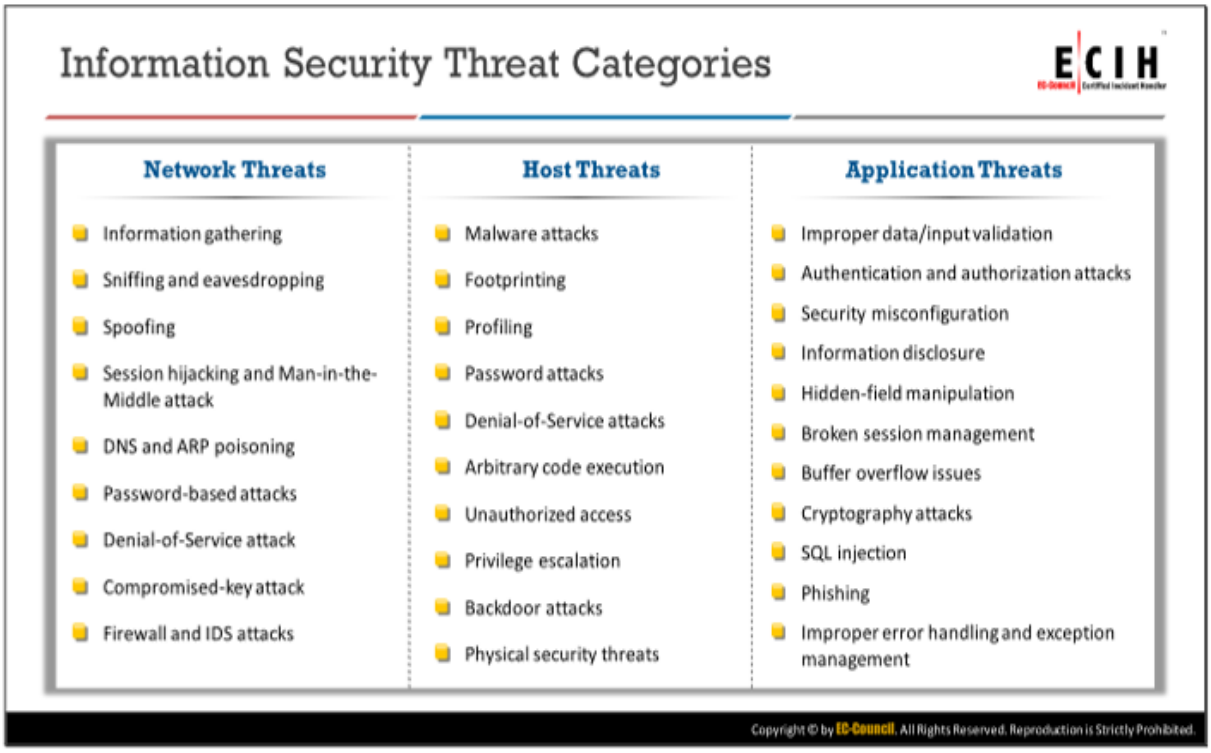
  Phishing is the practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information. Attackers perform phishing attacks by distributing malicious links via email or other communication channels to obtain private information like account numbers, credit card numbers, mobile numbers, etc. from the victim. Attackers design emails to lure victims in such a way that they appear to be from some legitimate source, or at times send malicious links that resemble legitimate websites.

- **Web Application Threats**

  Web application attacks, like SQL injection and cross-site scripting, have made web applications a favorable target for attackers to steal credentials, set up phishing sites, or acquire private information. The majority of such attacks are the result of flawed coding and improper sanitization of input and output data from a web application. Web application attacks can threaten the performance of a website and hamper its security.

- **Internet of Things (IoT) Threats**

  The IoT devices connected to the internet have little or no security, which makes them vulnerable to various types of attacks. These devices include many software applications that are used to access the devices remotely. Due to hardware constraints such as memory, battery, and so on, these IoT applications do not include complex security mechanisms to protect the devices from attacks. These drawbacks make IoT devices more vulnerable and allow attackers to access them remotely to perform various attacks.



Information Security Threat Categories

There are three types of information security threats:

- **Network Threats**

  A network is a collection of computers and other hardware connected by communication channels to share resources and information. As 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 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 attacks

- **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 host threats:

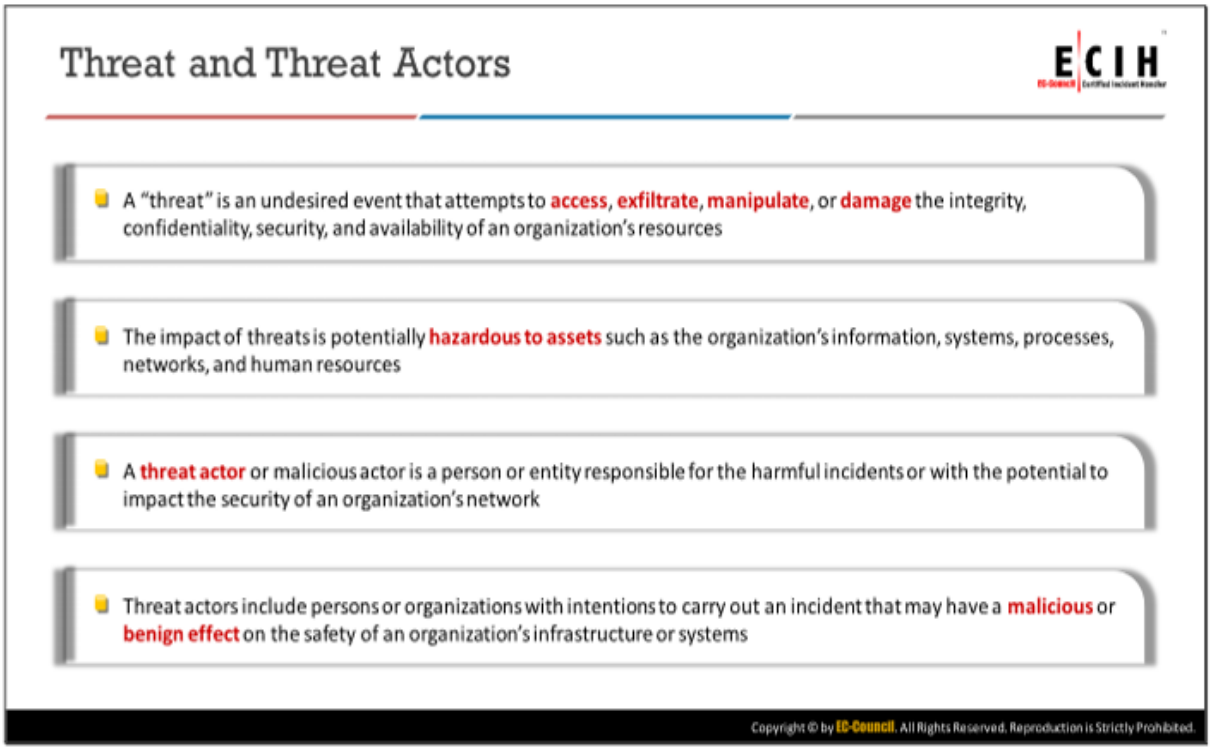
  - Malware attacks
  - Footprinting
  - Profiling
  - Password attacks
  - Denial-of-service attacks
  - Arbitrary code execution
  - Unauthorized access
  - Privilege escalation
  - Backdoor attacks
  - Physical security threats

- **Application Threats**

  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



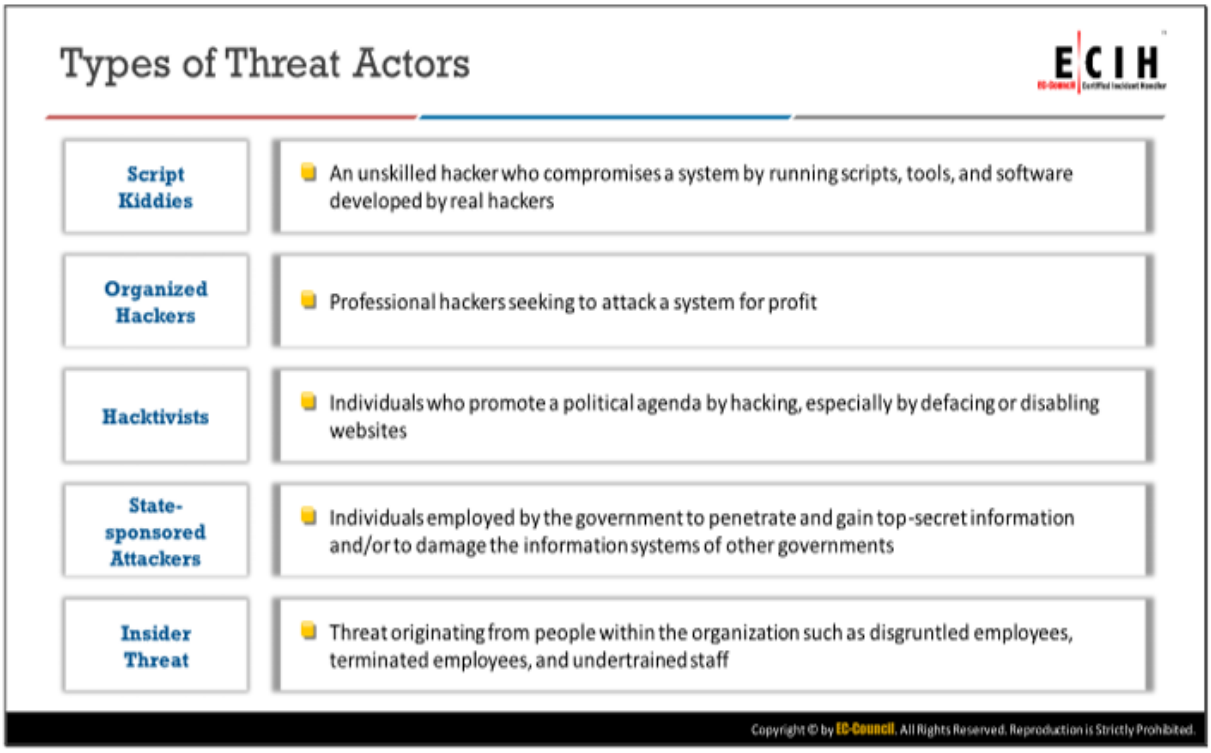
Threat and Threat Actors

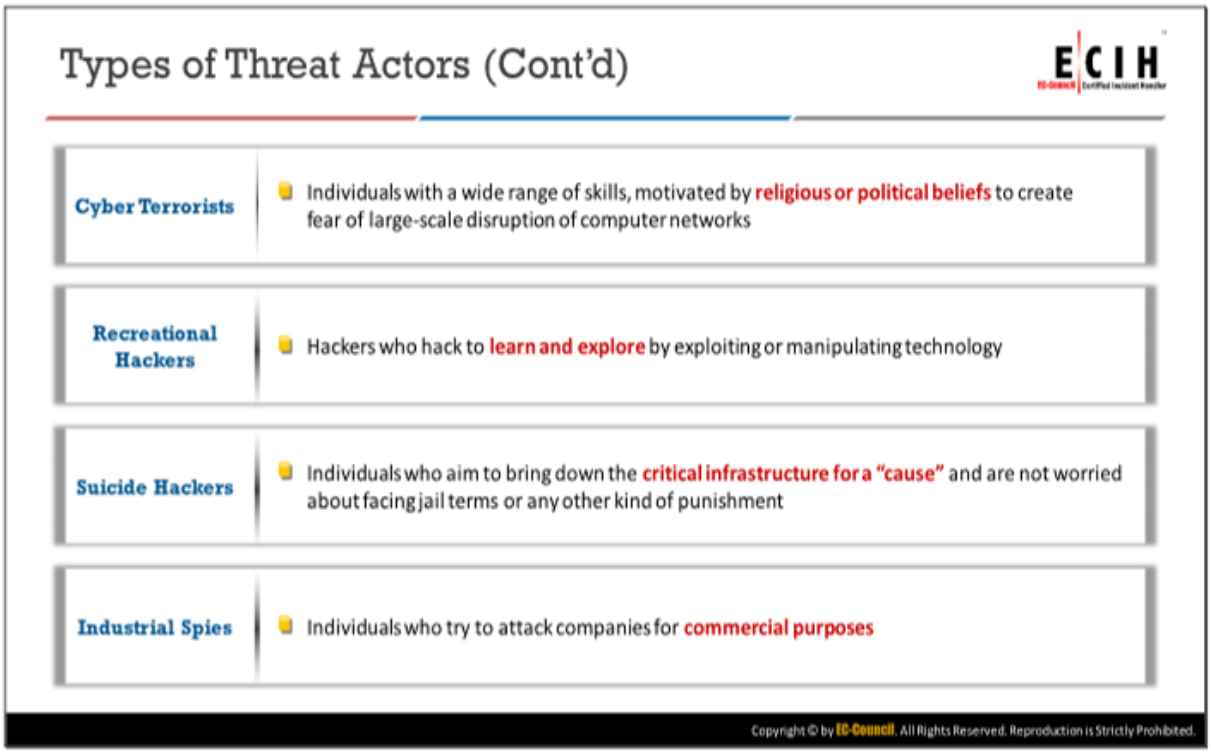
- **Threat**

  A threat refers to an undesired event that attempts to access, manipulate, or damage the integrity, confidentiality, security, and availability of an organization's resource. The impact of threats is potentially hazardous to assets such as information, systems, processes, networks, and human resources of the organizations. The existence of threats may be accidental, intentional, or due to the impact of some other action. They can be in any form, such as attackers, terrorists, and disgruntled employees.

- **Threat Actor**

  A threat actor or malicious actor is a person or entity that is responsible for the incidents or has the potential to impact the security of an organization's network. Unlike a hacker or attacker, it is not important for the threat actor to have technical skills. A threat actor could be a person or an organization with the intention to create an incident that can have a malicious effect on the safety of an organization's infrastructure or systems.





Types of Threat Actors

Discussed below are some of the important types of threat actors:

- **Script Kiddies**

  Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers. They usually focus on quantity rather than quality of the attacks that they initiate.

- **Organized Hackers**

  Organized hackers are professional hackers with the aim of attacking a system for profit. They hack to obtain confidential data such as social security numbers, personal identifiable information (PII) of an employee, health records, financial information such as bank records, and credit card information.

- **Hacktivists**

  Hacktivism is when hackers break into computer systems as an act of protest. Hacktivists use hacking to increase awareness of their social or political agendas as well as of themselves, in both the online and offline arenas. That is, 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 or a bad social actor. It remains a fact, however, that gaining unauthorized access is a crime, irrespective of their intentions.

- **State-sponsored Attackers**

  State-sponsored hackers are individuals employed by governments to penetrate, gain top-secret information from, and damage information systems of other governments or entities and to build sophisticated attacking setups to better target organizations. The motive behind such attacks is to fulfill political, economic, technical, or military agendas, and/or to obtain competitive information, resources, or users and exploit them for espionage purposes.

- **Insider Threat**

  An insider threat is a threat that originates from people within the organization; it is typically carried out by a privileged user, disgruntled employee, terminated employee, accident-prone employee, undertrained employee, or a third party. The main objective of such attacks is either to take revenge on an organization by damaging its reputation or to gain financial benefits.

- **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.

- **Recreational Hackers**

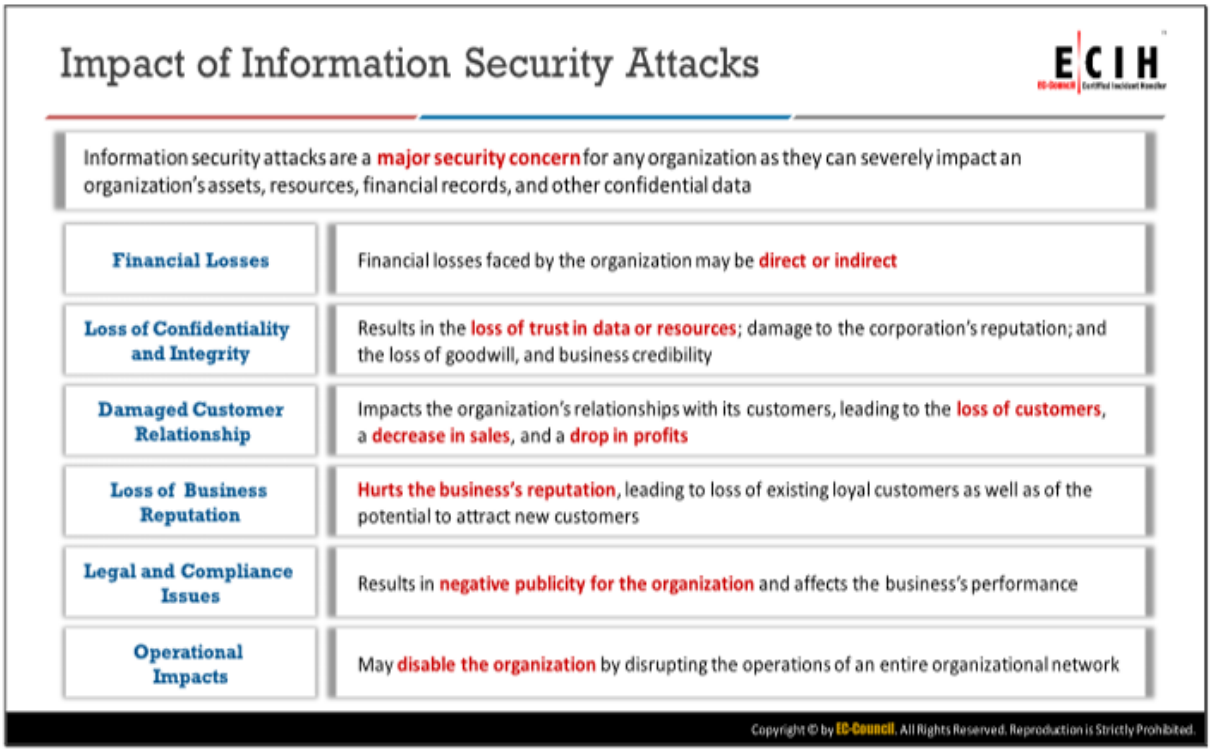
  Recreational hackers are hackers who hack to learn and explore by exploiting or manipulating technology. This type of hacker is usually not interested in gaining financial benefits.

- **Suicide Hackers**

  Suicide hackers are individuals who aim to bring down the 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 lives for an attack and are thus not concerned with the consequences of their actions.

- **Industrial Spies**

  Industrial spies are individuals who try to attack companies for commercial purposes. Business competitors often hire hackers or individuals, often called industrial spies, who attack the target organization to steal confidential information such as business strategy, financial records, and employees' information.



Impact of Information Security Attacks

Information security attacks are a major security concern for any organization, as they can have a severe impact on the organization's assets, resources, financial records, and other confidential data. Information security attacks are carried out by attackers with various motives and objectives and may have a severe impact on network and system resources as well as other organizational elements.

Following are the impacts that information security attacks can have on the organization:

- **Financial Losses**

  Organizations can go through huge financial losses due to information security attacks. Financial losses faced by organizations can be either direct or indirect: direct losses refer to the amount of money businesses have to remunerate for professional services, covering lost contracts and downtime, while indirect losses refer to the money that will be allocated by the organization to hire new staff, train them, and upgrade the organizational infrastructure.

- **Loss of Confidentiality and Integrity**

  Confidentiality and integrity are the most essential elements of information security. They assure that the information is accessible only to those who are authorized to have access and is sufficiently accurate for its purpose. Confidentiality and integrity breaches may occur due to improper data handling or a hacking attempt. This results in loss of trustworthiness of data or resources, damage to corporate reputation, and loss of goodwill, business credibility, and trust.

- **Damaged Customer Relationship**

  Trust is an important component that is required to establish customer relationship. Once an organization has been attacked, it causes permanent impact to organizational reputation and results in loss of trust among customers. This impacts the customer relationship and leads to loss of customers, decrease in sales, and drop in profits.

- **Loss of Business Reputation**

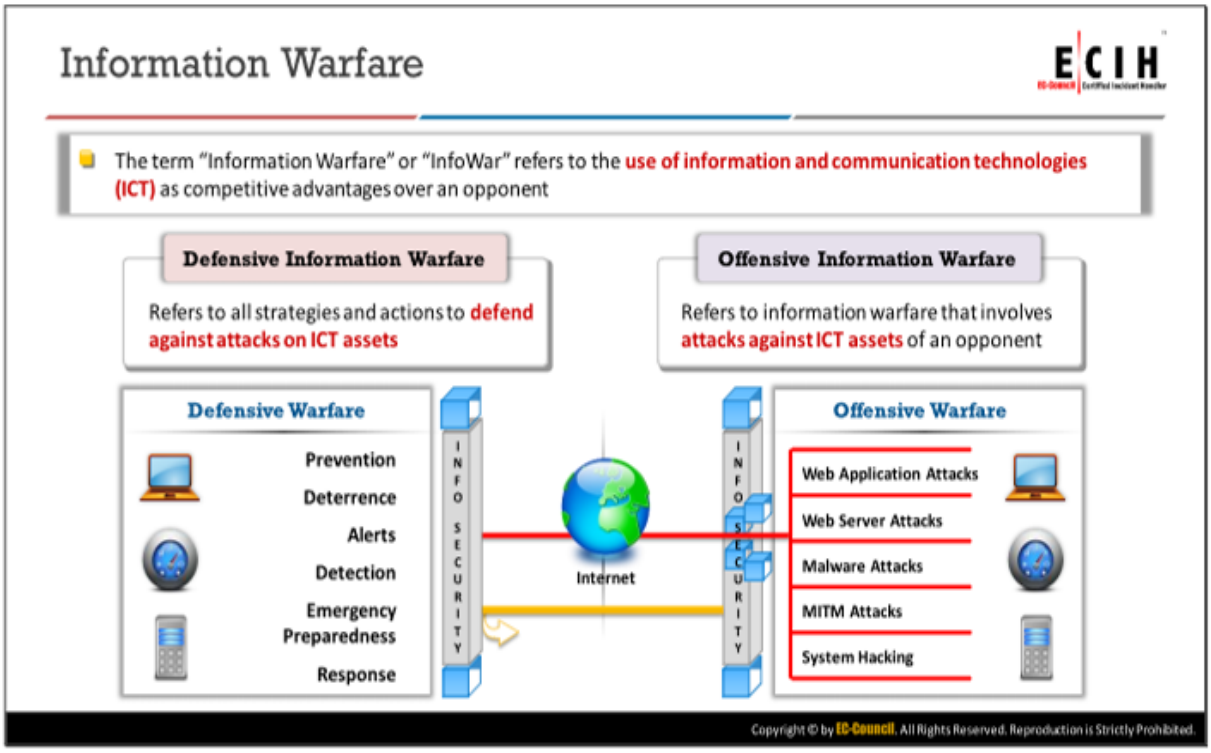
  Data protection and security are fundamental components that are helpful in protecting business reputation and maintaining customer loyalty. Information security attacks diminish business reputation and lead to loss of the existing loyal customers as well as the potential to attract new customers. The impact of reputational damage can even affect suppliers, relationships with partners, investors, and other third parties.

- **Legal and Compliance Issues**

  Organizations often face legal and compliance issues while dealing with security incidents. Managing the legal challenges of addressing information security is a complex process for organizations that impacts business reputation and public relations. Legal and compliance issues result in negative publicity for an organization and affect the business's performance.

- **Operational Impacts**

  Information security attacks may leave the organization disabled as they disrupt the working of an entire organizational network. They affect the operations of the organization by causing degradation in the quality of services, inability to meet service availability requirements, decrease in staff efficiency and productivity, and so on.



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, nanomachines 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 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 while the system is still 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**

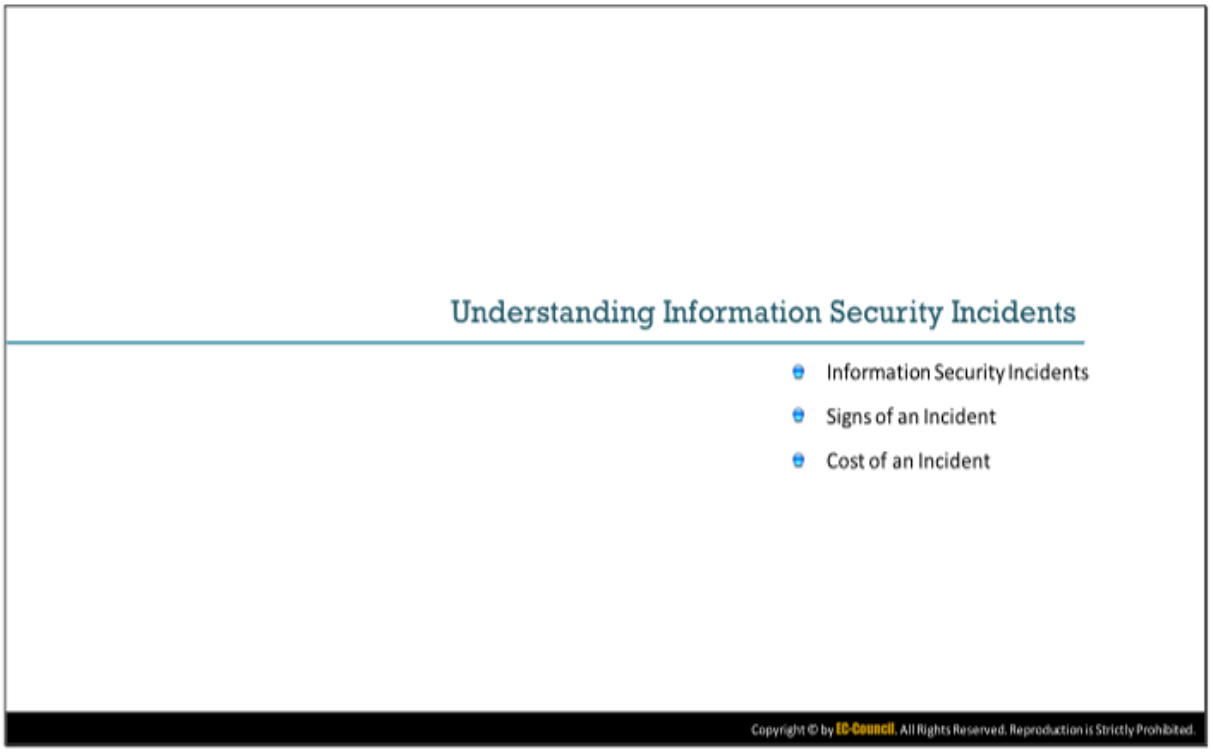
  This refers to all strategies and actions for security professionals and incident responders to defend their organization and its ICT assets from cyber attackers. It includes use of information to defend the organization from attack by performing:

  - Prevention
  - Deterrence
  - Alerts
  - Detection
  - Emergency preparedness
  - Response

- **Offensive Information Warfare**

  This refers to information warfare that involves attacks against ICT assets of an opponent, to compromise the target's assets. Techniques for offensive information warfare are:

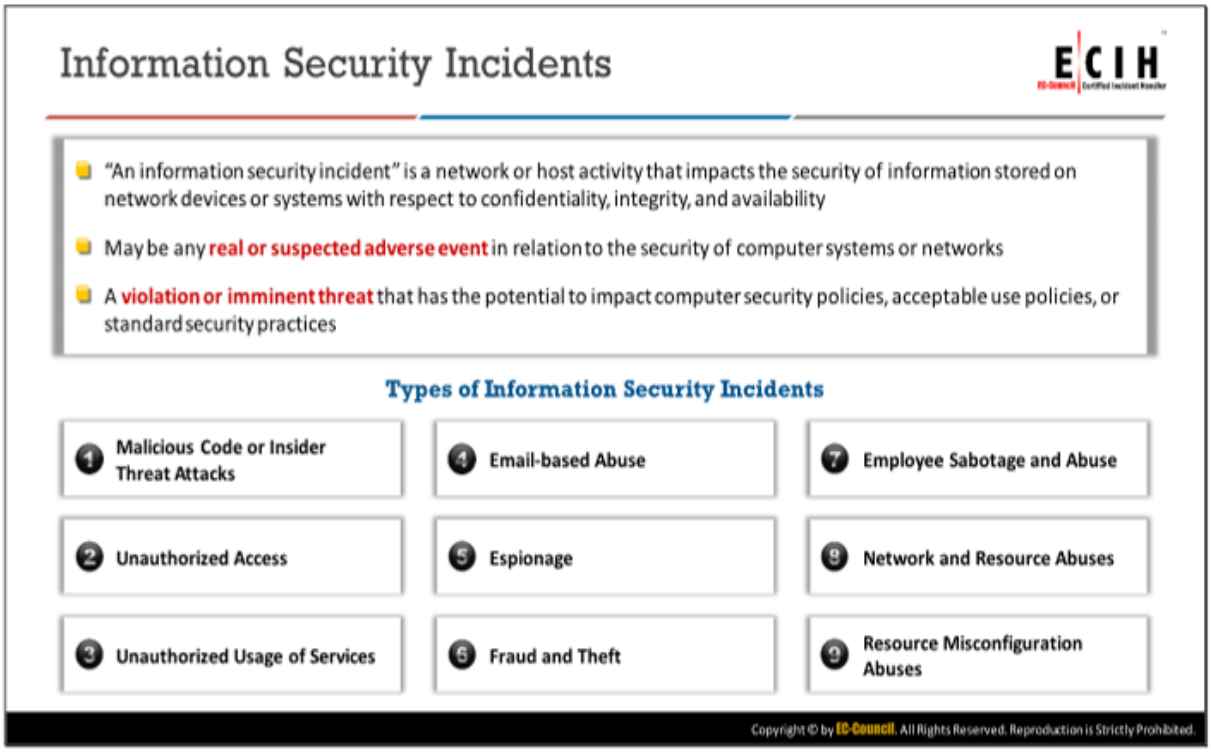
  - Web application attacks
  - Web server attacks
  - Malware attacks
  - Man-in-the-middle (MITM) attacks
  - System hacking



Understanding Information Security Incidents

With the complex landscape of cybercrime, security attacks, and data theft, organizations understand that properly handling potential security incidents plays a crucial role in their business strategy. Organizations plan to handle security incidents with the goal of minimizing the impact caused due to the incidents and strengthening defense strategies against evolving incidents.

This section discusses the various types of information security incidents, signs of an incident, and costs of an incident.



Information Security Incidents

An information security incident is any real or suspected network or host activity or event that potentially threatens the security of information stored on network devices and systems with respect to confidentiality, integrity, and availability. It is a violation or imminent threat that has the potential to impact computer security policies, acceptable use policies, and/or standard security practices.

Discussed below are the different types of information security incidents:

- **Malicious Code or Insider Threat Attacks**

  A malicious code attack is a type of attack that is generated by malicious programs such as viruses, Trojan horses, and worms. Insiders can use malicious code to gain administrative privileges, capture passwords, and alter audit logs to cover their tracks. Malicious code attacks are also called program threats. The intention behind this type of attack is to modify or destroy data, hide or steal data, or obtain unauthorized access and damage resources of the system or network.

- **Unauthorized Access**

  Unauthorized access refers to the process of obtaining illegal access to systems or network resources to steal or damage information. An attacker can achieve this by using network sniffers to capture network traffic in order to identify and obtain unencrypted usernames, passwords, and so on. Unauthorized access incidents include password attacks, session hijacking, and network sniffing.

- **Unauthorized Usage of Services**

  In this type of incident, an attacker uses another user's account to attack the system or network. It is a violation of the organization's information system policies and a misuse of the resources provided to users or employees. It could include using an office computer to download movies or store pirated software, removing content posted by another user, harassing other users, gaining credentials or personal information of other users, and so on. Inappropriate usage incident types include privilege escalation, insider attacks, and sharing of critical information.

- **Email-based Abuse**

  In this type of incident, an attacker creates a fake website mimicking a legitimate website and sends website links to users to steal sensitive information such as user credentials, bank account details, and credit card details. This type of incident includes +phishing mails.

- **Espionage**

  Espionage involves stealing the proprietary information of any organization and passing it to other organizations with the motive of negatively impacting the organization's reputation or for some financial benefit.

- **Fraud and Theft**

  This type of incident involves theft or loss of asset or equipment that contains confidential information. The motive behind fraud and theft is to gain control over and misuse information systems, such as access control systems, inventory systems, financial data, and telephone equipment.

- **Employee Sabotage and Abuse**

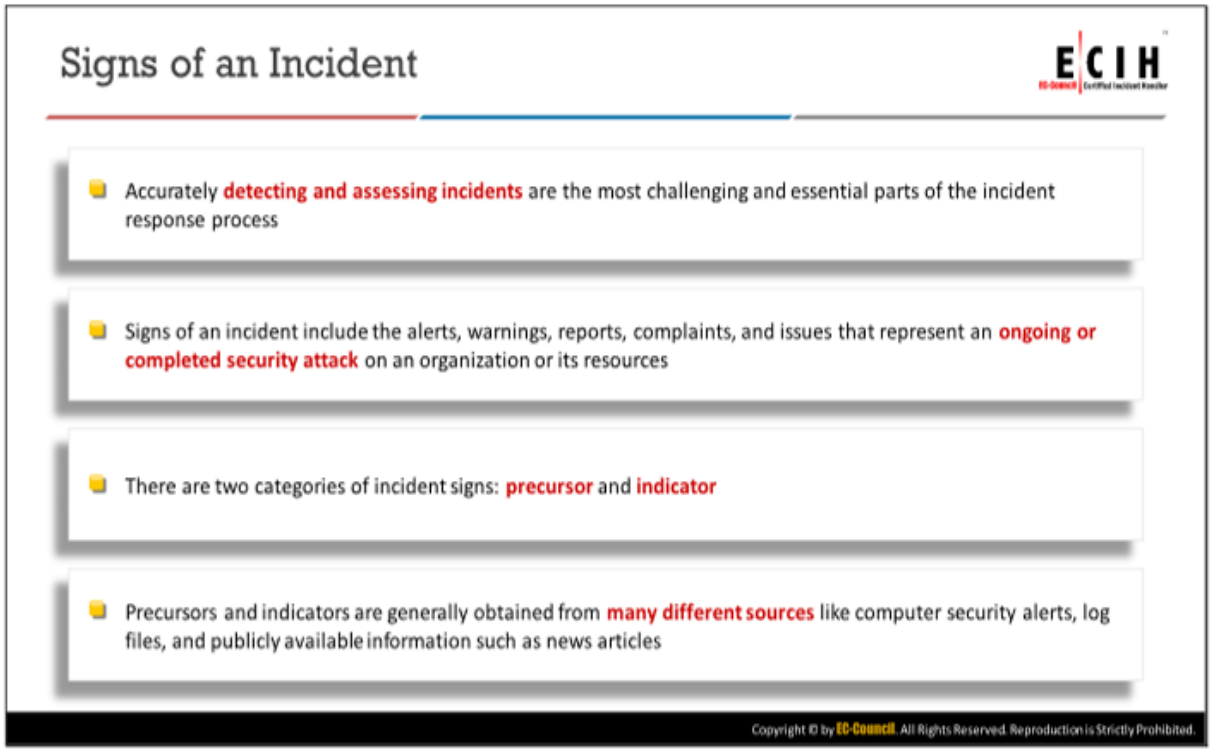
  Actions performed by an employee to abuse computer systems include removing hardware or services of a system, intentionally performing incorrect data entry, intentionally deleting data or altering data, placing logic bombs to delete information, applications, and system files, crashing systems, and so on.

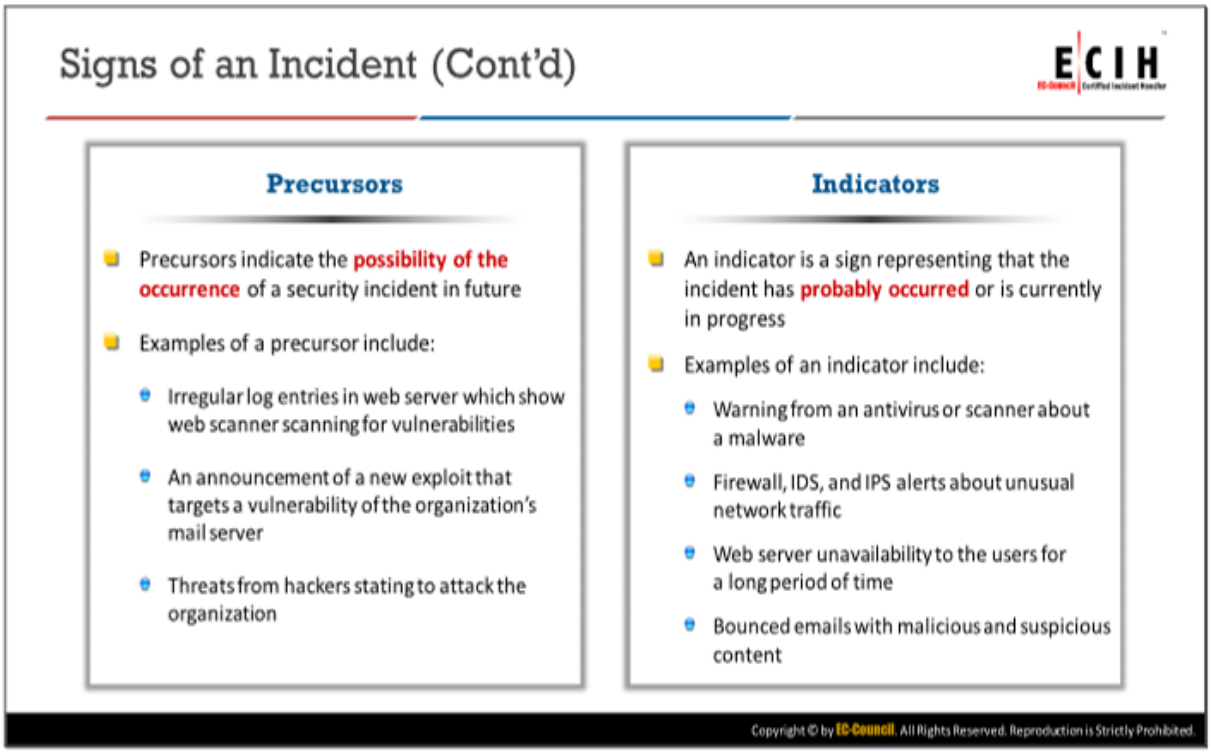
- **Network and Resource Abuses**

  In this type of incident, an attacker uses a network and resources to obtain critical organization details, or in some scenarios make the network services or resources unavailable to legitimate users by flooding servers or applications with traffic. Network and resource abuse incidents include DoS attacks, network scanning, and so on.

- **Resource Misconfiguration Abuses**

  In this type of incident, an attacker exploits resource misconfiguration such as vulnerable software configurations, open proxy servers or anonymous FTP servers, misconfigured web forms or blog sites, and so on. Resource misconfiguration abuses include SQL injection attacks, bypassing authentication, malicious code execution, and so on.





Signs of an Incident

Accurately detecting and assessing incidents is the most challenging and essential part of the incident response process. This includes detecting whether an incident had taken place, and if so, assessing its level of severity and magnitude. Signs or indicators of an incident are alerts, warnings, reports, complaints, and issues that reveal or refer to an ongoing or completed

security attack on an organization or its resources. They are varied in nature and can be from different sources and users.

Even though signs can sometimes be false alarms, incident responders must never be negligent in examining them thoroughly and analyzing their sources. Ignoring any signs can result in catastrophe and huge losses for the organization. Some commonly experienced signs of an attack are complaints from users, unavailability of resources, misbehavior of resources, alerts from security devices, and so on. Different sources of indicators include users, employees, vendors, customers, and hardware or software security solutions.

Based on their occurrence, there are two categories of incident signs, precursor and indicator signs:

- **Precursors**

  Precursors indicate the possibility of occurrence of a security incident in future. It is difficult to identify all precursors of incidents, as many attacks do not have detectable precursors from the target organization's perspective. Precursor detection may allow an organization to prevent incidents by enhancing its security posture either manually or by using automated tools, which will further protect the target from different attacks.

  Examples of precursors are:

  - Irregular log entries in a web server which show web scanner scanning for vulnerabilities
  - An announcement of a new exploit that targets a vulnerability of the organization's server database, operating system, or other resource
  - Threats from hackers stating that they intend to attack the organization

- **Indicators**

  Security incidents rarely have precursors but may have many indicators. An indicator is a sign representing that the incident has probably occurred or is currently in progress.

  Some of the important indicators of incidents include:

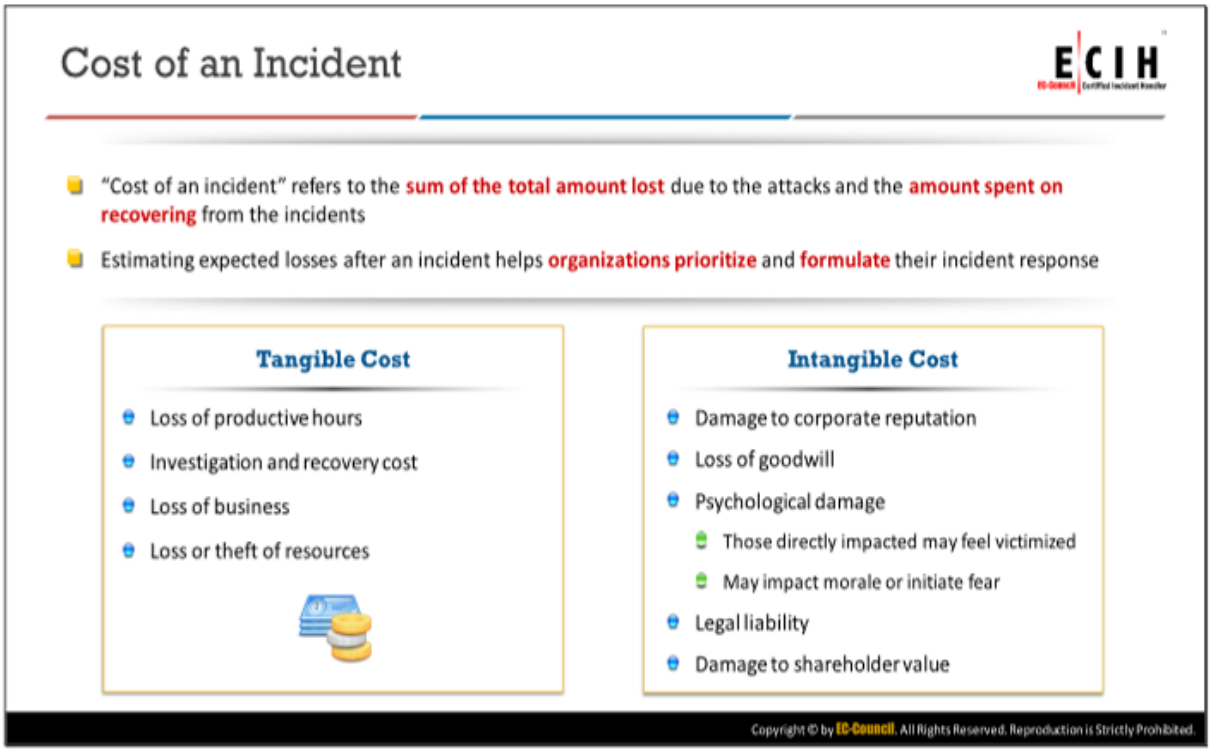
  - A user approaching the help desk to report abusing/threatening emails, issues with the network, system or server, inability to access accounts, and so on.
  - A warning from an antivirus or scanner about a malware
  - Firewall, IDS, and IPS alerts about unusual network traffic
  - Web server unavailability to users for a long period of time
  - Bounced emails with malicious and/or suspicious content
  - Multiple failed login attempts to access network resources or web server(s)
  - Inappropriate network traffic flow
  - Administrator-identified filenames with infrequent characters

Sources of Precursors and Indicators

Precursors and indicators are generally obtained from many different sources. The most commonly used sources include computer security alerts, log files, and publicly available information such as news articles and people.

Discussed below are common sources of precursors and indicators:

- **IDPS:** IDPS systems are used to detect suspicious events and log details related to the incidents, such as date and time of detection, type of incident, and source and destination IP addresses. Many IDPS systems generate multiple false-positive alerts; therefore, security analysts need to manually validate these security alerts by reviewing recorded data from multiple sources.
- **SIEM:** Security incident and event management (SIEM) systems are similar to IDPS systems but collect the log data from multiple sources, analyze the log data, and generate alerts based on the analysis.
- **Antivirus/Antispam Software:** Antivirus software detects malware, alerts administrators or users to it, and prevents it from infecting hosts. It detects and filters spam emails and prevents spam from reaching the inboxes of users. Alerts from such software are indicators of attack attempts.
- **File Integrity Checking Software:** File integrity checking software detects and alerts when critical system files are modified. This software calculates the cryptographic checksum of the original files and modified files. It compares checksums between these files to detect changes.
- **Third-Party Monitoring Services:** Third-party monitoring services, such as fraud detection systems, will notify an organization if any of the IP addresses or domain names belonging to the organization are misused to perform attacks on other organizations.
- **OS, Service, Network, and Application Logs:** Log details collected from operating systems (OS), services, networks, and applications reveal crucial information about security incidents such as user accounts accessed, date and time of access, actions performed, IP addresses, and domain names. These logs can be analyzed and correlated to detect suspicious events and generate alerts on security incidents.



Cost of an Incident

The cost of an incident is the sum of the total amount lost directly and indirectly due to the attack and the amount spent on recovering from the incident, including IH&R functions. Organizations must employ financial auditors to estimate the total cost of an incident and report it to the authorities.

Loss due to a cybersecurity incident may include but is not limited to:

- Infrastructure, such as servers, database systems, hosts, routers, and switches.
- Business credibility and trust
- Valuable information and human resources
- Physical losses

The cost of handling the breach includes:

- Cost of replacing the damaged infrastructure
- Amount spent to implement the incident handling process, including salaries of team members and cost of hardware and software tools
- Rents paid for backup services

Estimation of expected losses after an incident helps organizations prioritize and formulate their incident response. Although the estimated cost is often based on different highly variable parameters and is highly inaccurate, it helps in developing a basis for immediate incident handling and response. An incident results in both tangible and intangible losses, and the cost of an incident can be categorized as tangible and intangible costs:

- **Tangible Cost**

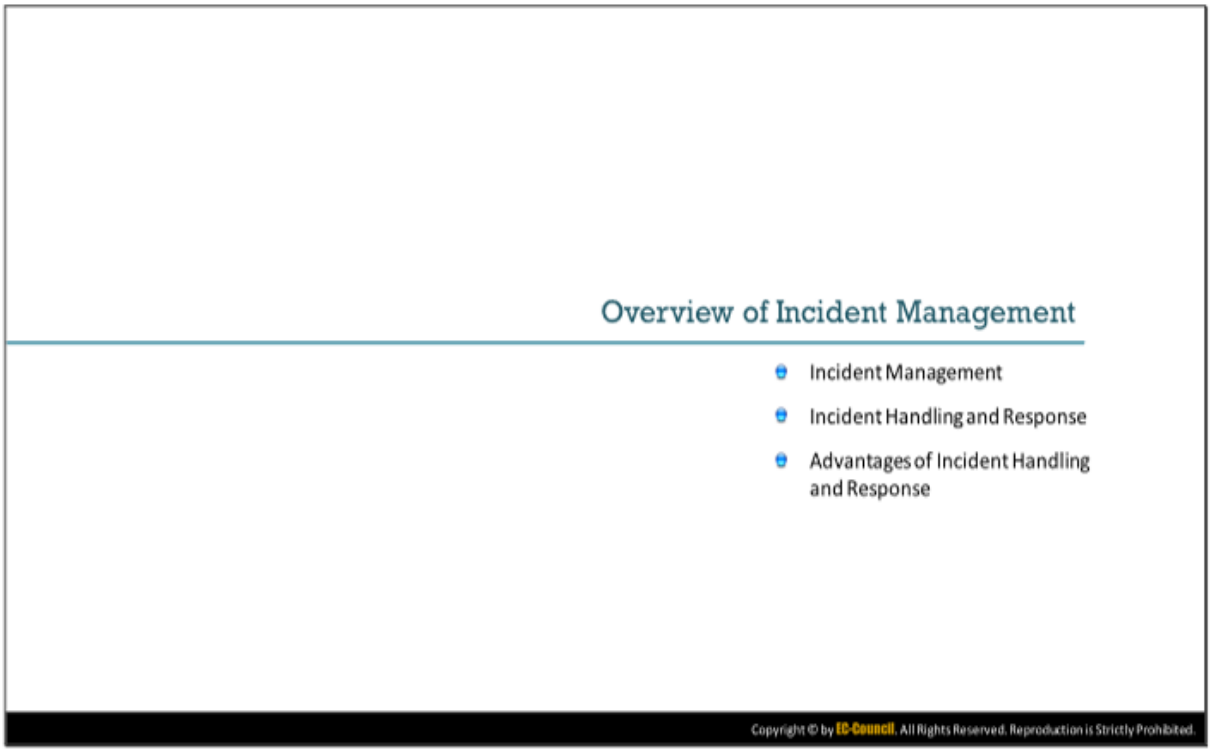
  This refers to the organization's direct expenditure due to an incident. Tangible cost can be quantified and identified. Tangible loss to an organization due to an incident may include:

  - Lost productive hours
  - Investigation and recovery costs
  - Loss of business
  - Loss or theft of resources

- **Intangible Cost**

  This refers to expenditures that the organization cannot calculate directly or value accurately. Intangible costs are difficult to identify and quantify, and include loss of assets, such as:

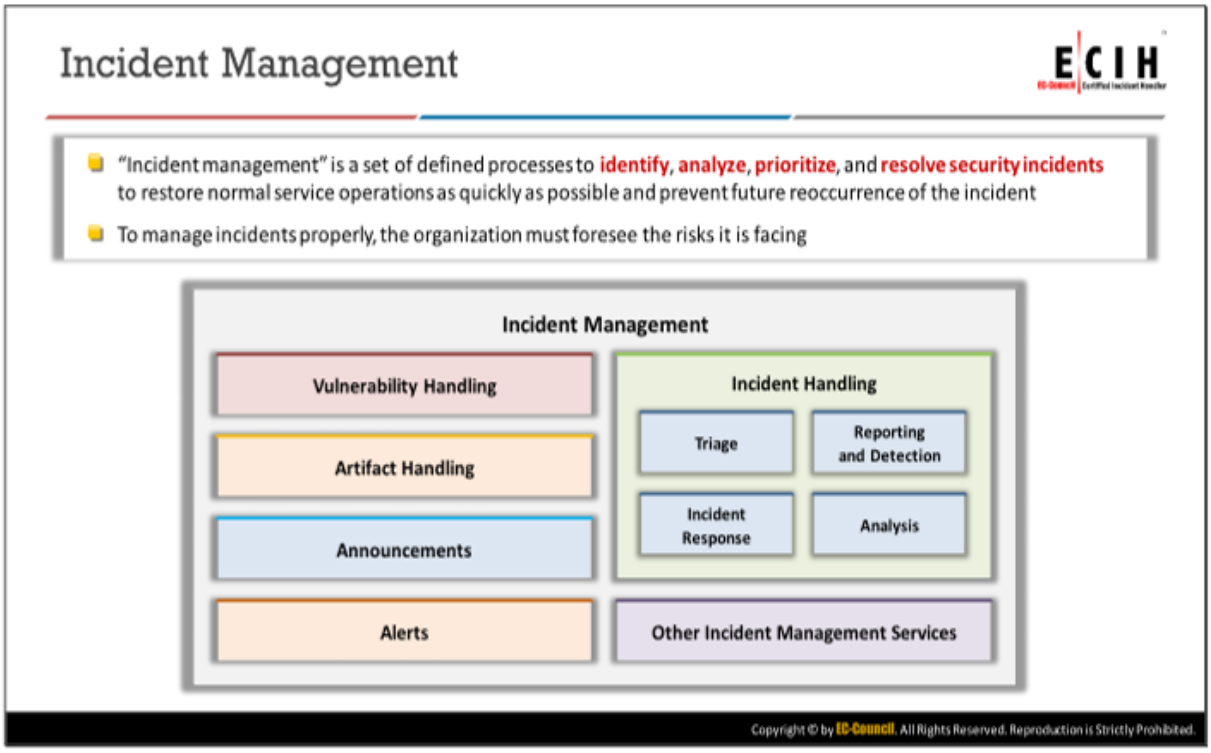
  - Damage to corporate reputation
  - Loss of goodwill
  - Psychological damage
    - Those directly impacted may feel victimized
    - May impact morale or initiate fear in them or more broadly
  - Legal liability
  - Damage to shareholders' value



Overview of Incident Management

Incident management keeps organizations prepared for unexpected security incidents and reduces the duration and severity of the damage caused to IT assets. It helps organizations return to normal service operations as early as possible after the incident and minimizes the impact to various business operations, ensuring that the required level of quality of service is maintained.

This section discusses in detail incident management, incident handling and response, and advantages of incident handling and response.



Incident Management

Incident management is an administrative function performed to effectively manage and respond to incidents and protect organizational assets, information, human resources, and customers from cyberattacks. It is a set of defined processes used to identify, analyze, prioritize, and resolve security incidents and restore a system to normal service and operations as soon as possible while preventing further recurrence of the incident. It involves not only responding to incidents but also providing advance alerts triggered to prevent potential risks and threats. The security administrator must therefore identify software that is open to attacks before someone takes advantage of the vulnerabilities; more broadly, to manage incidents properly, the organization must foresee the risks it is facing and manage them.

Incident management includes the following:

- Vulnerability analysis
- Artifact analysis
- Security awareness training
- Intrusion detection
- Technology monitoring

The purpose of the incident management process:

- Improves service quality
- Resolves problems proactively
- Reduces impact of incidents on businesses/organizations

- 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. This helps end users better recognize suspicious events or incidents with ease and makes them more 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 of 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 response to an insider or outside attacker using the organization's systems for harmful or malicious activities.
- The firewall manager keeps filters in place in areas where DoS attacks are made frequently.
- An outsourced service provider repairs systems infected by viruses and malware.

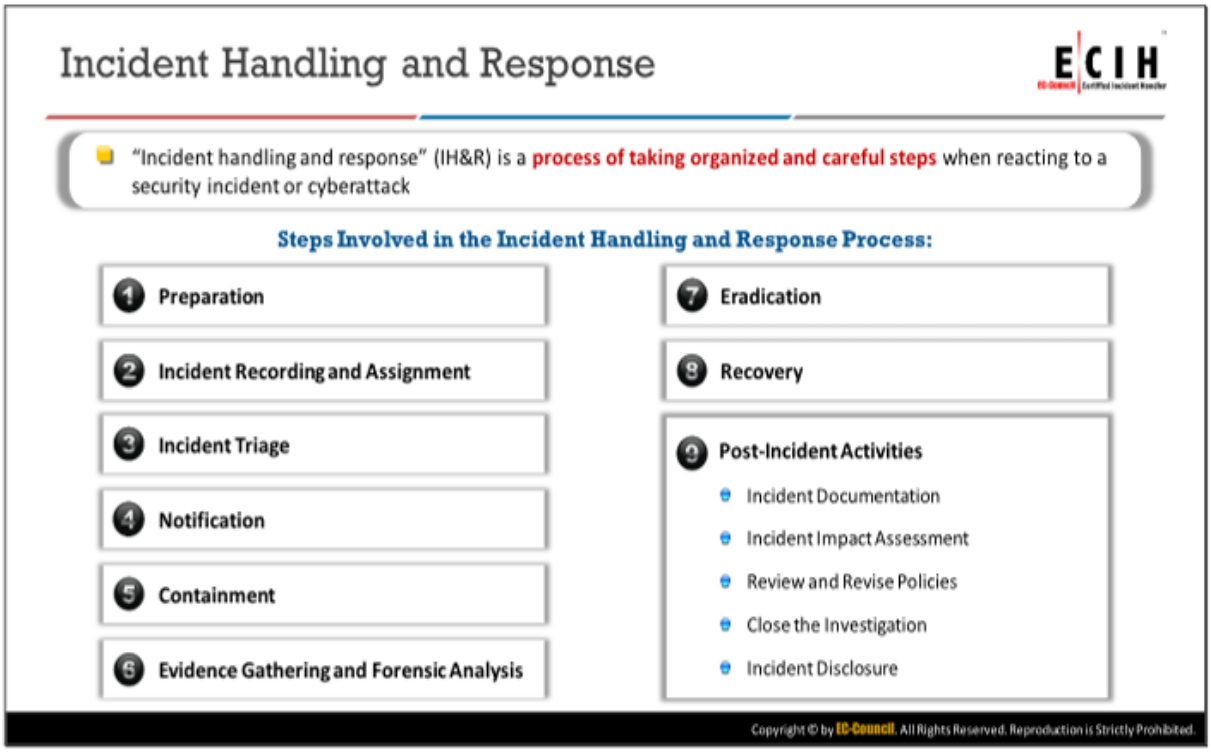
Incident management helps organizations overlook and manage all the components of information security, such as analyzing and managing risks; identifying and mitigating vulnerabilities; evaluating threats; handling customer and vendor relations; complying with laws, standards, and regulations; and proceeding legally when required.

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

It combines the incident handling process of triage, reporting, detection, analysis, containment, eradication, and forensics investigation. These processes, when performed accurately, can help the organization fight against incidents and prevent huge losses.

Recommended practices for incident management include:

- Defining roles and responsibilities of the different members of the incident response team in a clear and concise manner
- Ensuring proper training of the Incident Response Team (IRT) as per the objectives of the incident management plan
- Implementing strong objectives for collecting evidence and storing it safely
- Defining objectives for providing incident handling reports to internal stakeholders, partners, vendors, law enforcement, and so on.



Incident Handling and Response

Incident handling and response (IH&R) is a process and set of procedures, actions, and measures—organized, careful steps to react to a security incident, cyberattack, or other unexpected event occurrence. It involves identifying, logging, recording, and resolving the incident when it occurs and determining its impact and its cause. It is the practice of managing incident response processes, including preparation, detection, containment, eradication, and recovery, to overcome the impact of an incident quickly and efficiently. IH&R processes are important to provide a focused approach for restoring normal business operations as quickly as possible after an incident with minimal impact to the business.

The IH&R process involves defining user policies, developing protocols, building incident response teams, auditing organizational assets, planning incident response procedures, getting management approvals, and incident reporting, prioritization, and response management. It also includes establishment of proper communication between individuals responding to an incident and guidance to help them detect, analyze, contain, recover, and prevent incidents.

Discussed below are the steps involved in the IH&R process:

- **Step 1: Preparation**

  The preparation phase includes audit of resources and assets to determine the purpose of security and defining the rules, policies, and procedures that drive the IH&R process. It also includes building and training an incident response team, defining incident readiness procedures, and gathering required tools as well as training employees to secure their systems and accounts.

- **Step 2: Incident Recording and Assignment**

  In this phase, initial reporting and recording of the incident take places. This phase includes the identification of an incident, defines proper incident communication plans for employees, and also includes communication methods involving informing IT support personnel or raising an appropriate ticket.

- **Step 3: Incident Triage**

  In this phase, identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident details such as the type of attack, severity, target, impact, method of propagation, and the vulnerabilities it exploited.

- **Step 4: Notification**

  In the notification phase, the IH&R team informs various stakeholders, including management, third-party vendors, and clients, about the identified incident.

- **Step 5: Containment**

  This phase involves stopping the spread of infection to other organizational assets and preventing additional damage.

- **Step 6: Evidence-Gathering and Forensic Analysis**

  In this phase, the IH&R team accumulates all possible evidence related to the incident and submits it to the forensic department for investigation. Forensic analysis of an incident would reveal details such as method of attack, vulnerabilities exploited, security mechanisms averted, network devices infected, and applications compromised.

- **Step 7: Eradication**

  In the eradication phase, the IH&R team removes or eliminates the root cause of the incident and closes all the attack vectors to prevent similar incidents in future.

- **Step 8: Recovery**

  After eliminating the causes of the incidents, the IH&R team restores the affected systems, services, resources, and data through recovery. It is the responsibility of the incident response team to ensure that there is no disruption to the services or business of the organization owing to the incident.

- **Step 9: 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 IH&R process which includes:

  - Incident documentation
  - Incident impact assessment
  - Reviewing and revising policies
  - Closing the investigation
  - Incident disclosure

Advantages of Incident Handling and Response

Given the ever-evolving cyber threat landscape, employing IH&R processes has become critically important to organizations. Having a well-defined incident management process helps organizations to resolve incidents faster and more efficiently; moreover, it helps them focus exclusively on handling and escalating occurred incidents so as to restore operations and service levels to the normal state after an incident has occurred.

Having an IH&R process will help organizations to:

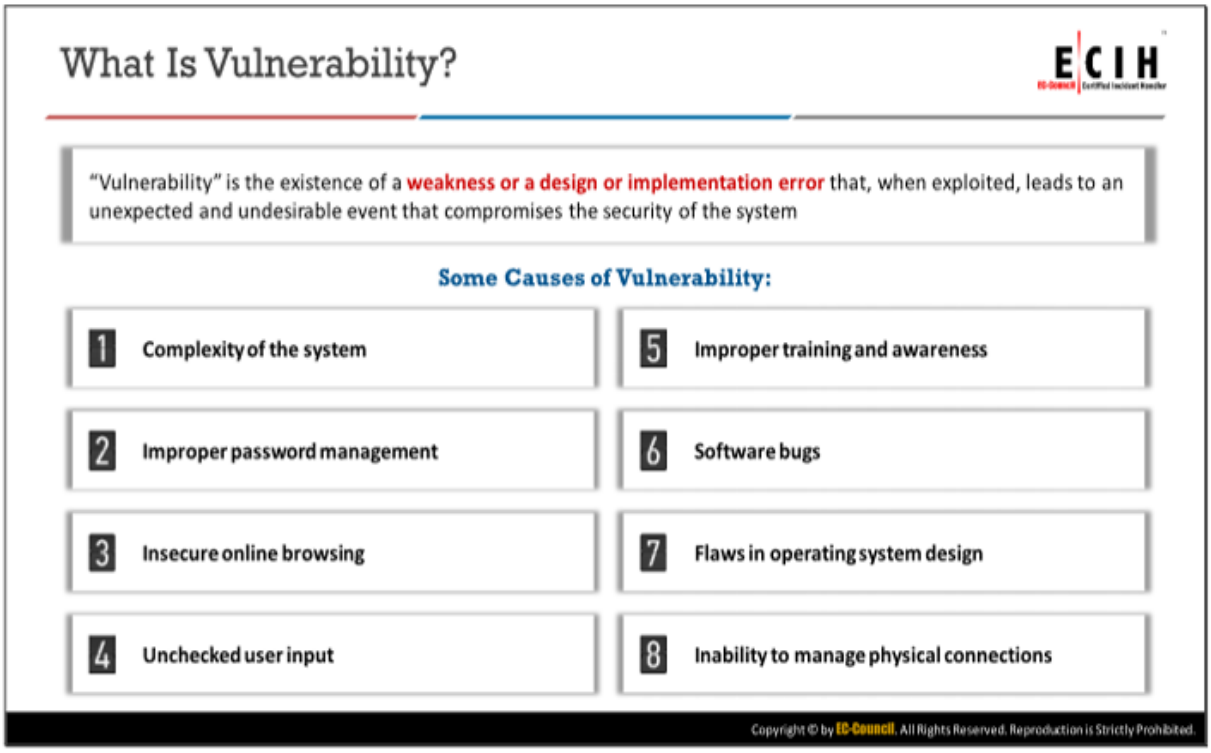
- Identify crucial data and resources that require protection
- Develop an incident readiness strategy for prediction of future threats and attacks
- Prepare to monitor different resources and attack vectors
- Frame and implement security and usage policies
- Create a centralized communication plan
- Find vulnerabilities and identify the risks they can result in
- Build the ability to prevent crimes
- Reduce the impact of incidents
- Reduce the incident cost and investigation cost
- Easily detect and contain of incidents
- Prevent similar incidents in future
- Reduce reputational risk caused by incidents and improve client and investor confidence

- Comply with standards as well as local and international laws and regulations
- Gain trust among customers, partners, and vendors
- Develop good coordination among the relevant employees within the organization and with other organizations' security teams
- Increase efficiency and productivity throughout the organization

Overview of Vulnerability Management

In a network, there are generally two main causes of system vulnerability: software or hardware misconfiguration and poor programming practice. Attackers exploit these vulnerabilities to perform various attacks on organizational resources, while organizations use vulnerability management to manage and defend against the exploitation of underlying vulnerabilities in their systems, applications, and networks. Vulnerability management is a proactive approach designed to identify, classify, and mitigate vulnerabilities.

This section discusses vulnerability as a concept, common areas of vulnerability, vulnerability research, vulnerability classification, vulnerability assessment, types of vulnerability assessment, and the vulnerability management life cycle.

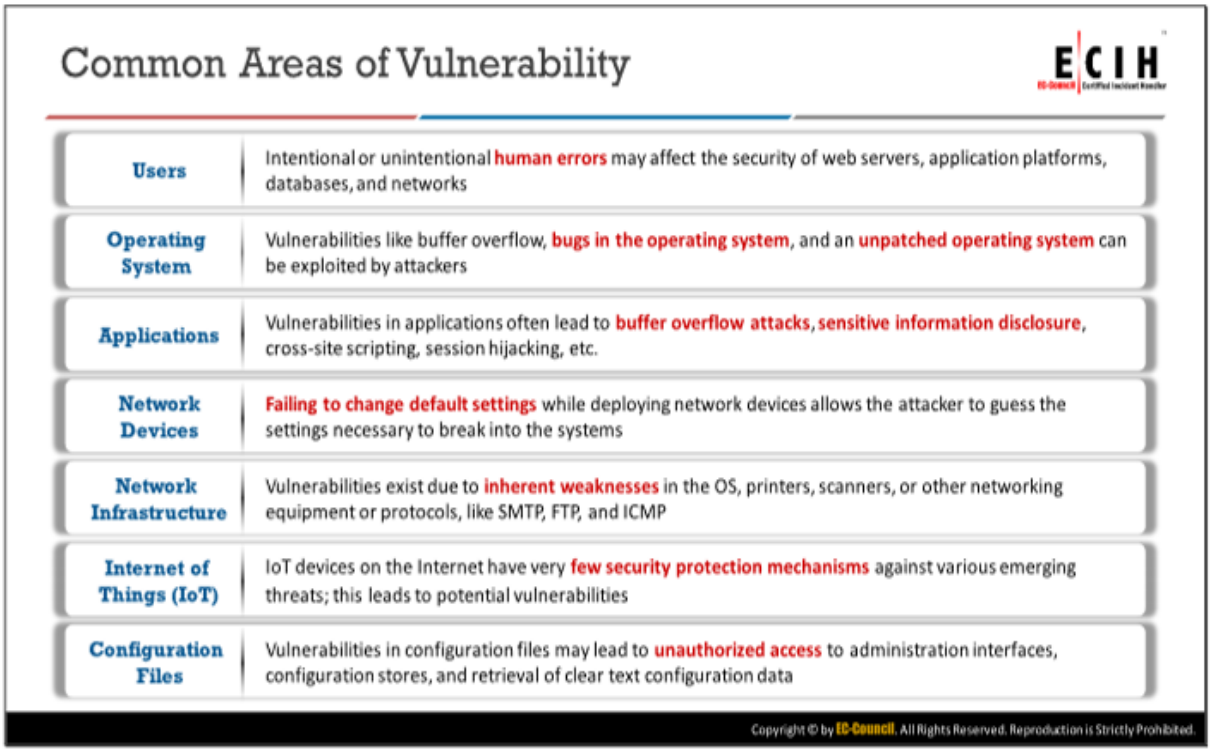


What Is Vulnerability?

In cybersecurity, vulnerability refers to the existence of a weakness, whether in design or implementation, that when exploited by attackers leads to an unexpected and undesirable event compromising the security of the system—a security loophole that allows an attacker to enter the system by bypassing various user authentication mechanisms using various tools and techniques.

Listed below are some of the common causes of vulnerabilities:

- Complexity of a system
- Improper password management
- Insecure internet website browsing
- Unchecked user input
- Improper training and awareness
- Software bugs
- Flaws in operating system design
- Inability to manage physical connections
- Missing authentication for critical function
- Missing authorization
- Missing data encryption
- Unrestricted upload of dangerous file types
- Reliance on untrusted inputs in a security decision
- Download of codes without integrity checks
- URL redirection to untrusted sites
- Weak passwords
- Buffer overflow
- Use of broken algorithms
- Software corrupted with virus



Common Areas of Vulnerability

There are several approaches that are used by attackers to gain access to a system. One common requirement of all such approaches is that the attacker finds and exploits the system's weakness or vulnerability.

Discussed below are the common areas where attackers search for vulnerabilities:

- **Users**

  Human error is one of the most common factors leading to vulnerabilities that allow attackers to gain unauthorized access to a system. It may happen intentionally or unintentionally, affecting web servers, application platforms, databases, and networks. Misconfiguration is the most common vulnerability (mainly) caused by human error.

  Listed below are some of the human errors which can be exploited by the attacker:

  - Not changing default settings while deploying the software
  - Using default passwords
  - Buffer overflows that happen due to coding errors
  - Failing to protect the confidentiality of a password
  - Errors in programming

- **Operating System**

  The operating system (OS) is one of the key locations of vulnerabilities. Attackers constantly look for OS vulnerabilities that allow them to exploit and gain access to a target system or network. OS vulnerabilities like buffer overflow vulnerabilities, bugs in

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

- **Applications**

  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, which tend to come with more and more features and functionality, making them more and more complex; this increase in complexity means more opportunity for attackers to find and exploit resulting vulnerabilities using different tools and techniques in order to gain unauthorized access and steal or manipulate data. Vulnerabilities in applications often lead to buffer overflow attacks, sensitive information disclosure, cross-site scripting, session hijacking, and so on.

  Common areas of vulnerability in applications are as follows:

  - Networking software
  - Network operations and management
  - Firewall and network security applications
  - Database software

- **Network Devices**

  Vulnerabilities in network devices exist when an administrator configures a user account or system services insecurely, for instance leaving default settings or engaging in improper password management. Attackers can detect lack of authentication of networking equipment like switches and routers, which allows system intrusion. In some cases, infected devices may not contain any valuable information but may be connected to networks or systems that do have confidential information, leading to a data breach. Not changing the default settings while deploying software or hardware makes it plausible for an attacker to guess the settings and break into the systems. The security administrator must identify devices that are open to attacks before someone takes advantage of the vulnerabilities.

  Network devices that are susceptible to vulnerabilities include:

  - Access points
  - Routers
  - Wireless routers
  - Switches
  - Firewall

- **Network Infrastructure**

  Network infrastructure vulnerabilities are mainly responsible for the major security issues in the organizational systems. These vulnerabilities have a huge impact on almost every element of or device running on the network. They exist mainly due to inherent weaknesses in the operating system, printers, scanners or other networking equipment or to loopholes in protocols, like SMTP, FTP, and ICMP. Regular security audits by the network administrator or information security officer will help keep track of any irregular activities on the network.

- **Internet of Things (IoT)**

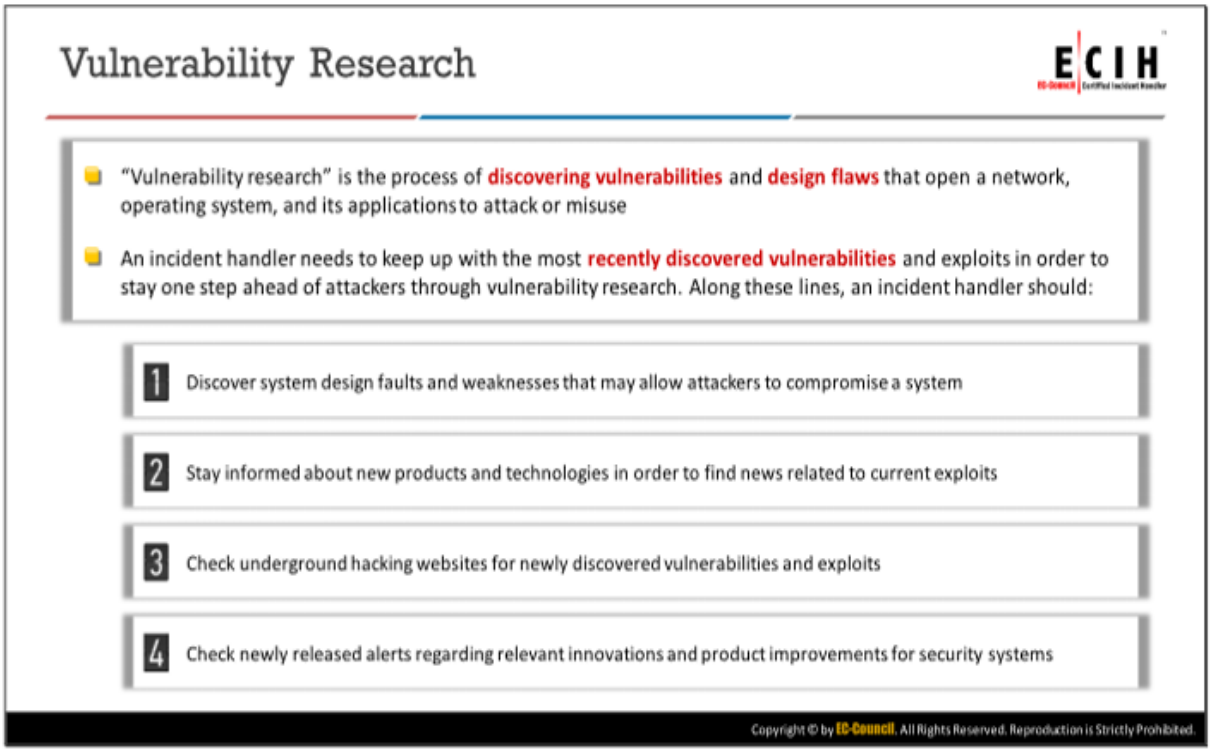
  Potential vulnerabilities in the IoT system can result in severe threats to organizations, as a majority of IoT devices come with security issues. IoT devices on the internet have very few security protection mechanisms against various emerging threats. These devices can thus be infected by malware or malicious code due to the absence of proper authentication mechanisms or use of default credentials, absence of lockout mechanism, absence of strong encryption scheme, absence of proper key management systems, improper physical security, and so on. Attackers often exploit these poorly protected devices on the internet to cause physical damage to the network, to wiretap communication, and also to launch disruptive attacks such as DDoS.

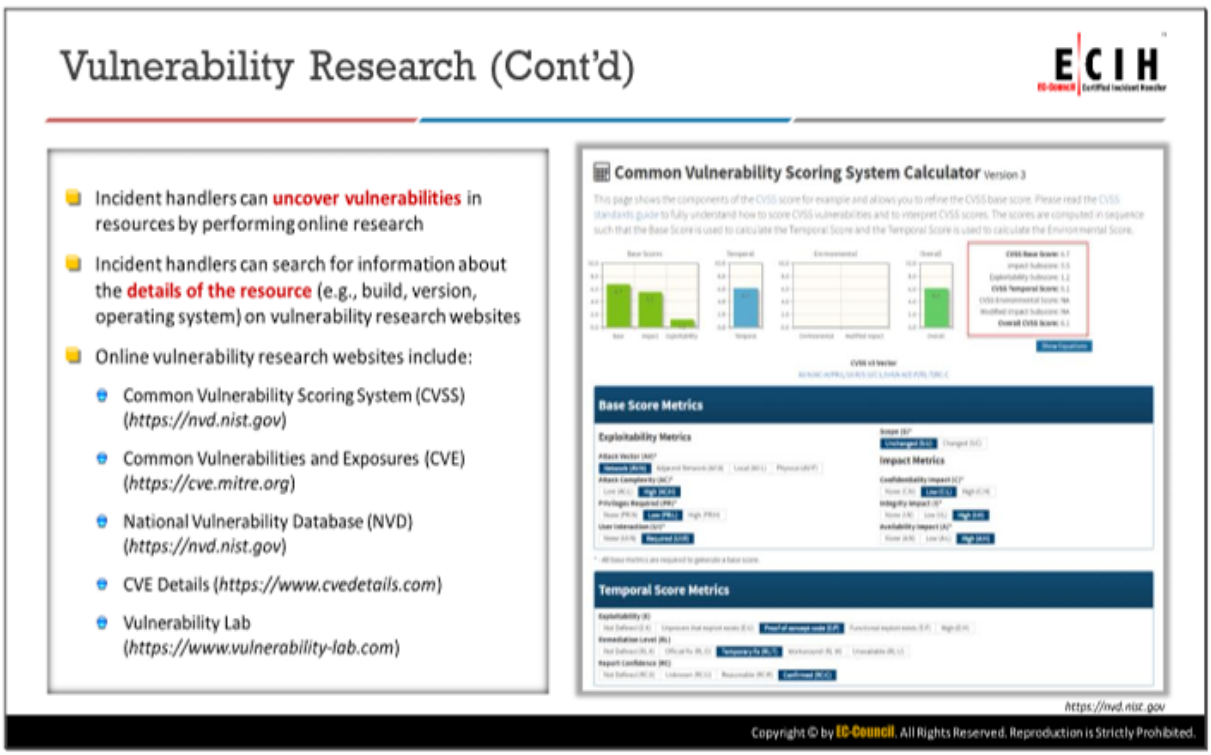
  Listed below are the common areas of vulnerabilities in IoT devices:

  - Device memory
  - Ecosystem access control
  - Decommissioning system
  - Device physical interfaces
  - Device web interface
  - Device firmware
  - Device network services
  - Administrative interface
  - Local data storage
  - Third-party backend APIs
  - Ecosystem communication

- **Configuration Files**

  System configuration files consist of critical configuration information utilized to set up and operate an organizational network efficiently. If configuration files are not properly authenticated before it is loaded, it will allow the attacker to make unauthorized changes to the files, which could harm the network. Moreover, modifications to configuration files can also allow system intrusion. In application-based attacks, attackers also use external configuration files to gain unauthorized access to administration interfaces, configuration stores, and clear text configuration data.





Vulnerability Research

Vulnerability research is the process of discovering vulnerabilities and design flaws that will open a network, operating system, or applications to attack or misuse. Organizations must perform vulnerability research on their products and resources to identify and eradicate all security flaws.

An administrator needs vulnerability research:

- To gather information about security trends, threats, and attacks
- To find weaknesses and alert the network administrator before a network attack
- To get information that helps prevent security problems
- To know how to recover from a network attack

An incident handler needs to keep up with the most recently discovered vulnerabilities and exploits in order to stay one step ahead of attackers. This is done through vulnerability research, which includes:

- Discovering system design faults and weaknesses that might allow attackers to compromise a system
- Being informed about new products and technologies in order to find news related to current exploits
- Checking underground hacking websites for newly discovered vulnerabilities and exploits
- Checking newly released alerts regarding relevant innovations and product improvements for security systems

Security experts and vulnerability scanners classify vulnerabilities by:

- Severity level (low, medium, or high)
- Exploit range (local or remote)

Incident handlers can research vulnerabilities online by using details of the resources in question, such as build, version, or operating system.

Some online vulnerability research websites include:

- **Common Vulnerability Scoring System (CVSS)**

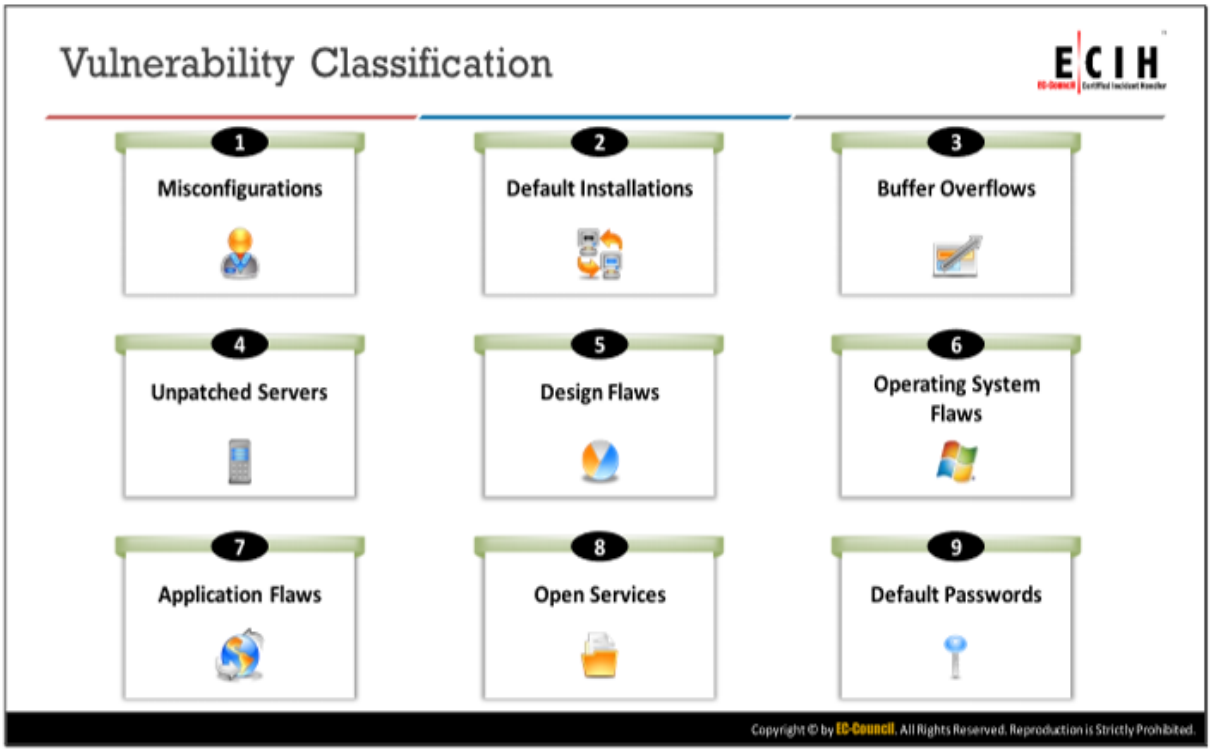
  Source: *https://nvd.nist.gov*

  CVSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited to the role of a standard measurement system for industries, organizations, and governments that need accurate, consistent vulnerability impact scores. Two common uses of CVSS are in the prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

  CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be

translated into a qualitative representation (e.g., low, medium, high, or critical) to help organizations properly assess and prioritize their vulnerability management processes.

- Common Vulnerabilities and Exposures (CVE) (*https://cve.mitre.org*)
- National Vulnerability Database (NVD) (*https://nvd.nist.gov*)
- CVE Details (*https://www.cvedetails.com*)
- Vulnerability Lab (*https://www.vulnerability-lab.com*)
- Microsoft Vulnerability Research (MSVR) (*https://technet.microsoft.com*)
- Security Magazine (*https://www.securitymagazine.com*)
- SecurityFocus (*https://www.securityfocus.com*)
- Help Net Security (*https://www.net-security.org*)
- HackerStorm (*http://www.hackerstorm.co.uk*)
- SC Magazine (*https://www.scmagazine.com*)
- Computerworld (*https://www.computerworld.com*)
- WindowsSecurity (*http://www.windowsecurity.com*)
- Exploit Database (*https://www.exploit-db.com*)
- Security Tracker (*https://securitytracker.com*)
- D'Crypt (*https://www.d-crypt.com*)
- Trend Micro (*https://www.trendmicro.com*)
- Rapid7 (*https://www.rapid7.com*)
- Dark Reading (*https://www.darkreading.com*)



Vulnerability Classification

Vulnerabilities present in a system or network are classified into the following categories:

- **Misconfigurations**

  Misconfiguration is the most common vulnerability mainly caused by human error, and allows attackers to gain unauthorized access to a system. This may happen intentionally or unintentionally, affecting web servers, application platforms, databases, and networks.

  A system can be misconfigured in many ways:

  - An application running with debug enabled
  - Outdated software running on the system
  - Running unnecessary services on a machine
  - Using misconfigured SSL certificates and default certificates
  - Improperly authenticated external systems
  - Disabling security settings and features

  Attackers can easily detect these misconfigurations using scanning tools and then exploit the backend systems. It is important for the administrators to change the default configuration and optimize the security of the devices.

- **Default Installations**

  Default installations are usually kept user friendly, especially when the device is being used for the first time, as the primary concern is usability of the device rather than the

device's security. In some cases, infected devices may not contain any valuable information but may still be connected to networks or systems containing confidential information that would result in a data breach. Not changing the default settings while deploying the software or hardware allows the attacker to guess the settings and break into the systems.

- **Buffer Overflows**

  Buffer overflows are a common software vulnerability; they happen due to coding errors and allow attackers to get access to the target system. In a buffer overflow attack, attackers undermine the functioning of programs and try to take control of the system by writing content beyond the allocated size of the buffer. Insufficient bounds checking in the program is thus the root cause of this issue; because of it, the buffer is not able to handle data beyond its limit, causing flow of data to adjacent memory locations and overwriting their data values. Systems often crash, become unstable, or show erratic program behavior when buffer overflow occurs.

- **Unpatched Servers**

  Servers are an essential component of the infrastructure of any organization. There are many cases, however, in which organizations run unpatched and misconfigured servers, compromising the security and integrity of the data in the system. Hackers look out for these vulnerabilities in the servers and exploit them. As servers serve as a hub for the network, unpatched servers can also serve attackers as an entry point into it. This can lead to exposure of private data, financial loss, discontinuation of operations, and so on. Updating software regularly and maintaining systems properly by patching and fixing bugs can help mitigate vulnerabilities caused due to unpatched servers.

- **Design Flaws**

  Vulnerabilities due to design flaws are present in all operating devices and systems. Design vulnerabilities such as incorrect encryption or poor validation of data constitute logical flaws in the functionality of a system that are exploited by attackers to bypass detection mechanisms and acquire access to secure systems.

- **Operating System Flaws**

  Due to vulnerabilities in operating systems, applications such as Trojans, worms, and viruses pose threats. These attacks are performed using malicious code, scripts, or unwanted software, which result in loss of sensitive information and loss of control of computer operations. Timely patching of the OS, installing only required software applications, and use of applications with firewall capabilities are essential steps that an administrator needs to take to protect an OS from any attack.

- **Application Flaws**

  Application flaws are vulnerabilities in applications that are exploited by attackers. Applications should be secured using validation and authorization requirements for users. Unsecured applications pose security threats such as data tampering and unauthorized access to configuration stores; if they are not secured, sensitive

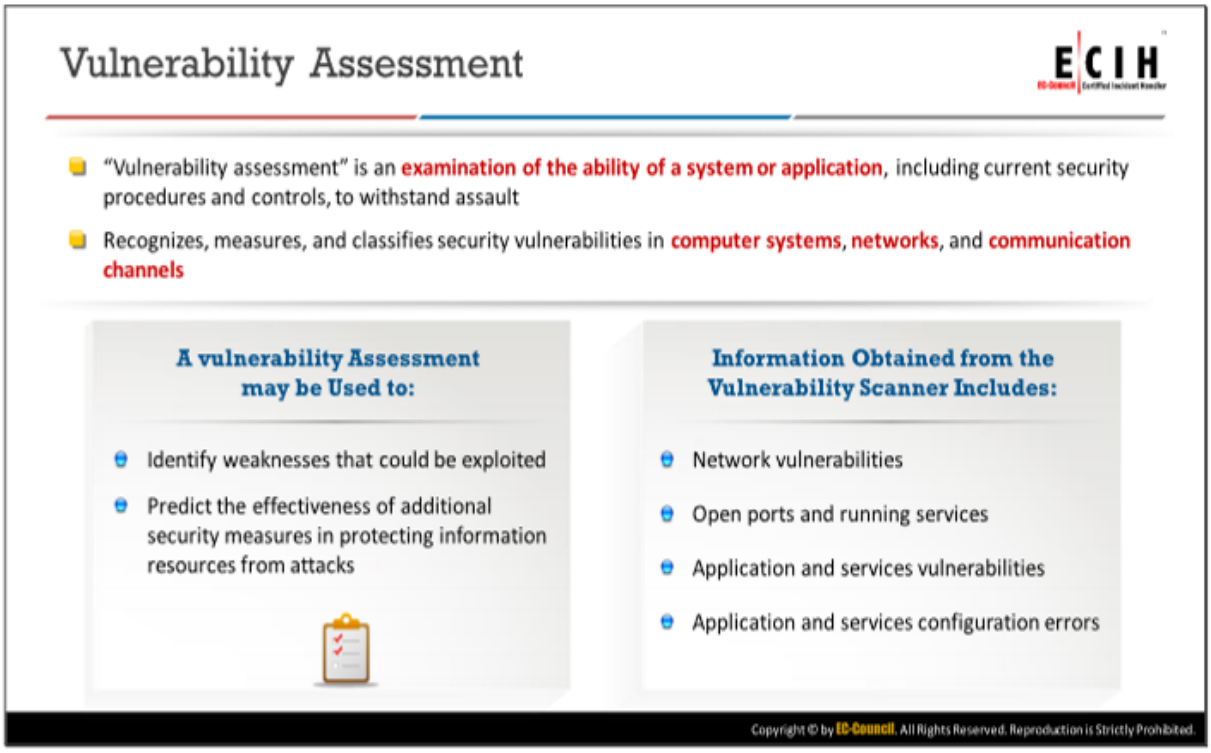
information may be lost or corrupted. Hence, it is important for developers to understand the anatomy of common security vulnerabilities and to develop highly secure applications by providing proper user validation and authorization.

- **Open Services**

  Open ports and services may lead to loss of data, enable DoS attacks, and also allow attackers to perform further attacks on other connected devices. Administrators need to continuously check for unnecessary or insecure ports and services to reduce the risk to the network.

- **Default Passwords**

  Manufacturers provide default passwords to users to access devices during initial setup, and users then need to change the passwords for future use. However, users may forget to update the passwords and continue using the default passwords, making devices and systems vulnerable to various attacks, such as brute-force and dictionary attacks. Attackers can thus exploit this vulnerability to obtain access to the system. Passwords should be kept secret; failing to protect the confidentiality of a password can allow the system to be compromised with ease.



Vulnerability Assessment

Vulnerability assessment is an examination of the ability of a system or application, including its current security procedures and controls, to withstand assault. Vulnerability assessment scans networks for known security weaknesses, and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It also assists security professionals or incident handlers to secure the network by determining security loopholes or vulnerabilities in the current security mechanism before the "bad guys" can exploit them.

A vulnerability assessment may be used to:

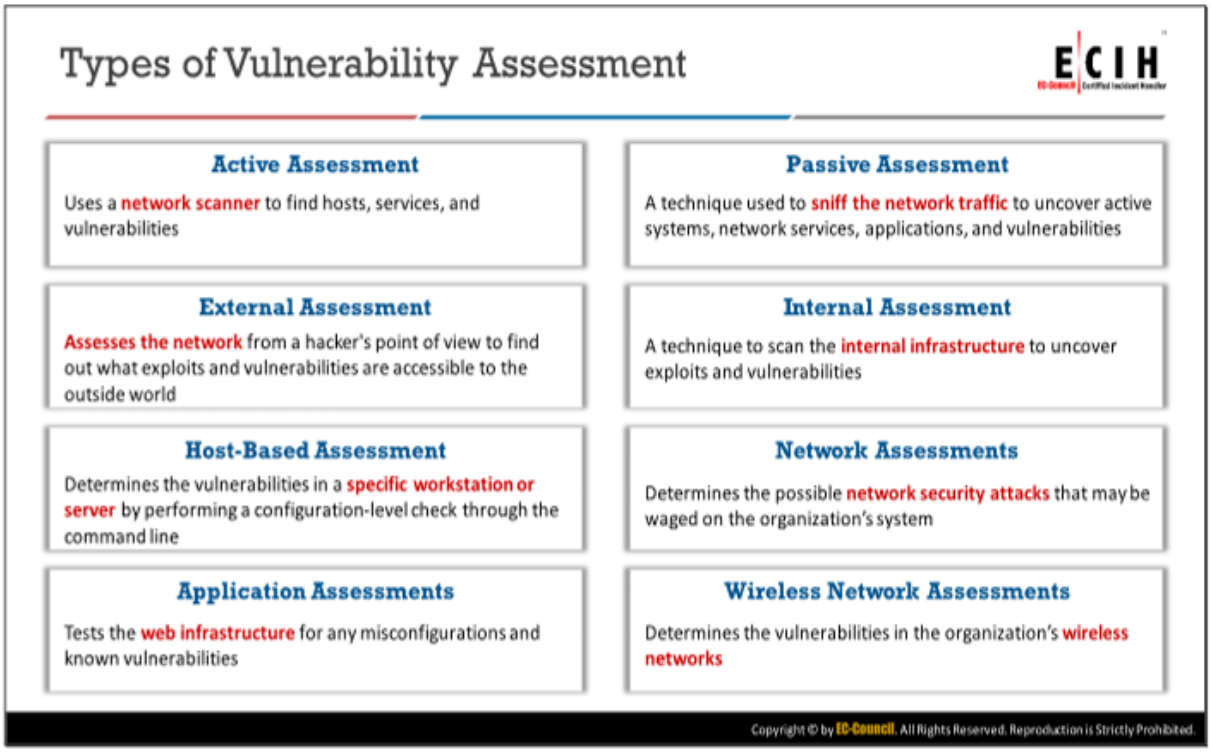
- Identify weaknesses that can be exploited
- Predict the effectiveness of additional security measures in protecting information resources from attack

Typically, vulnerability-scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications. Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

Vulnerability scanners are capable of identifying the following information:

- The OS version running on computers or devices
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening
- Applications installed on computers

- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled
- Mistakes in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities



Types of Vulnerability Assessment

Given below are the different types of vulnerability assessments:

- **Active Assessment**

  Active assessments are a type of vulnerability assessment that uses network scanners to scan the network to identify the hosts, services, and vulnerabilities present in that network. They have the capability to reduce the intrusiveness of the checks they perform.

- **Passive Assessment**

  Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. They also provide a list of the users who are currently using the network.

- **External Assessment**

  External assessments assess the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world. They assess external devices such as firewalls, routers, and servers, estimating the threat from network security attacks external to the organization to determine how secure the external network and firewall are.

  The following are some possible steps in performing an external assessment:

  - Determine the set of rules for firewall and router configurations for the external network.
  - Check whether external server devices and network devices are mapped.

- Identify open ports and related services on the external network.
- Examine patch levels on the server and external network devices.
- Review detection systems such as IDS, firewalls, and application-layer protection systems.
- Get information on DNS zones.
- Scan the external network through a variety of proprietary tools available on the Internet.
- Examine web applications such as e-commerce and shopping cart software for vulnerabilities.

- **Internal Assessment**

  An internal assessment involves scrutinizing the internal network to find exploits and vulnerabilities. The following are some possible steps involved in performing an internal assessment:

  - Specify the open ports and related services on network devices, servers, and systems
  - Check for router configurations and firewall rule sets
  - List the internal vulnerabilities of the operating system and server
  - Scan for Trojans that may be present in the internal environment
  - Check the patch levels on the organization's internal network devices, servers, and systems
  - Check for the existence of malware, spyware, and virus activity and document them
  - Evaluate the physical security
  - Identify and review the remote management process and events
  - Assess the file-sharing mechanism(s) (for example, NFS or SMB/CIFS shares)
  - Examine antivirus implementation and events

- **Host-based Assessment**

  Host-based assessments are a type of security check that entails carrying out a configuration-level check through the command line to check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as incorrect registry and file permissions, as well as software configuration errors. Host-based assessment can use many commercial and open-source scanning tools.

- **Network Assessments**

  Network assessments determine possible network security attacks that may occur on an organization's system. They evaluate the organization's system for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption.

Network assessment professionals use firewall and network scanners such as Nessus that find open ports, recognize the services running on those ports, and find vulnerabilities associated with these services. These assessments help organizations determine how vulnerable systems are to internet and intranet attacks and how an attacker can gain access to important information. A typical network assessment conducts the following tests on a network:

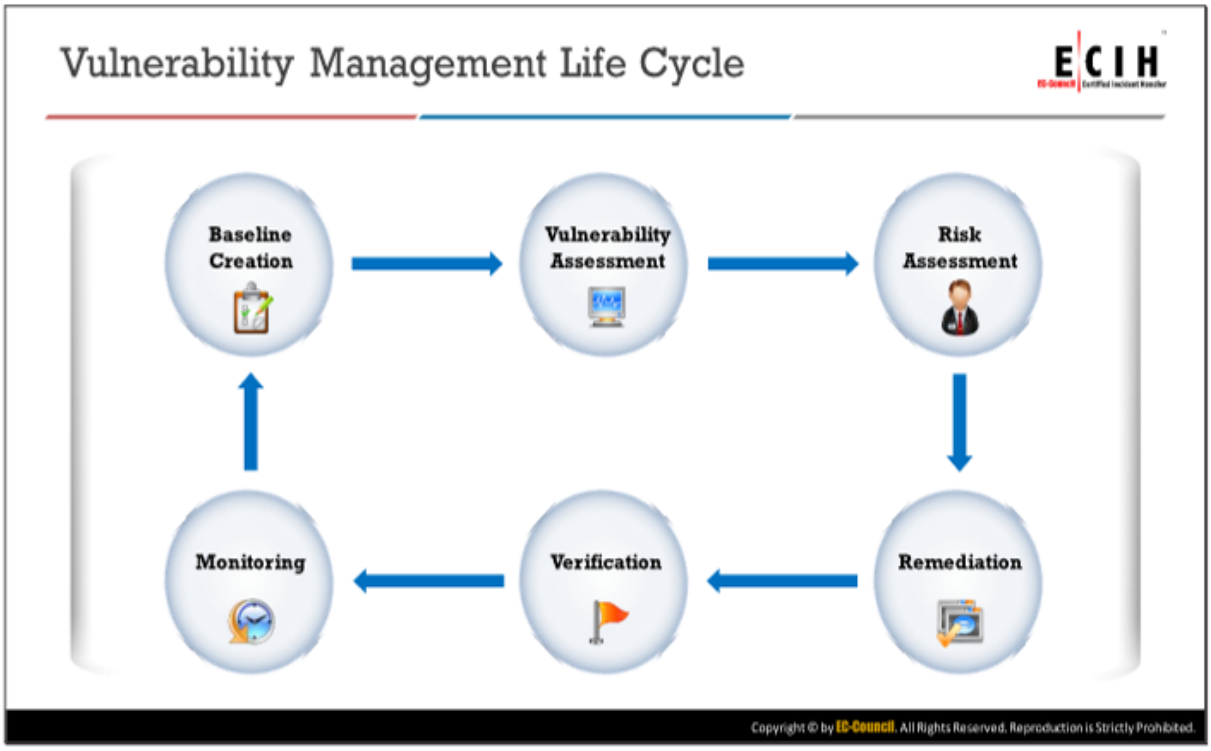
- Checks the network topologies for inappropriate firewall configuration
- Examines the router filtering rules
- Identifies inappropriately configured database servers
- Tests individual services and protocols such as HTTP, SNMP, and FTP
- Reviews HTML source code for unnecessary information
- Performs bounds checking on variables

- **Application Assessments**

  An application assessment focuses on transactional web applications, traditional client-server applications, and hybrid systems. It analyzes all elements of an application infrastructure, including deployment and communication within the client and server. This type of assessment tests the web server infrastructure for any misconfiguration, outdated content, and known vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

- **Wireless Network Assessments**

  Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms; now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and get unauthorized access in order to test wireless networks and identify rogue wireless networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network, sniff wireless network traffic, and try to crack encryption keys.



Vulnerability Management Life Cycle

The vulnerability management life cycle is an important process for finding and remediating security weaknesses before they are exploited. It includes defining the risk posture and policies for an organization, creating a complete asset list of systems, scanning and assessing the environment for vulnerabilities and exposures, and taking action to mitigate the vulnerabilities that are found. Implementation of the vulnerability management life cycle makes insecure computing environments more resilient to attacks.

Vulnerability management should be implemented in every organization to help evaluate and control risks and vulnerabilities in the system. The management process continuously examines the IT environments for vulnerabilities and risks associated with the system.

Organizations should maintain a proper vulnerability management program for ensuring overall information security. Vulnerability management provides best results if it is implemented in a sequence of well-organized phases.

The phases optimally or in principle involved in vulnerability management are:

- **Baseline Creation**

  In this phase, critical assets are identified and prioritized to create a good baseline for vulnerability management.

- **Vulnerability Assessment**

  This is a very crucial phase in vulnerability management. In this step, the security analyst identifies the known vulnerabilities in the organizational infrastructure.

- **Risk Assessment**

  In this phase, all the serious uncertainties that are associated with the system are assessed, fixed, and permanently eliminated to ensure a flaw-free system. Risk assessment summarizes the vulnerability and risk level identified for each of the selected assets, whether high, moderate, or low.

- **Remediation**

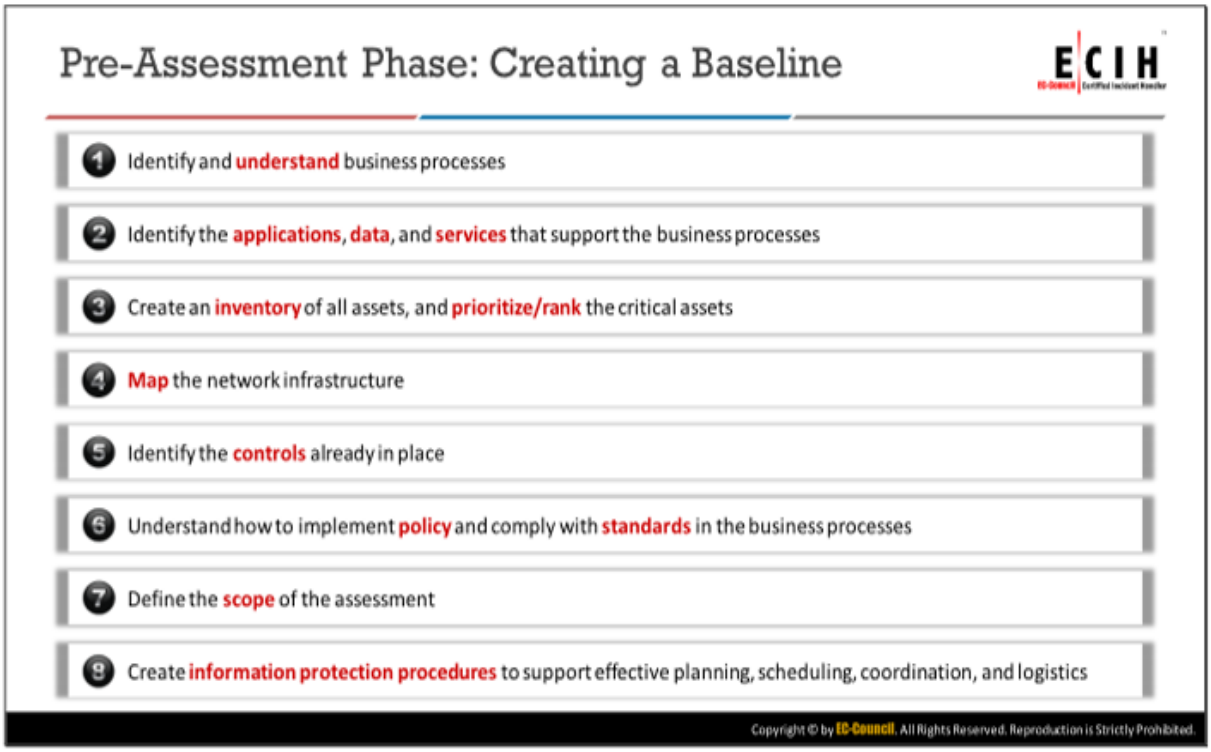
  Remediation is the process of reducing the severity of vulnerabilities. This phase is initiated after the successful implementation of baselining and assessment steps.

- **Verification**

  This phase provides clear visibility into the firm and allows the security team to check whether all the previous phases are perfectly applied and employed. Verification can be performed using various means such as ticking systems, scanners, and reports.

- **Monitoring**

  Regular monitoring needs to be performed to maintain system security using tools such as IDS/IPS and firewalls. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved.



Pre-Assessment Phase: Creating a Baseline

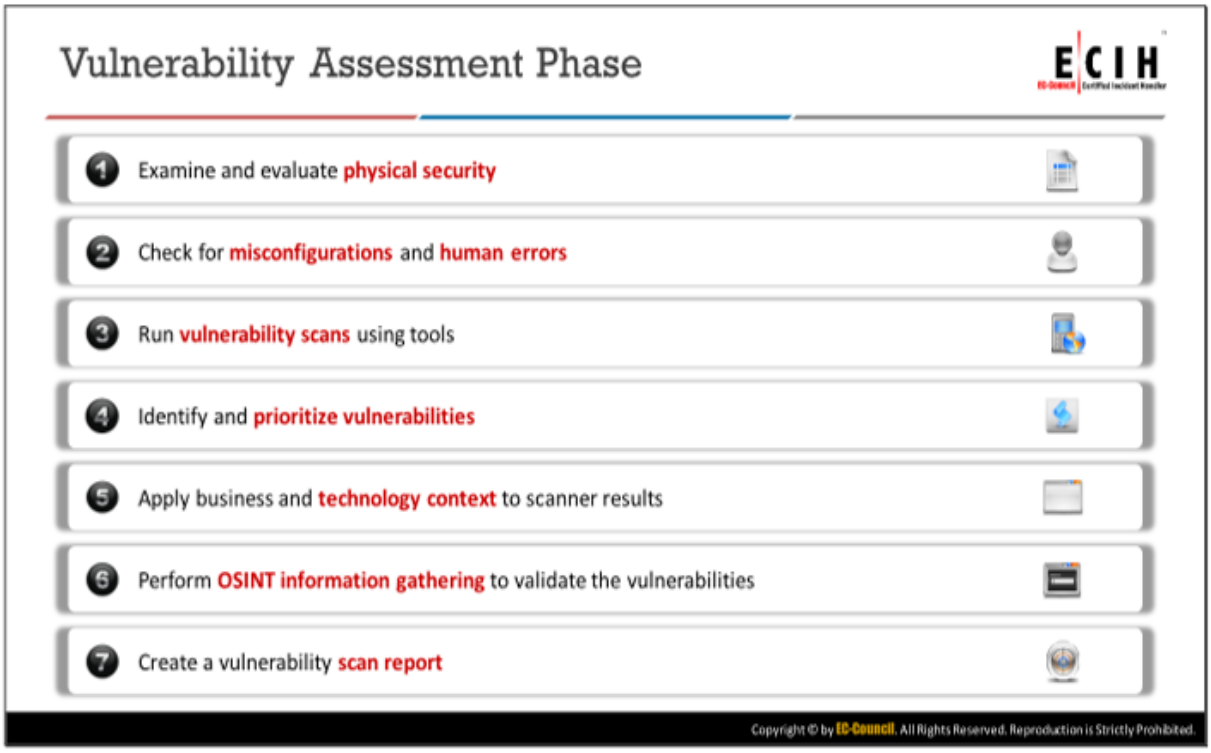
The pre-assessment or preparatory phase includes defining policies and standards, the scope of assessment, and appropriate information protection procedures and identifying and prioritizing critical assets to create a good baseline for vulnerability management.

Steps involved in creating a baseline:

1. Identify and understand business processes
2. Identify the applications, data, and services that support the business processes
3. Create an inventory of all assets and prioritize/rank critical assets
4. Map the network infrastructure
5. Identify the controls already in place
6. Understand policy implementation and standards compliance within/of business processes
7. Define the scope of the assessment
8. Create information protection procedures to support effective planning, scheduling, coordination, and logistics

Classify identified assets according to business needs. Classification helps identify high risks in an organization, prioritizing the rated assets based on the potential impact of their failure and on their reliability in the business's context. Prioritization helps with:

- Evaluating and deciding on solutions to the consequence of the assets failing
- Examining the risk tolerance level
- Organizing methods for prioritizing assets



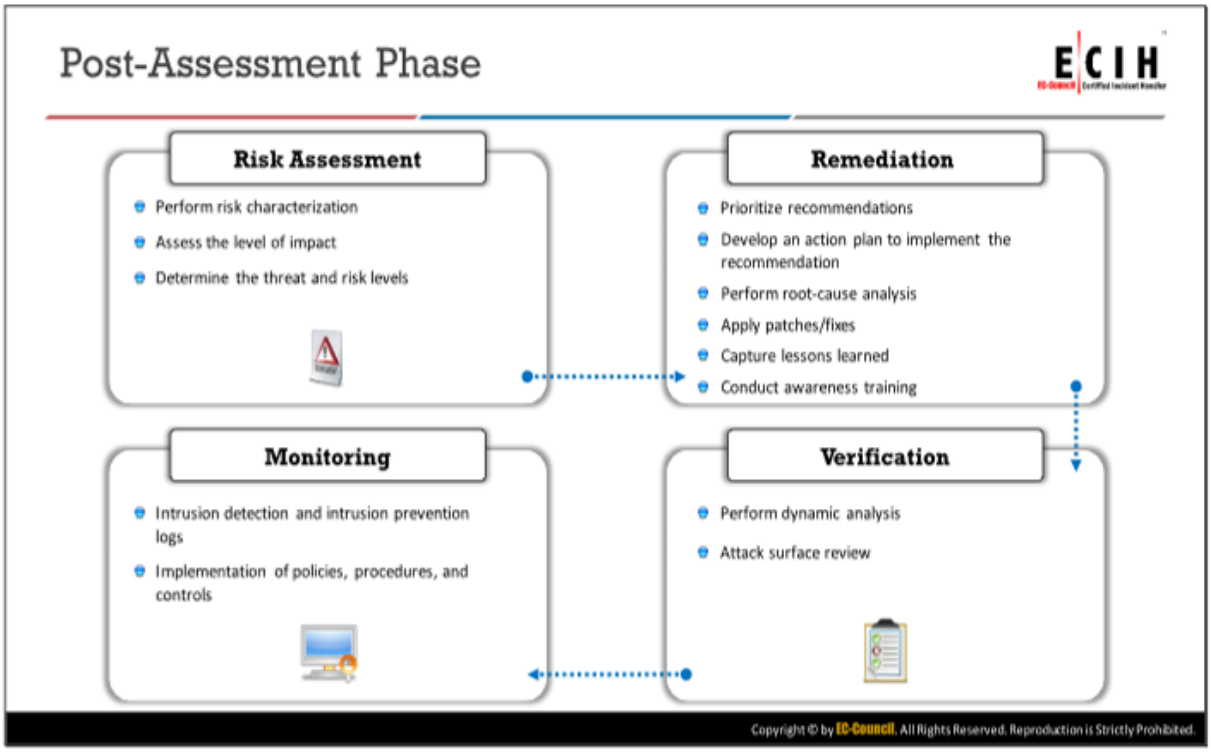
Vulnerability Assessment Phase

The vulnerability assessment phase involves identifying vulnerabilities in the organizational infrastructure, including operating systems, web applications, and web servers. It helps identify the category and criticality of the vulnerabilities in an organization and minimize the levels of risk. The ultimate goal of vulnerability scanning includes scanning, examining, evaluating, and reporting vulnerabilities in the organization's information system.

The assessment phase involves examining the architecture of the network, evaluating threats to the network environment, performing penetration testing, examining and evaluating physical security, analyzing physical assets, assessing operational security, observing policies and procedures, and assessing infrastructure interdependencies.

Steps involved in assessment phase:

1. Examine and evaluate physical security
2. Check for misconfigurations and human errors
3. Run vulnerability scans using tools
4. Identify vulnerabilities and prioritize them by severity
5. Apply business and technology context to scanner results
6. Perform OSINT information gathering to validate the vulnerabilities
7. Create a vulnerability scan report



Post-Assessment Phase

The post-assessment phase is also known as the recommendation phase, and is performed after and based on risk assessment. Risks are characterized or categorized by key criteria, which helps to prioritize the list of recommendations.

The tasks performed in the post-assessment phase include:

- Making a priority list for assessment recommendations
- Developing action plans to implement the proposed recommendations
- Capturing lessons learned to improve the overall process in the future
- Conducting training for employees

Post-assessment includes risk assessment, remediation, verification, and monitoring.

- **Risk Assessment**

  In the risk assessment phase, risks are identified, characterized, and classified along with the techniques used to control or reduce their impact. This is an important step in identifying security weaknesses in the IT architecture of an organization.

  The tasks performed in the risk assessment phase include:

  - Perform risk characterization
  - Assess the level of impact
  - Determine the threat and risk level

- **Remediation**

  Remediation refers to the steps that are taken to mitigate found vulnerabilities, such as evaluating them, accessing risks, and designing responses for the vulnerabilities. It is important for the remediation process to be specific, measurable, attainable, relevant, and time-bound.

  The tasks performed in the remediation phase include:

  - Prioritizing recommendations
  - Developing action plans to implement the recommendations
  - Performing root-cause analysis
  - Applying patches/fixes
  - Capturing lessons learned
  - Conducting awareness training

- **Verification**

  The verification phase helps security analysts verify whether all previous phases were soundly implemented. It includes the verification of remedies taken for the mitigation of risk.

  The tasks performed in the verification phase include:

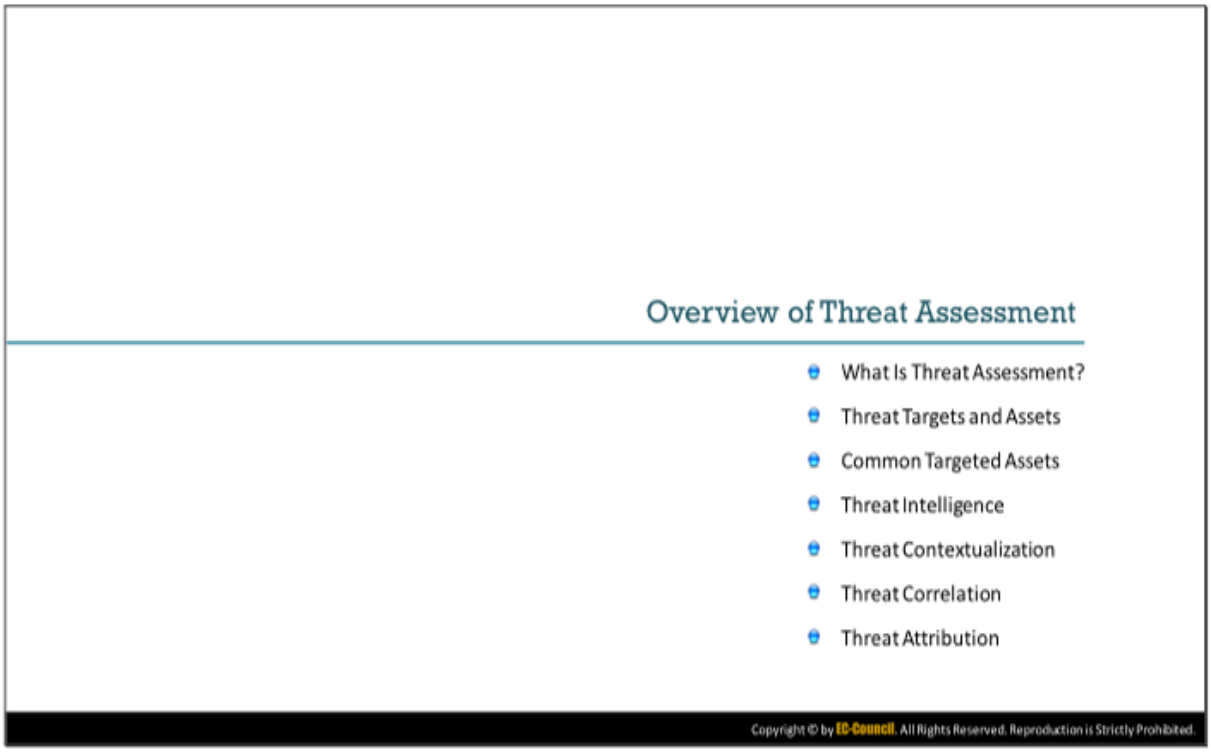
  - Perform dynamic analysis
  - Attack surface review

- **Monitoring**

  In this phase, incident monitoring is performed using tools such as IDS/IPS, SIEM, and firewalls. This phase implements continuous security monitoring to thwart ever-evolving threats.

  The tasks performed in the monitoring phase include:

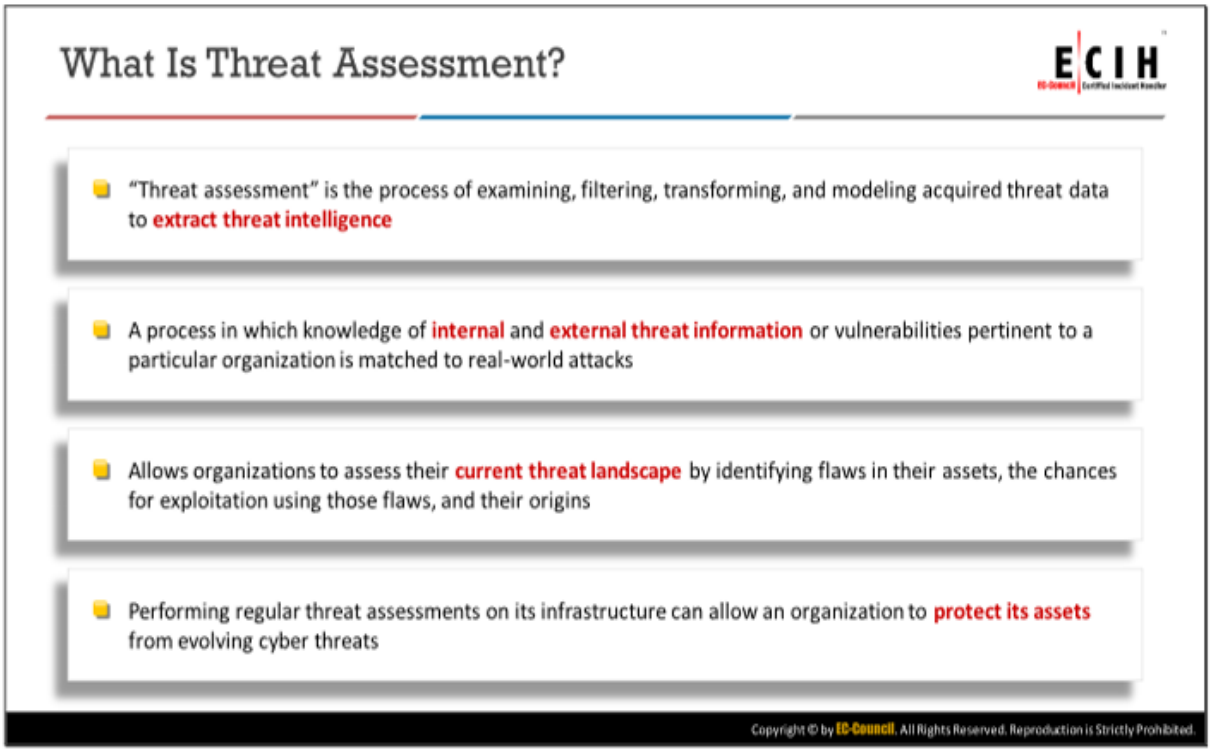
  - Monitoring intrusion detection and intrusion prevention logs
  - Implementation of policies, procedures, and controls



Overview of Threat Assessment

Organizations need to perform continuous threat assessment to keep their cybersecurity posture strong against evolving, multifaceted, sophisticated cyberattacks. Threat assessment helps organizations build a strong protection plan that addresses evolving threats before they cause any damage to organizational assets.

This section gives an overview of threat assessment, threat targets and assets, threat intelligence, threat contextualization, threat correlation, and threat attribution.



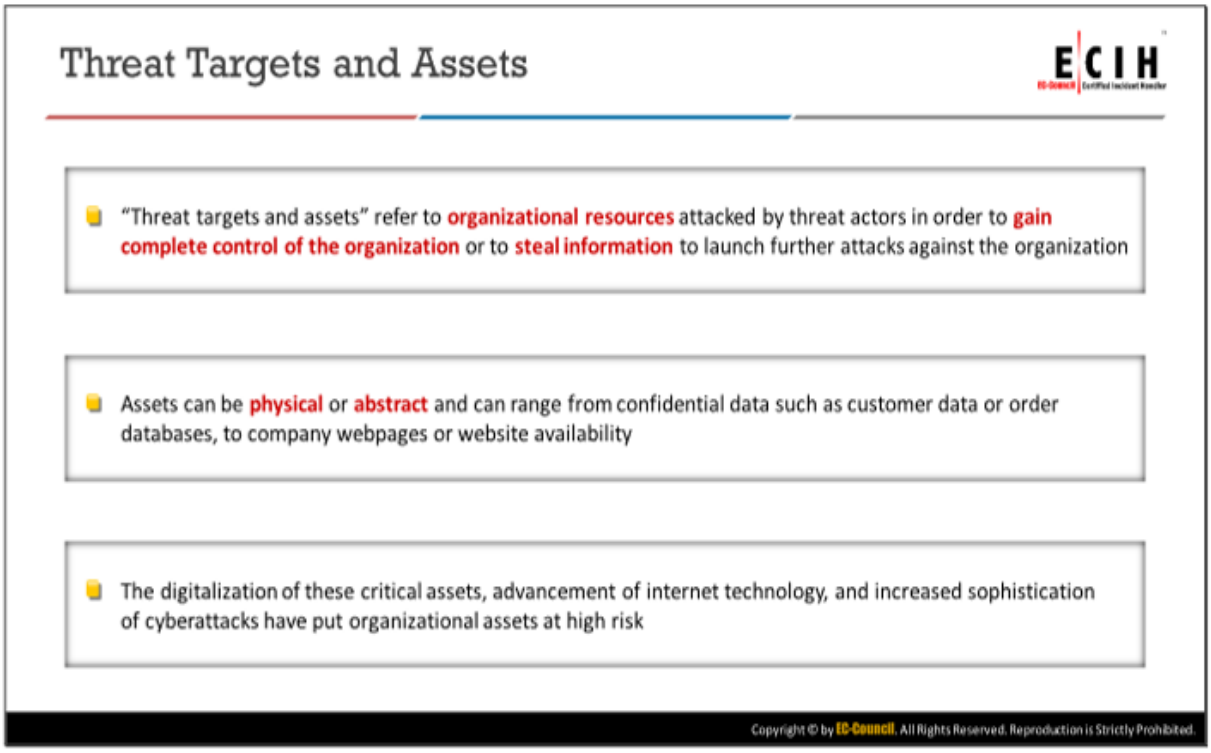
What Is Threat Assessment?

Threat assessment is the process of examining, filtering, transforming, and modeling of acquired threat data to extract threat intelligence. It is a process where the knowledge of internal and external threat information or vulnerabilities pertinent to a particular organization is matched to real-world attacks. Threat assessment allows organizations to assess their current threat landscape by identifying flaws in their assets, chances of exploiting those flaws, and their origin. Regular threat assessment enables the organization to predict, prevent, and combat possible threats to the organization.

The definition of threat and the nature of threat assessment vary from industry to industry and organization to organization, depending on organizational requirements. Threat assessment improves the security measures of the organization by providing insights into internal and external threat data.

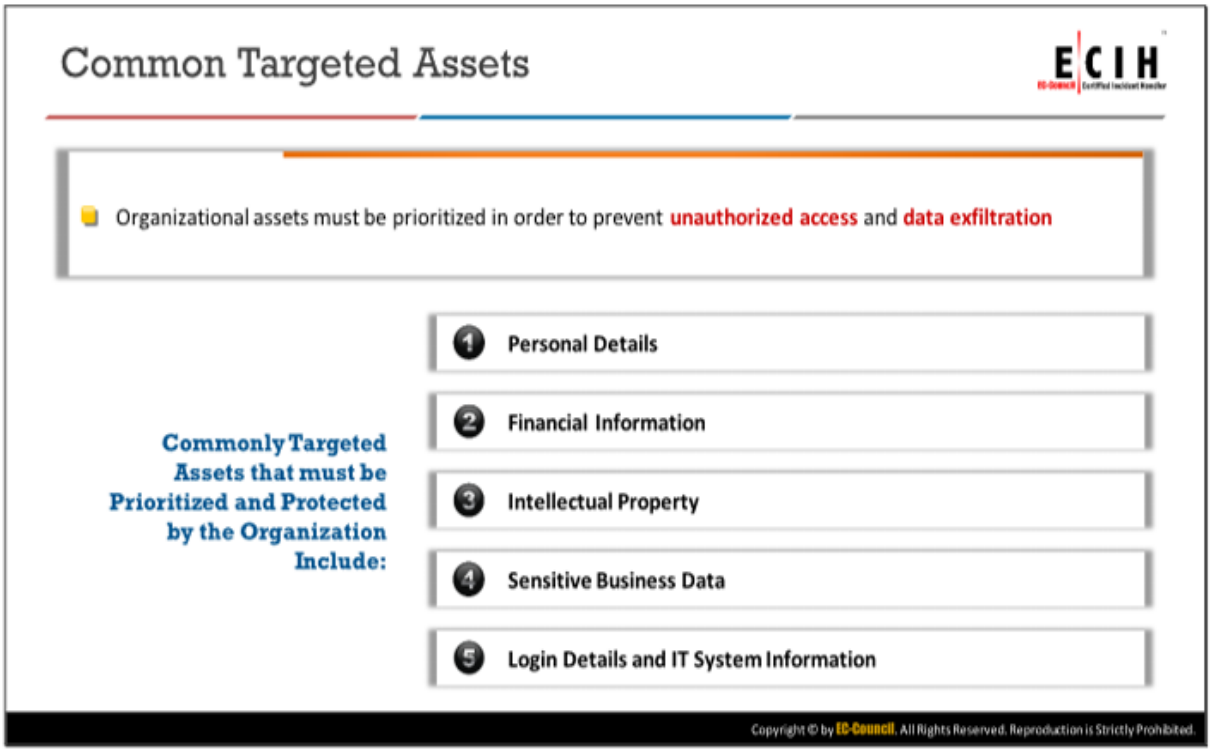
Organizations need to perform continuous threat assessment for the following reasons:

- Threats change constantly as attackers try to compromise the networks with new techniques.
- There is no way to predict how threats will evolve or from which direction they will come.
- Simply implementing extreme security measures cannot protect the environment. Evolving threats may affect business operations and lead to loss of revenue.
- Threat assessment allows organizations to think wisely about how to invest revenue in the protection of resources and how to avoid unnecessary expenditure.



Threat Targets and Assets

Threat target and assets are the organizational resources attacked by threat actors in order to gain control of or steal information and launch further attacks on the organization. Assets can be either physical or abstract, ranging from confidential data such as customer data or orders data to the company's web pages or website access. Due to the increase in global industrial competition and the resulting increased importance of certain critical information, organizational assets have become an ever more valuable target for threat actors. The digitalization of these critical assets, advancement in internet technology, and the increased sophistication of cyberattacks have put organizational assets at high risk.



Common Targeted Assets

Many organizations keep their critical data in cloud or digital sources. This data may include personal information such as employee and customer records, information on business infrastructure and strategies, and financial records, among others. Protection of these assets must be prioritized in order to prevent unauthorized access and data exfiltration.

Some commonly targeted assets that must be prioritized for protection by organizations include:

- **Personal Details**

  Personal information of employees, such as social security number (SSN), sensitive personal information (SPI), or personal identifiable information (PII), can be used to trace a person's identity; this may include their name, birthday, medical information, address, national identification number, and so on. Information obtained from PII can be used to carry out phishing attacks, create fake accounts, obtain financial records, and so on, or to launch spear phishing attacks against a target organization.

- **Financial Information**

  Credit card details, account numbers, online banking credentials, and ATM pins are valuable information that can be used by threat actors to steal money, sell information on the black market, open fake accounts, and so on. Losing financial information can lead to loss of customers, business disruption, regulatory fines, legal costs, and data breach notification charges.

- **Intellectual Property**

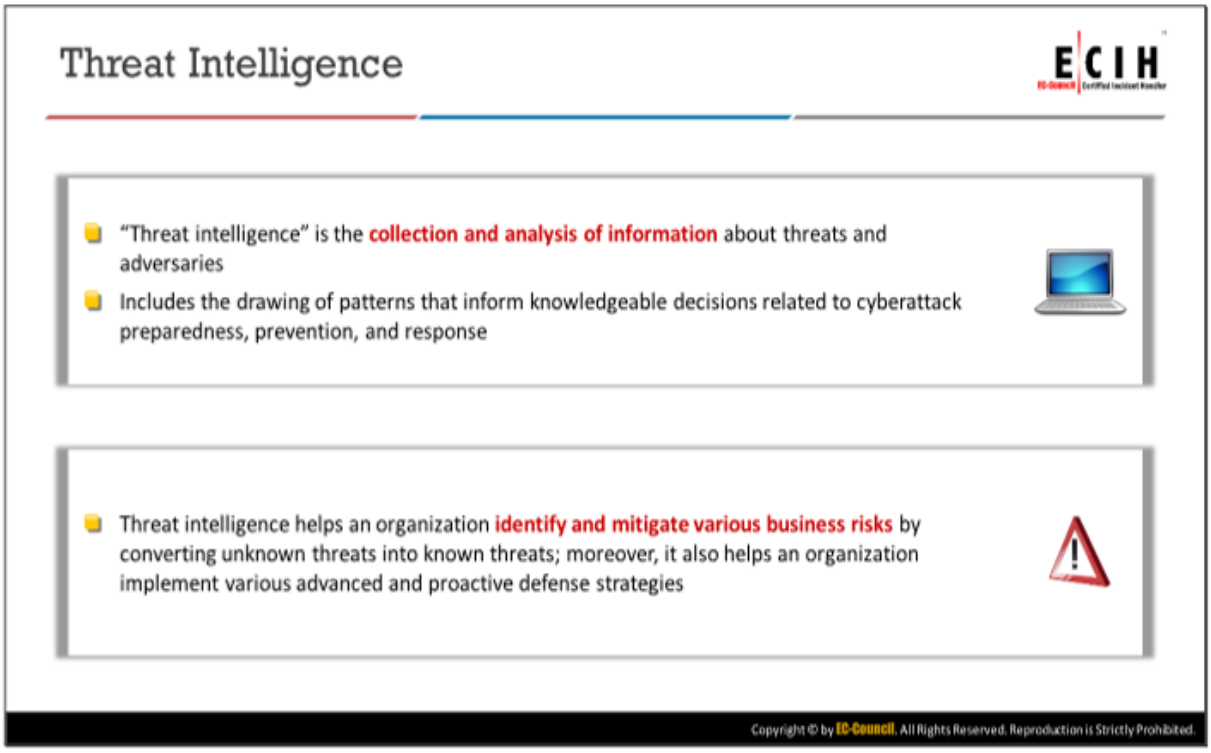
  Intellectual property (IP) includes business designs and infrastructure, technical content, software programs, product descriptions or manuals, and so on. Loss of intellectual property can result in a violation of contractual obligations, loss of clients, lowered revenues, and eroding profits.

- **Sensitive Business Data**

  Sensitive business data involve any information that poses a risk to the organization's security and reputation: financial records, business tactics, trade secrets, contact information, customer information, acquisition plans, competitive bid information, and so on. With the increase in the data generated by the business sector, organizations must incorporate methods in their security infrastructure to protect their crucial data against unauthorized access and other attacks.

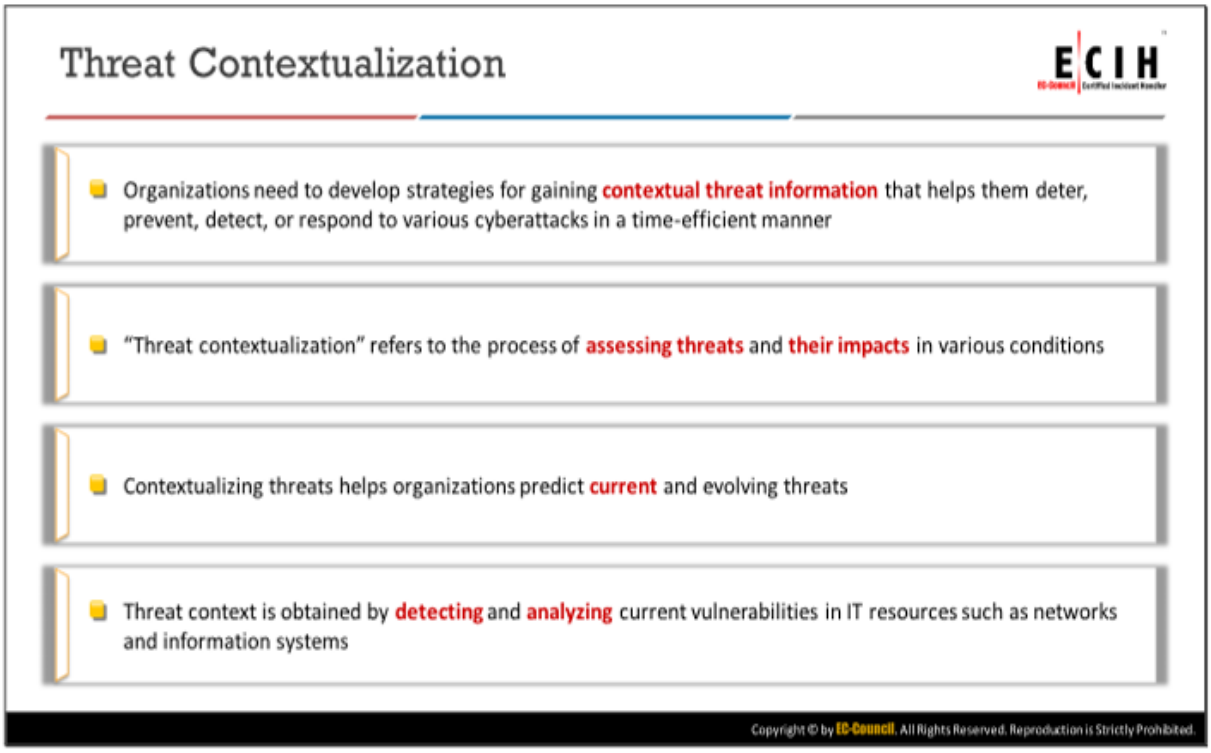
- **Login Details and IT System Information**

  Login credentials and information about IT systems are extremely important to threat actors, as they can be the first step in getting a foothold in the target organization before launching further attacks. That is, gaining access to a single system can open the door for a threat actor to access other systems present in the target network. Therefore, suppliers, service providers, and third parties must keep their login credentials safe from threat actors.



Threat Intelligence

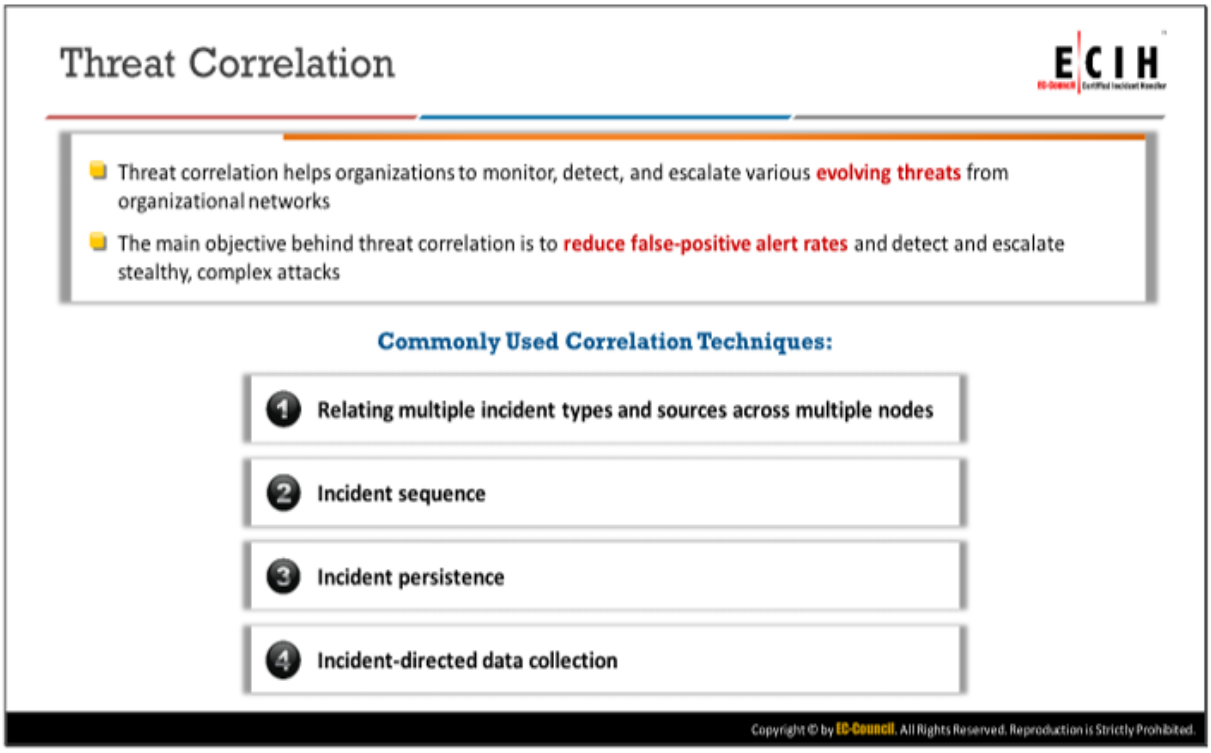
Threat intelligence, usually known as cyber threat intelligence (CTI), is defined as the collection and analysis of information about known and unknown threats and adversaries and drawing patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against cyberattacks. Any knowledge about threats that results in the planning and decision-making in an organization to handle it is threat intelligence. The main aim of CTI is to make the organization aware of existing or emerging threats and prepare a proactive cybersecurity posture before these threats can manifest. This process, where unknown threats are converted into the possibly known ones, helps anticipate the attack before it can happen and ultimately results in a better and more secure system in the organization, in turn protecting the viability of secured data sharing and transactions among organizations globally.



Threat Contextualization

Nowadays, almost all organizations are extensively connected to the internet and are more susceptible than previously to cyberattacks. Among the information important to thwart cyberattacks and protect organizational assets from evolving threats is contextual threat information that helps to deter, prevent, detect, or respond to various cyberattacks in a timely manner; organizations thus need strategies for gathering such information. It is not possible to protect organizations from all threats, but determining the context of a current or potential threat across various IT assets and networks of an organization may lead to a more successful, stronger cybersecurity posture.

Threat contextualization refers to the process of assessing threats and their impacts under various (contextual) conditions. Threat context is obtained by detecting and analyzing current vulnerabilities in the IT resources, such as networks and information systems. Threat analytics help organizations detect incidents, identify infected systems, trace infection vectors, analyze actions and events occurring after infection, and finally determine the impact of incidents. This helps organizations identify malicious and other anomalous actions and extract real-time context of threats to combat threats.



Threat Correlation

Threat correlation helps organizations monitor, detect, and escalate evolving threats to organizational systems and networks. The main objective of threat correlation is to reduce false-positive alert rates and detect and escalate stealthy, complex attacks. Threat correlation helps incident response teams mainly focus on topmost priority issues, reducing potential risk and corporate liabilities.

The main aim behind the collection of valuable threat data from different security systems and application platforms is to find correlations between threat data in order to provide accurate and timely information to incident handling teams.

Discussed below are the most commonly used correlation techniques:

- **Relating Multiple Incident Types and Sources across Multiple Nodes**

  In order to recognize an incident as harmful, it is necessary to use incident data from various sources and nodes. The correlation mechanism must have the capability of processing data irrespective of its origin.

- **Incident Sequence**

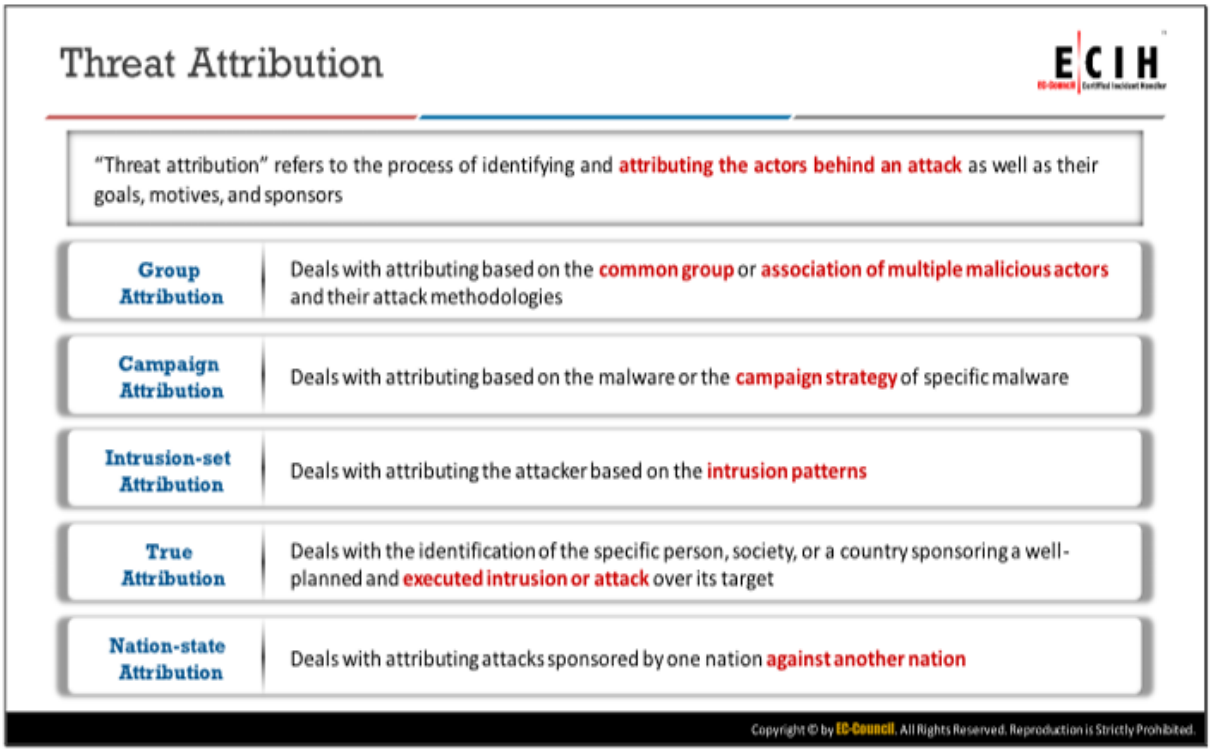
  Past security incidents faced by an organization might influence security-related decisions taken presently. For instance, scanning a single port in the network cannot determine anything; instead, comparison of past short- and long-term incidents can be used to obtain valuable information, which can then be used to take immediate security action.

- **Incident Persistence**

  A prolonged and targeted incident on a network can indicate an attack. For instance, a small amount of traffic on an organizational network can be considered normal, whereas continuous incoming traffic can indicate a denial-of-service attack. Therefore, in order to encounter such incidents, the correlation mechanism must have the capability of identifying incident persistence over time.

- **Incident-directed Data Collection**

  In many situations, it is necessary to interact with other systems in the network in order to complete the correlation process. For example, in correlating threat data, simple security data are not sufficient; data such as customer databases, network devices, asset databases, and other information may be required for effective threat correlation.



Threat Attribution

Threat attribution is the process of identifying and attributing actors behind an attack, their goals and motives, and the sponsors. It also involves analyzing threats to obtain indicators of compromise (IoCs) and derive threat intelligence from such analysis.

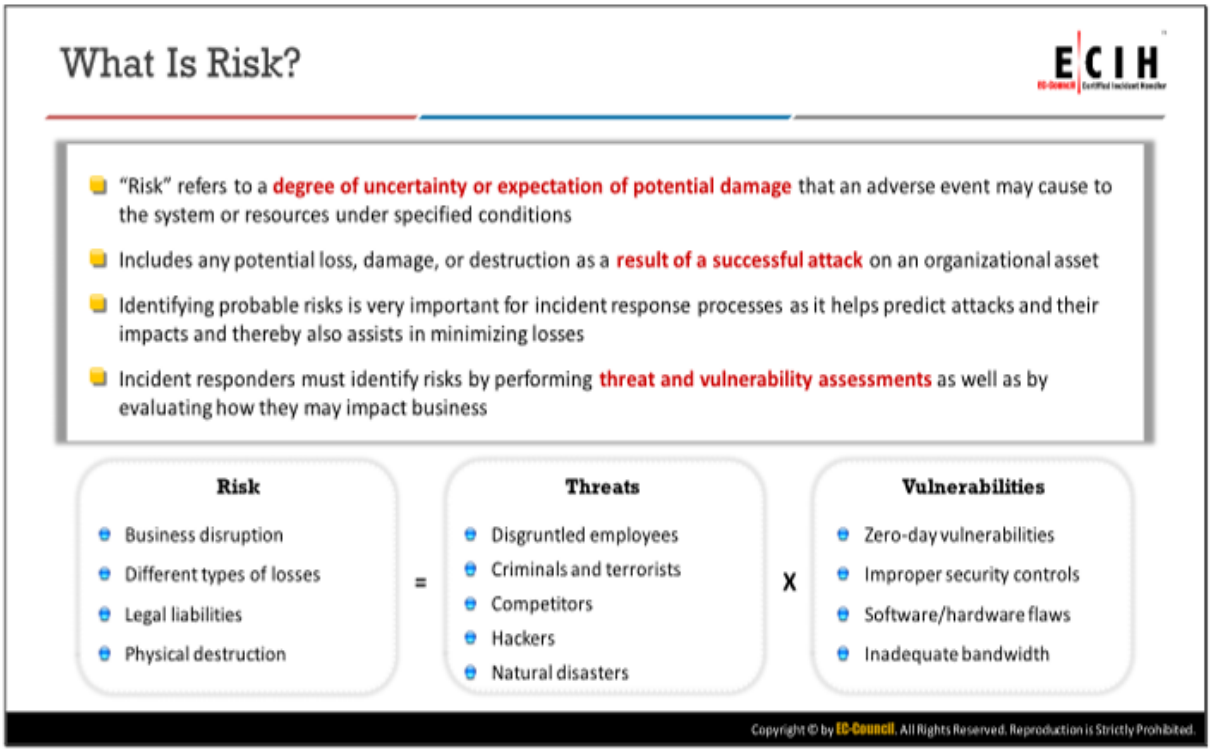
Discussed below are different types of attributions:

- **Group Attribution:** Attribution based on the common grouping or association of multiple malicious actors and their attack methodologies.
- **Campaign Attribution:** Attribution based on the malware or the campaign strategy of specific malware.
- **Intrusion-set Attribution:** Attribution the attacker based on the intrusion patterns.
- **True Attribution:** Identification of a specific person, society, or country sponsoring a well-planned and executed intrusion into or attack on its target.
- **Nation-state Attribution:** Attribution of attacks sponsored by any nation against another nation.

Understanding Risk Management

Establishing an appropriate risk management plan helps organizations face unexpected incidents, minimize risks, and reduce the cost of incidents. Having knowledge of risks or incidents before they occur and developing a proper risk management plan helps protect the organization from evolving risks and threats.

This section explains in detail about risk, the risk management process, risk assessment steps, risk mitigation, controlling risks, risk management plan evaluation and updating, the NIST risk management framework, and risk assessment and management tools.



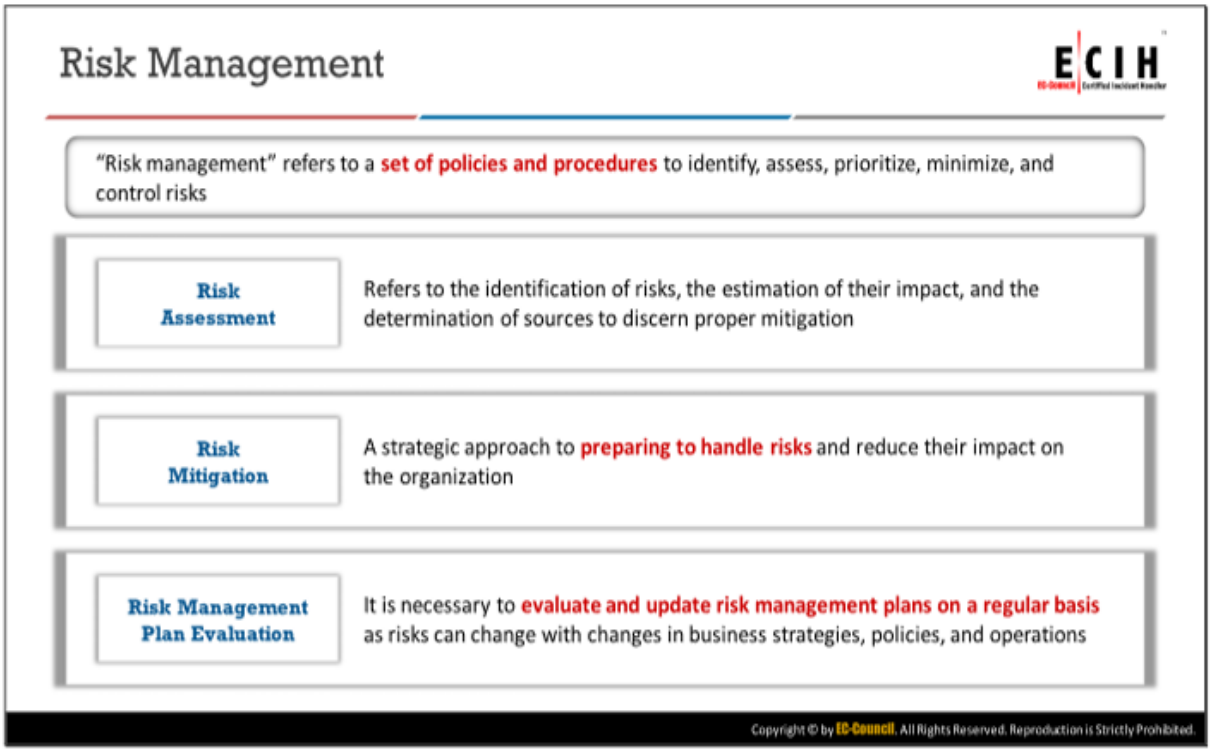
What Is Risk?

Risk refers to a situation involving exposure to danger or the possibility that something unpleasant or unwelcome will happen, with a degree of uncertainty about expected or potential damage that an adverse event may cause to the system or resources. A cybersecurity risk is anything that leads to the loss of expensive assets, revenue, reputation, or similar due to the failure of an organization's information systems as a result of a successful cyberattack.

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 from either 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.

Identifying risks is very important for incident response processes, as it helps in predicting attacks and their impacts and prepares to minimize losses. Incident responders must identify risks by performing assessments of threat, vulnerability, and impact.



Risk Management

Risk management refers to policies and procedures to identify, assess, prioritize, minimize, and control risks. It has a prominent place throughout the security life cycle and is a continuous and ever more complex process. Types of risks vary from organization to organization, but the need to prepare a risk management plan is common among all organizations.

Listed below are the objectives of risk management:

- Identifying the potential risks is the main objective.
- Identifying the impact of risks and helping the organization develop better risk management strategies and plans.
- Prioritizing risks depending on their severity and using established risk management methods, tools, and techniques to assist.
- Analyzing and understanding risks and reporting identified risk events.
- Controlling risks and mitigating their effects.
- Creating awareness among security staff and developing risk management strategies that last.

Risk management is a continuous process performed by achieving defined goals at every phase to maintain risk at an acceptable level in all strategic and operational contexts and network locations relevant to the organization.

There are several standards developed effectively to implement risk management process in organizations, such as ISO 31000 2009 - Risk Management Principles and Guidelines, ISO/IEC 31010:2009 - Risk Management—Risk Assessment Techniques, and COSO 2004 - Enterprise

Risk Management—Integrated Framework. As risk management is a continuous process, organizations must regularly supplement and update their processes accordingly.

The risk management process includes the following phases:

- **Risk Assessment**

  Risk assessment refers to identification of risks, estimation of their impact, and determination of sources to recommend proper mitigation measures. Identification of risk is the initial step of the risk management plan; it entails identifying sources, causes, consequences, and so on of internal and external risks affecting the security of the organization before they cause harm to the organization. This process depends on the skill set of the people involved and differs from one organization to the other.

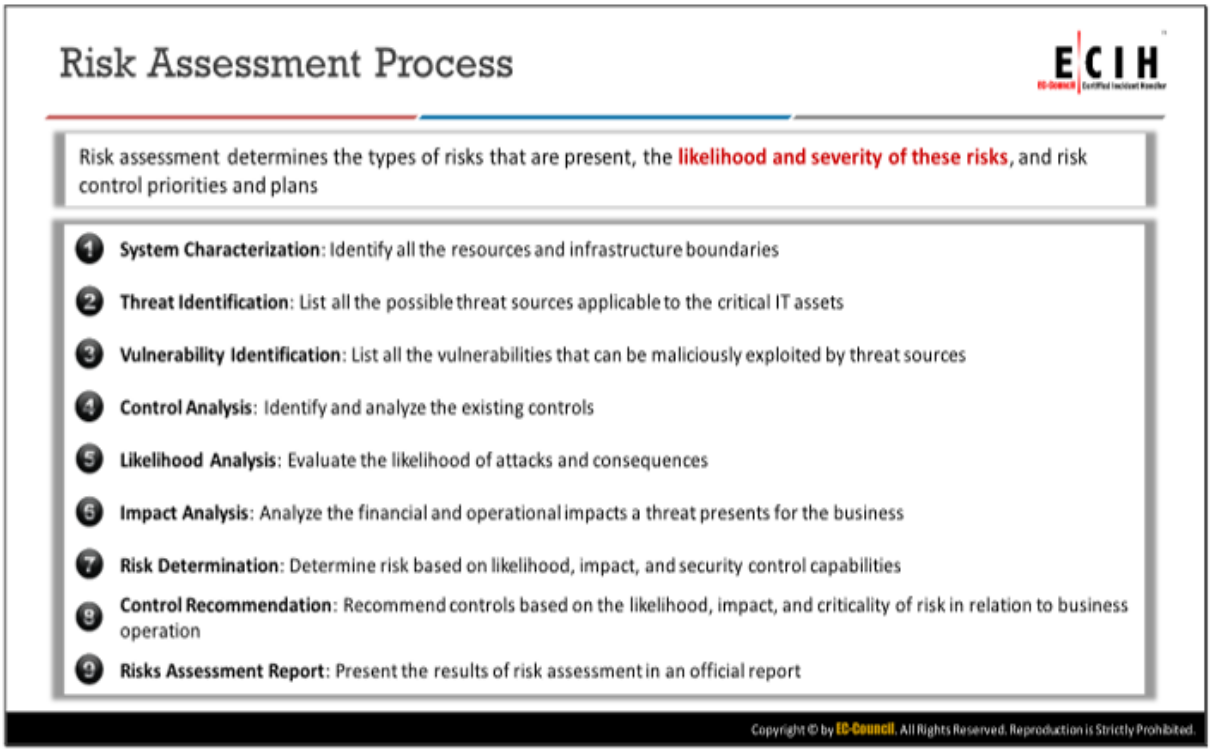
  The process of identifying hazards that could have some negative impact on an organization's business process. This will help in identifying potential business risks and inform the development of measures, processes, and controls to minimize the impact.

- **Risk Mitigation**

  Risk mitigation is a strategic approach to handling risks and reducing their impact on organizations. It treats risks according to their severity level.

- **Risk Management Plan Evaluation**

  It is important for organizations to update their risk management plan on a regular basis, as risks can change due to changes in business strategies, policies, and operations.



Risk Assessment Process

Risk assessment determines the kind of risks present, the likelihood and severity of risk, and the priorities and plans for risk control. It is an ongoing iterative process that 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.

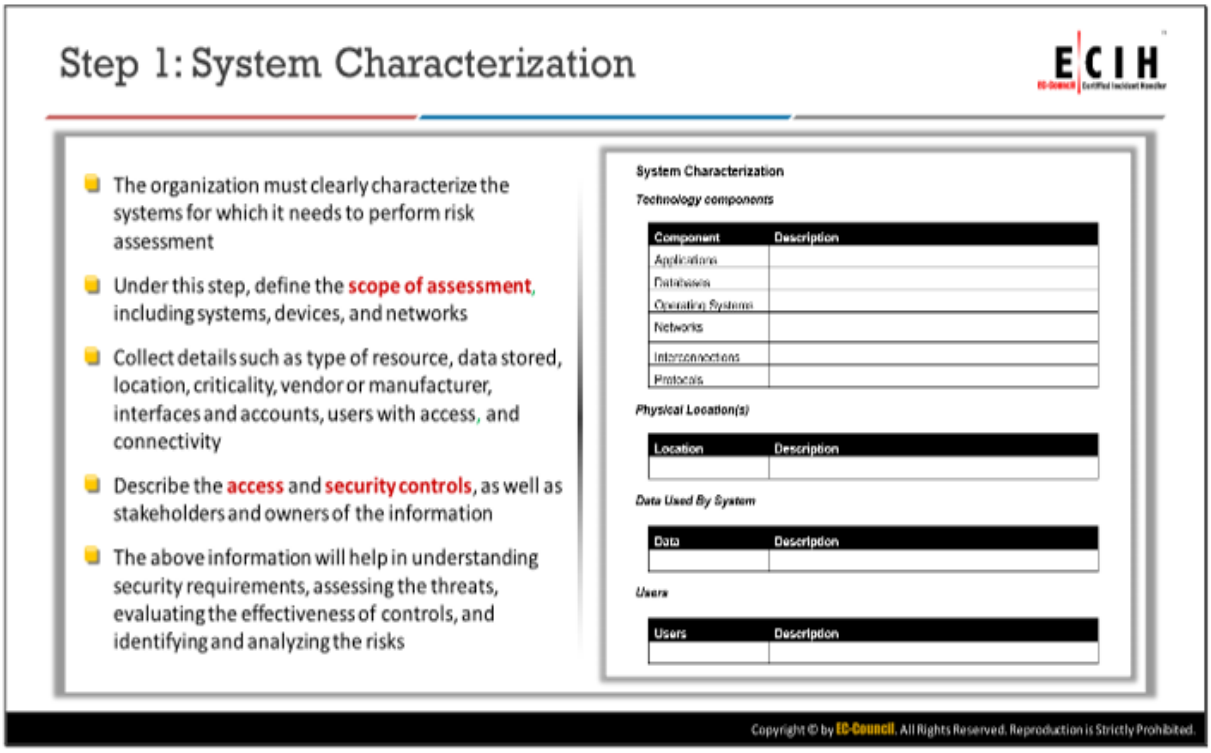
Generally, organizations perform risk assessment when they identify a hazard but are not able to control it immediately. After risk assessment, update of all information facilities is needed at regular intervals.

This allows incident responders to perform various tasks like risk assessment preparation, risk assessment processing, communication with management, and risk assessment maintenance.

The following are steps involved in risk assessment:

- **System Characterization**: Identify all relevant resources and infrastructure boundaries.
- **Threat Identification:** List all possible threat sources applicable to critical IT assets.
- **Vulnerability Identification:** List all vulnerabilities.
- **Control Analysis**: Identify and analyze existing controls.
- **Likelihood Analysis**: Evaluate the likelihood of attacks and their consequences.
- **Impact Analysis**: Analyze the financial and operational impact of a threat over the business.
- **Risk Determination:** Determine risk based on likelihood, impact, and capability of security controls.

- **Control Recommendation:** Recommend controls based on the likelihood, impact, and criticality of risk for business operations.
- **Risks Assessment Report:** Present the results of risk assessment in an official report.



Step 1: System Characterization

An organization must clearly characterize the scope of the systems and resources for which it needs to perform risk assessment. This scope must include all networking devices such as systems, servers, and security control systems, and the type of the data that they contain.

To identify the risks in an organization, responders must have knowledge about the assets involved in risk assessment. They must obtain details such as type of resource, data stored, location, criticality, vendor or manufacturer, interfaces and accounts, users having access and connectivity, access and security controls, and stakeholders and owners of the information. This information will help them understand security requirements, assess threats, evaluate the effectiveness of security controls, and so on.

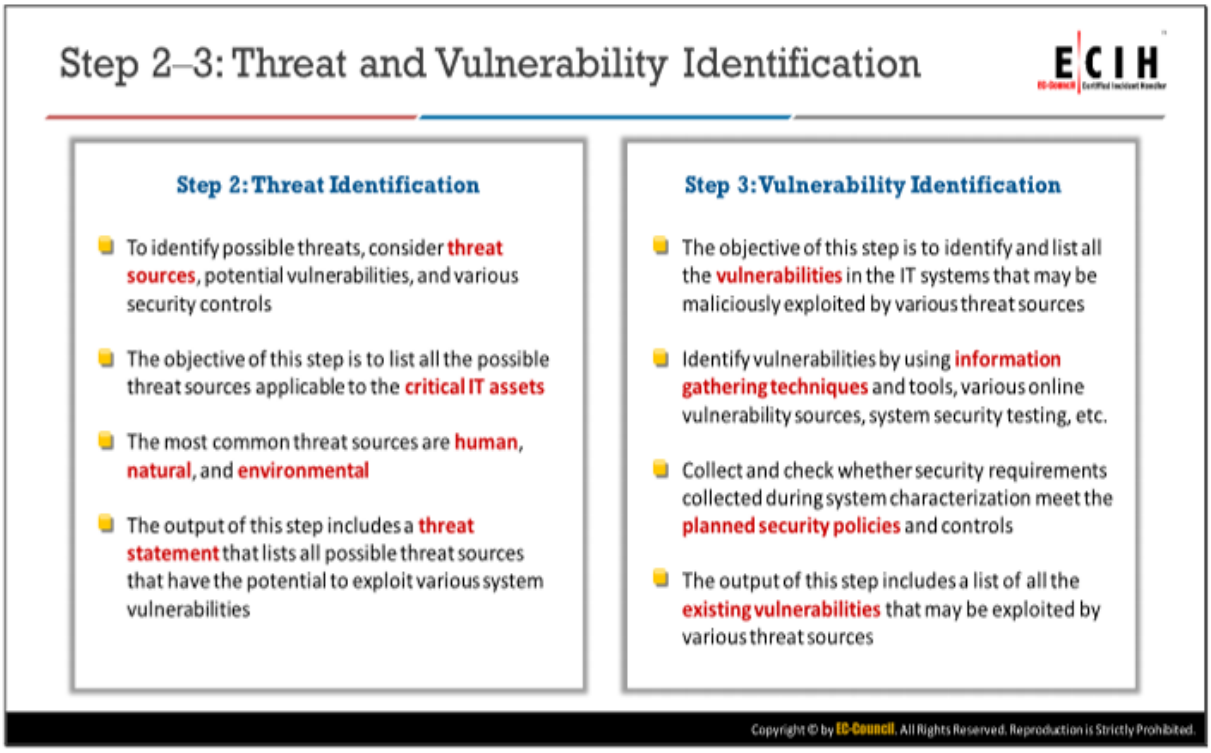
To perform risk assessment, incident responders need to collect the following details:

- System software details
- System peripheral details
- Data processed by systems
- Critical systems and data
- System and data sensitivity levels
- Users of the systems
- Security policies implemented
- System security architecture and network topology
- Technical, management, and operational controls used for the systems

Techniques used by incident responders to gather the abovementioned information include:

- Questionnaires to collect information from management and team members responsible for designing and deploying these systems
- Site visits to examine the surroundings of relevant devices and collect data from them
- Gathering information from security policy documents, system documents, and so on
- Using various tools available to scan systems and obtain details

All this information will help responders understand security requirements, assess threats, evaluate the effectiveness of security controls, identify and analyze risks, and calculate their impact.



Step 2: Threat Identification

After performing system characterization, incident responders need to identify possible threats to critical organizational assets—the primary objective of the risk assessment process. To identify possible threats, the incident responder needs to consider threat sources, potential vulnerabilities, and security controls. A threat source is any situation or incident that may lead to exploitation of organizational assets. The main objective of this step is to list out all possible threat sources applicable to critical IT assets. The most common threat sources include human threats, natural threats, and environmental threats.

A human can cause harm either intentionally or unintentionally. If attackers have proper motivation and skills to perform attacks, then they are particularly dangerous threat sources. Assessing the motivation and skills of threat sources is thus also part of threat identification.

The output of this step includes a threat statement listing out all possible threat sources (that is, all sources of potential exploitation of various system vulnerabilities).

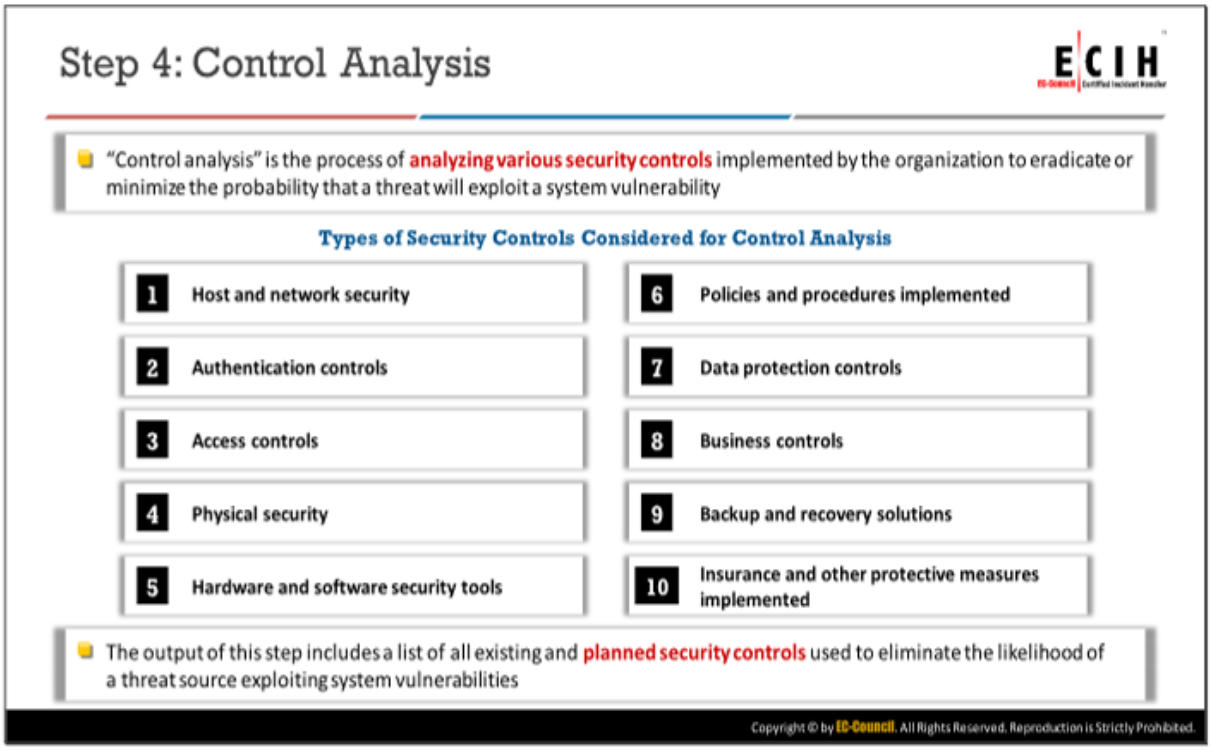
Step 3: Vulnerability Identification

The identification and analysis of threats must also include identification and analysis of vulnerabilities related to critical IT systems. In this step, the incident responder needs to identify and list out all vulnerabilities existing in IT systems that can be maliciously exploited by threat sources.

To identify vulnerabilities, responders can use information gathering techniques and tools, various online vulnerability sources, system security testing, and so on. The latest vulnerability information can also be obtained from search engines, vulnerability news feeds, etc. Further vulnerabilities can be identified by testing the applications and network devices of an organization through processes such as vulnerability scanning and penetration testing.

In this step, incident responders need to prepare a security requirement checklist that includes defined security requirements for IT systems and check whether the security requirements collected during system characterization meet the planned or set security policies and controls.

The main output of this step is a list of all existing vulnerabilities that may be exploited by threat sources.



Step 4: Control Analysis

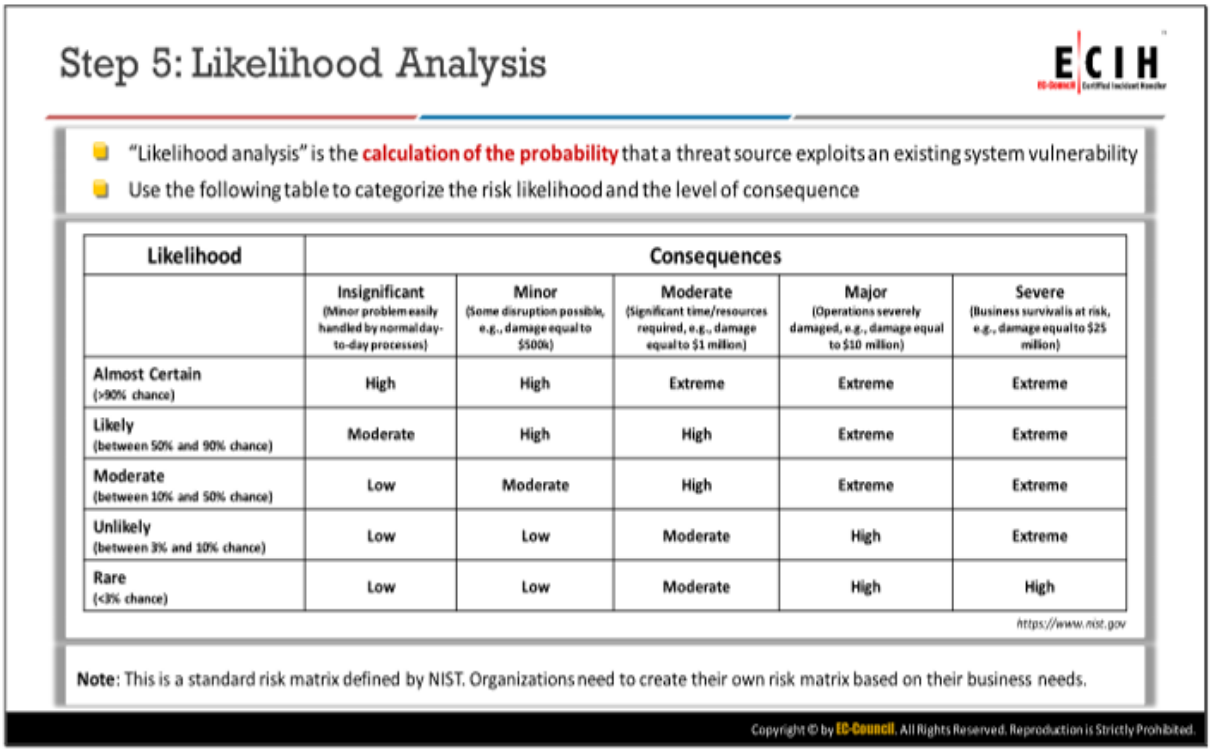
Control analysis is the process of analyzing various security controls implemented by an organization to eradicate or minimize the probability of a threat source's exploiting a system vulnerability within the threat environment. To derive a likelihood rating for such a situation, all existing and planned security controls must be considered.

Security controls comprise both technical controls, such as ACLs, authentication, encryption, firewalls, and IDS, and non-technical controls, such as policies and procedures, security personnel, and physical and environmental security. Listed below are various types of security controls that need to be considered:

- Host and network security
- Authentication controls
- Access controls
- Physical security
- Hardware and software security tools
- Policies and procedures implemented
- Data protection controls
- Business controls
- Backup and recovery solutions
- Insurance and other protective measures implemented

To analyze security controls in an efficient and effective way, a current security requirement checklist should be used. This checklist helps in evaluating security controls against both compliance and non-compliance requirements. Checklists need to be updated continuously to reflect the changes made to the organization's control environment.

The output of this step is a list of all existing and planned security controls used to eliminate the likelihood of a threat source's exploiting system vulnerabilities and minimize the adverse effect of any such exploitation.

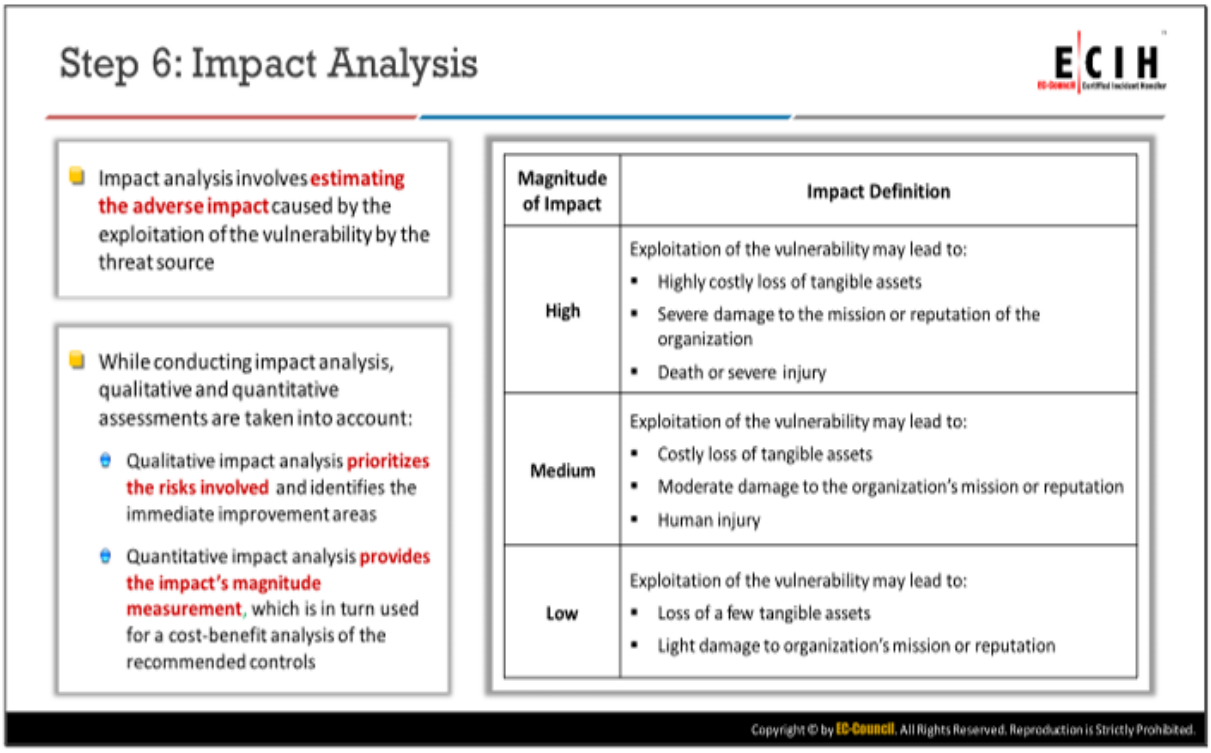


Step 5: Likelihood Analysis

Likelihood analysis is the calculation of the probability that a threat source exploits an existing system vulnerability. It depends on factors such as motivation and capability of threat source, type of vulnerability, and effectiveness of existing security controls. The information gathered in the previous steps, such as identified threats and vulnerabilities and existing and planned security controls, helps incident responders rate the likelihood of security incidents. For example, if the threat source has a strong motive and is highly capable of compromising the target systems, the available vulnerability is easily exploitable, and the security controls implemented are not so effective, then the likelihood of an incident occurring is extreme.

The table shown on the above slide illustrates the risk in terms of likelihood rating and corresponding consequences of security incidents. The output of this step is the likelihood rating of a potential vulnerability being exploited by a threat source.

Note: This is a standard risk matrix defined by NIST; organizations need to create their own risk matrix based on their business needs.



Step 6: Impact Analysis

Impact analysis involves estimating the adverse impact of exploitation of a vulnerability by a threat source. This is an important step in measuring the level of risk. The following information must be collected prior to performing impact analysis:

- System mission (for example, IT system processes)
- Criticality of systems and data (for example, system and data value based on importance to the organization)
- Sensitivity level of system and data

This information can be obtained from organizational reports such as mission impact analysis reports or asset criticality assessment reports.

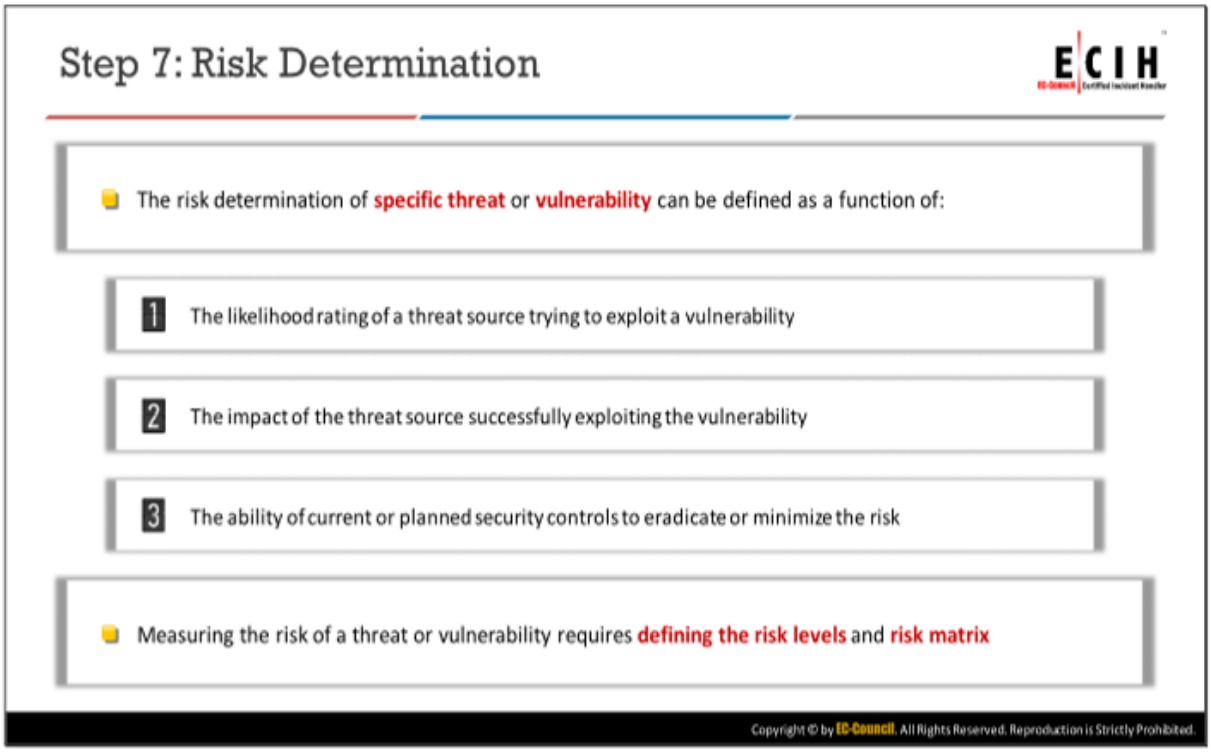
- Based on a qualitative or quantitative assessment of the sensitivity and criticality of the assets, a **mission impact analysis** prioritizes the impact levels associated with the compromise of those assets.
- An **asset criticality assessment** identifies and prioritizes the sensitive and critical information assets that support the critical missions of the organization.

In case these reports do not exist, system and data sensitivity can be evaluated (depending upon the confidentiality, integrity, and availability of the information). Generally, the sensitivity level of the systems and data and the level of impact caused due to exploitation can only be determined by the information and system owners. Therefore, the impact of security incidents can be explained in terms of loss of integrity, loss of confidentiality, and loss of availability.

While conducting impact analysis, both qualitative and quantitative assessments are taken into account. Here, qualitative impact analysis prioritizes the risks involved and thus identifies

immediate improvement areas, whereas quantitative impact analysis provides the impact's magnitude measurement, which in turn is used for cost–benefit analysis of the recommended controls.

The output of this step is the impact magnitude of various security incidents.



Step 7: Risk Determination

Risk determination is a crucial task in a risk assessment effort. It is a complex process that depends upon various tangible and intangible factors. Though it is generally difficult to precisely determine level of risk to different organizational processes and assets, a careful consideration of various risk determinants gives an overall perception of risks faced by an organization.

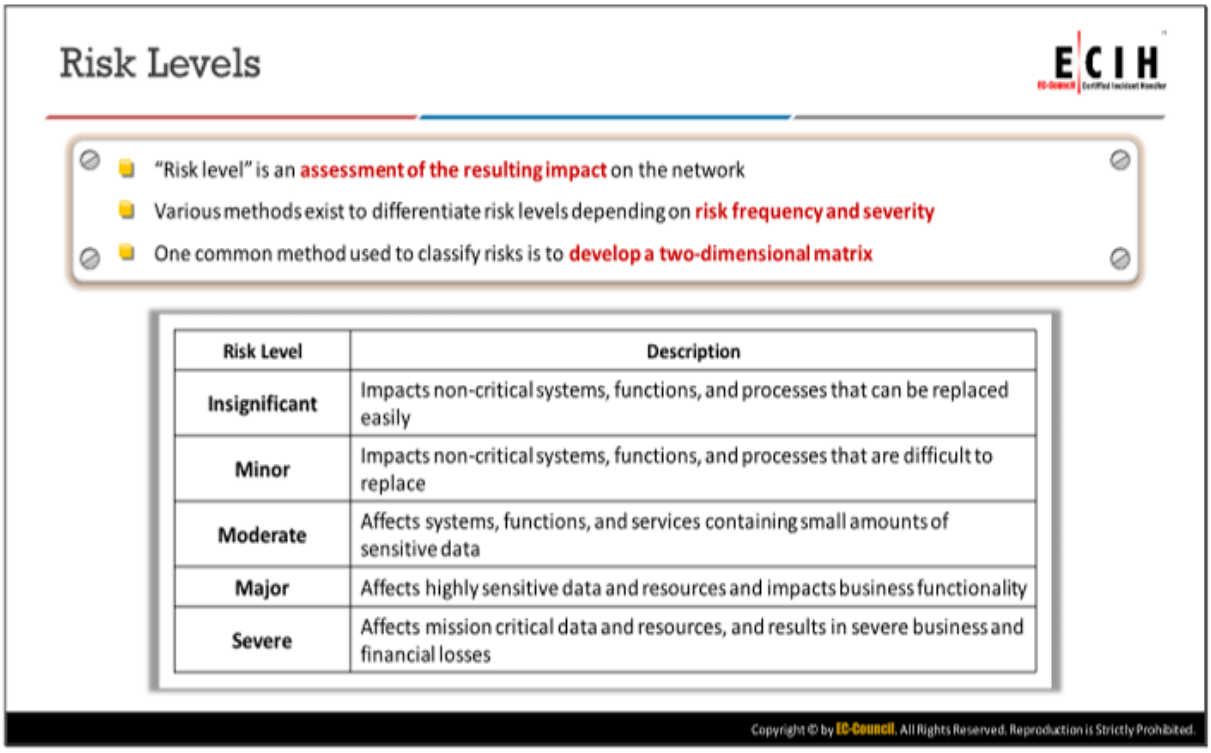
Risk determination involves consideration of the following:

- The probability of occurrence of an anticipated incident. An incident is the result of a threat source exploiting system vulnerabilities.
- The tangible and intangible impacts of an incident on an organization's resources. Tangible impacts of a risk are easier to measure and can be identified and represented by statistical analysis, whereas intangible impacts such as loss of reputation and customer trust are difficult to assess and can be determined only subjectively.
- Control measures to minimize impact or totally avoid the incident. Selection and implementation of control measures are based on risk determination and take into account various management issues such as cost–benefit analysis and availability of resources.

The risk determination of a specific threat or vulnerability can be defined as a function of:

- Likelihood rating of a threat source trying to exploit a vulnerability
- The impact caused after the threat source successfully exploits the vulnerability
- The capability of current or planned security controls to eradicate or minimize the risk

To measure risk, it is important to define the risk levels and risk matrix. The output of this step is the identification of risk levels.



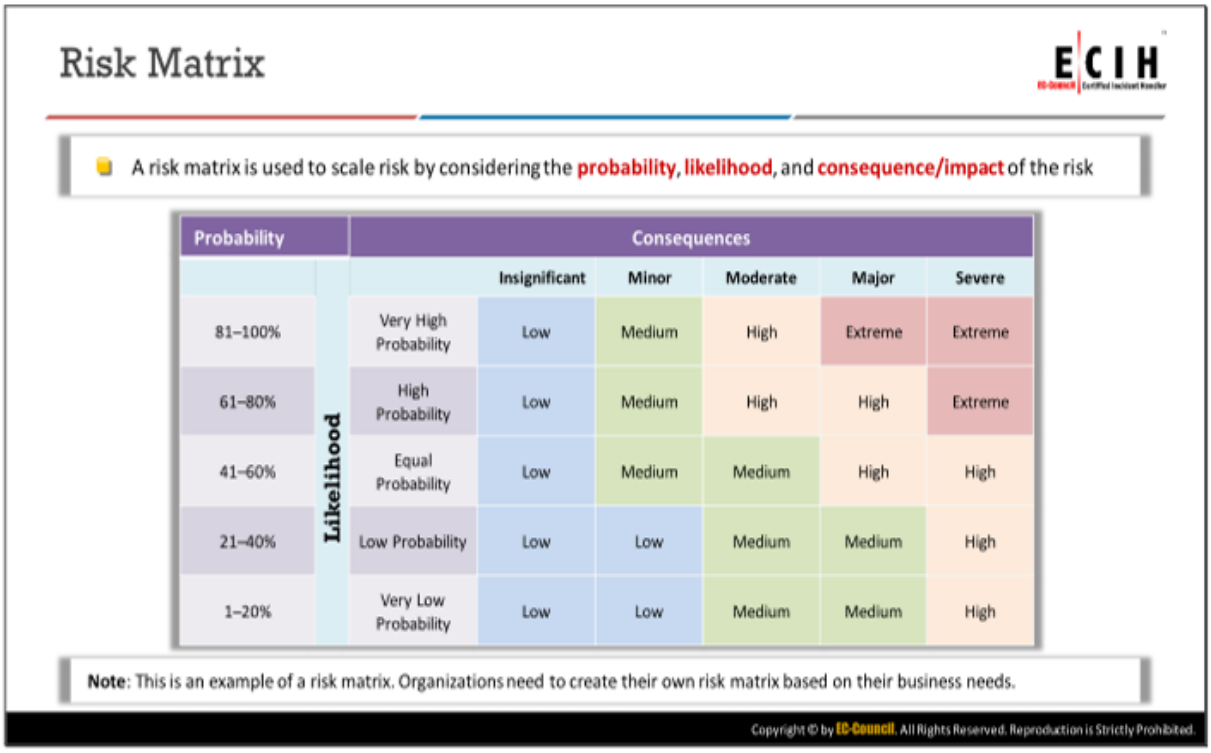
Risk Levels

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

To analyze risk, you need to work out the frequency or probability of an incident happening (likelihood) and the size of the consequences it would have. This is referred to as the level of risk. Incident responders can represent and calculate risk levels using the following formula:

Level of risk = consequence × likelihood

There are five risk levels. Those include insignificant, minor, moderate, major, and severe. Remember that control measures decrease the level of risk but do not always eliminate it.



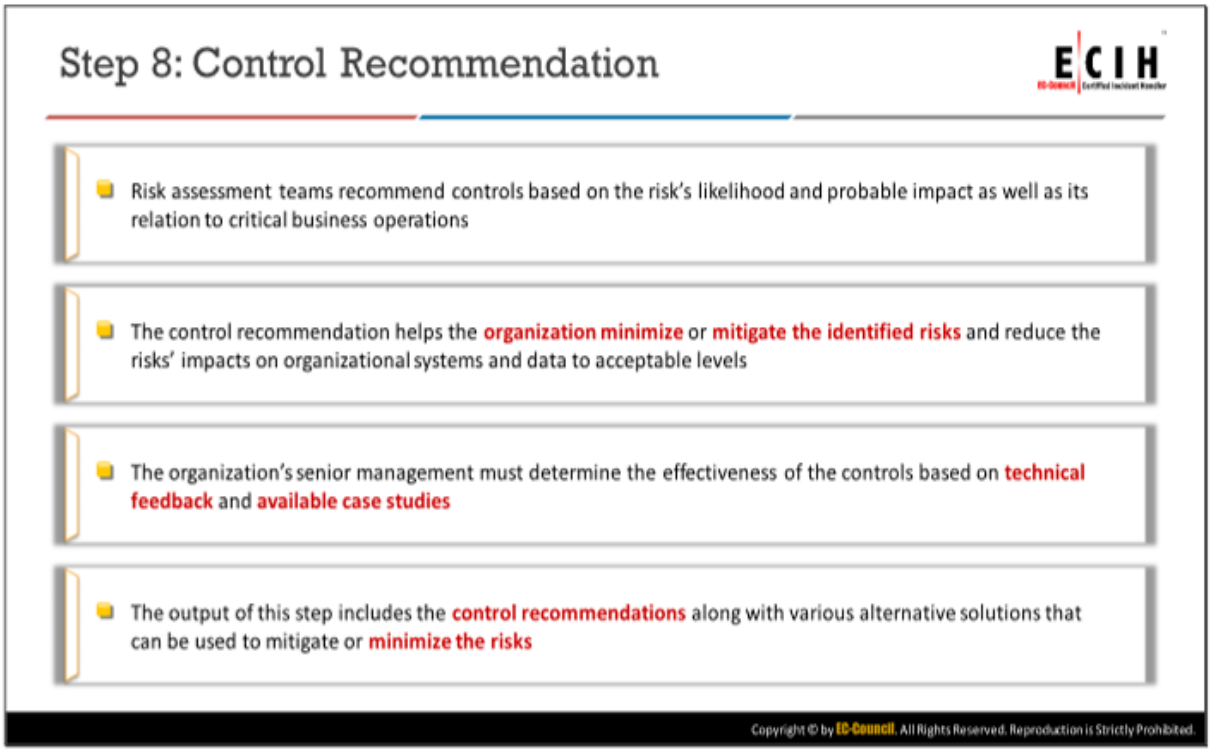
Risk Matrix

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 to represent increased visibility of risk and contributes to management's decision-making capability. It 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.

The table shown on the above slide is a graphical representation of the risk matrix, for visualizing and comparing risk. It differentiates two elements of risk.

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

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



Step 8: Control Recommendation

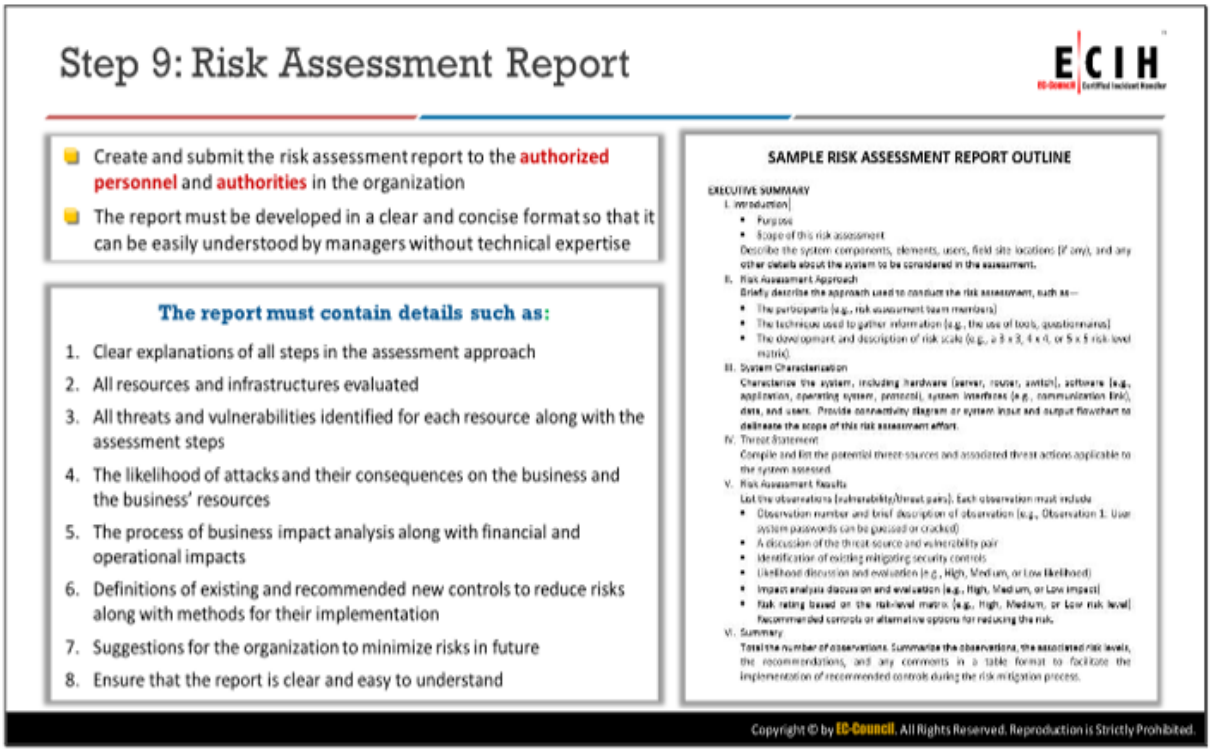
Control recommendation and implementation are the main purpose of the entire risk assessment exercise. Risk assessment teams recommend controls based on the likelihood, impact, and criticality of risk for business operations. The control recommendations help the organization minimize or mitigate the identified risks and reduces the impact caused to organizational systems and data to an acceptable level.

Risk assessment teams need to consider the following factors while recommending the risk control measures:

- Controls should meet the basic principle of the cost–benefit ratio.
- Controls should be implementable within the organization's ethics and security policy as it stands or with minor updates.
- Controls should be compatible with the organization's existing systems and practices.
- Controls must be within legislative and regulatory boundaries.
- Reliability and operational impact of controls should be verified using previous case studies and pre-implementation tests.
- Controls should not go against safety requirements.

Implementation of controls, especially those that meet the above requirements, depends on many business and management issues. Senior management in the organization has to determine the effectiveness of controls based on technical feedback and available case studies.

The output of this step includes control recommendations along with alternative solutions that can be used to mitigate or minimize the risk.



Step 9: Risk Assessment Report

Each step of risk assessment and its results should be properly documented. Documentation is critical for the purpose of risk assessment. An official, detailed, clear risk assessment report helps senior management make decisions on policies, procedures, and system operational and management changes.

Documentation should be well structured and should include supporting information that could be helpful for senior management to decide on and implement mitigation strategies and allocate resources to them.

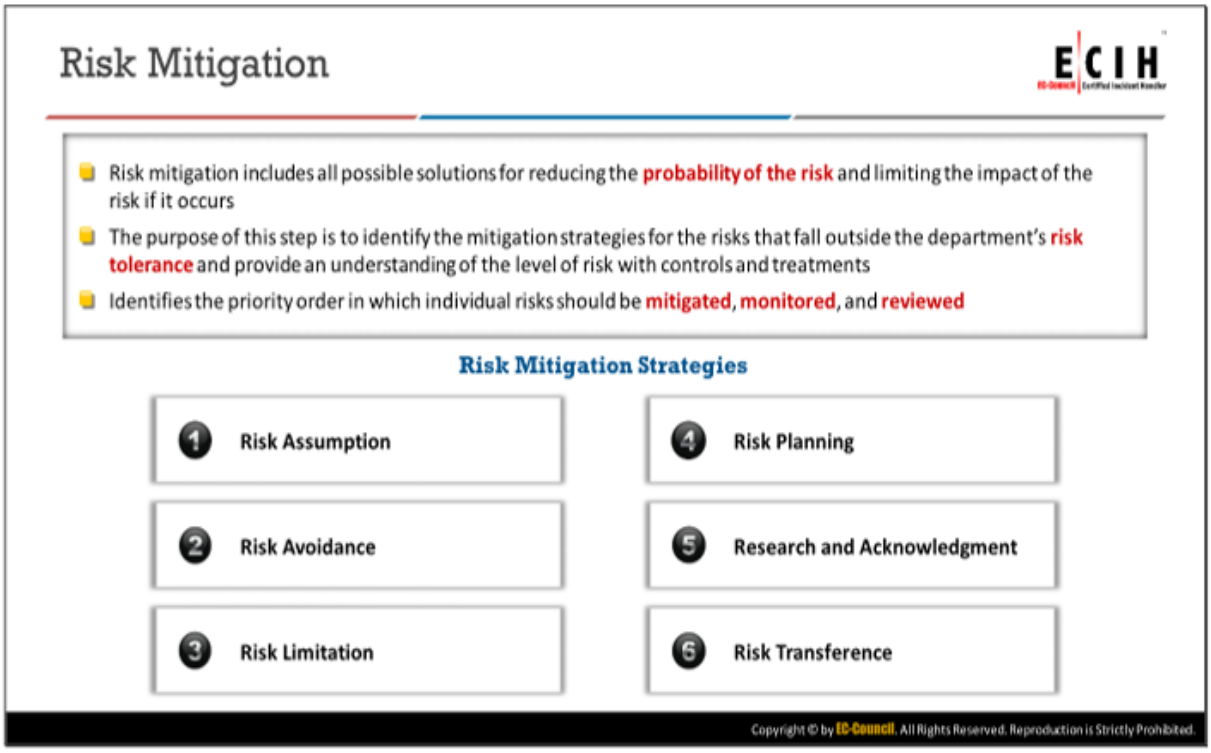
Such documents must cover all the actions performed, results obtained, threat sources identified, vulnerabilities identified, recommendations, and so on. They should use a clear and concise format that can easily understood by nontechnical management.

The report must:

- Clearly explain all the steps performed under the assessment approach
- List all the resources and infrastructure evaluated
- Mention all the threats and vulnerabilities identified for each resource along with the assessment steps
- Include the likelihood of attacks and consequences for the business and other resources
- Clearly state the process of business impact analysis along with financial and operational impact
- Define existing and new controls recommended along with the method of implementation to reduce risks

- Provide suggestions for the organization to minimize risks in future
- Ensure that the report is clear and easy to understand

A sample risk assessment report is shown on the above slide.



Risk Mitigation

Risk mitigation includes all possible solutions for reducing the probability of a risk and limiting its impact if it occurs. The risk mitigation method addresses and mitigates risks according to their severity level. Decisions made in this phase are based on the results of the risk assessment. The purpose of this step is to identify the mitigation strategies for risks that fall outside the department's risk tolerance, provide an understanding of the level of risk, and suggest controls and treatments. It also identifies the priority order in which individual risks should be mitigated, monitored, and reviewed.

Before mitigating the risk, you need to gather information about:

- Appropriate method for mitigation
- People responsible for mitigation
- Costs involved
- Benefits of mitigation
- Likelihood of success
- Ways to measure and assess mitigation

Risk mitigation involves defining, assessing, planning, and implementing for a series of options for mitigating risks in priority order. Organizations should select their risk mitigation strategies from among the following:

- **Risk Assumption**

  This method executes controls so as to reduce the risk factor and bring it to an acceptable level or simply accepts the potential risk and continues operating the IT system as is.

- **Risk Avoidance**

  This refers to preventing risk by curbing the cause of the risk and/or its consequences. Example: *Whenever risks are identified, shut down the system.*

- **Risk Limitation**

  This procedure implements controls to diminish the level of controls which in turn condenses the impact of a threat's exercising vulnerability. Example: *Use of supporting, preventive, and detective controls*.

- **Risk Planning**

  A risk mitigation plan is to be developed in order to prioritize, implement, and maintain the controls.

- **Research and Acknowledgment**

  It is vital to analyze the vulnerability of flaw and to evaluate what actions can be taken to correct the vulnerability in order to reduce the loss caused by the risk.

- **Risk Transference**

  This is transferring the risk and/or getting compensation for losses, such as purchasing insurance and making claims when there are losses.

The steps taken in risk mitigation will differ from case to case as these options reflect, and stakeholders and process owners mutually decide on these steps.

Key points while considering risk mitigation strategies are:

- Implementing an appropriate strategy
- Checking whether adequate resources are available to implement the plan
- Risk mitigation plan should reduce the risk factor to a certain acceptable level
- If there are risks to be handled immediately, remedial actions are taken for those risks

Controlling Risk

Once you have decided how to mitigate identified risks, you need to develop and regularly review your risk management plan. The different options for treating risk are avoiding the risk itself (avoiding the activities that lead to a rise of risk), reducing the risk (reducing the likelihood of the risk occurring and reducing the impact if the risk occurs), and transferring the risk (shifting the risk responsibilities to another party through insurance or partnership).

Identify all the existing security controls that can help organizations in reducing security risks. Recommend any new security controls that the organization must implement. Use results of vulnerability and threat assessment to minimize risks, as risks are directly proportionate to them. Incident responders must first try to eliminate threats and vulnerabilities if they are to control the risks.

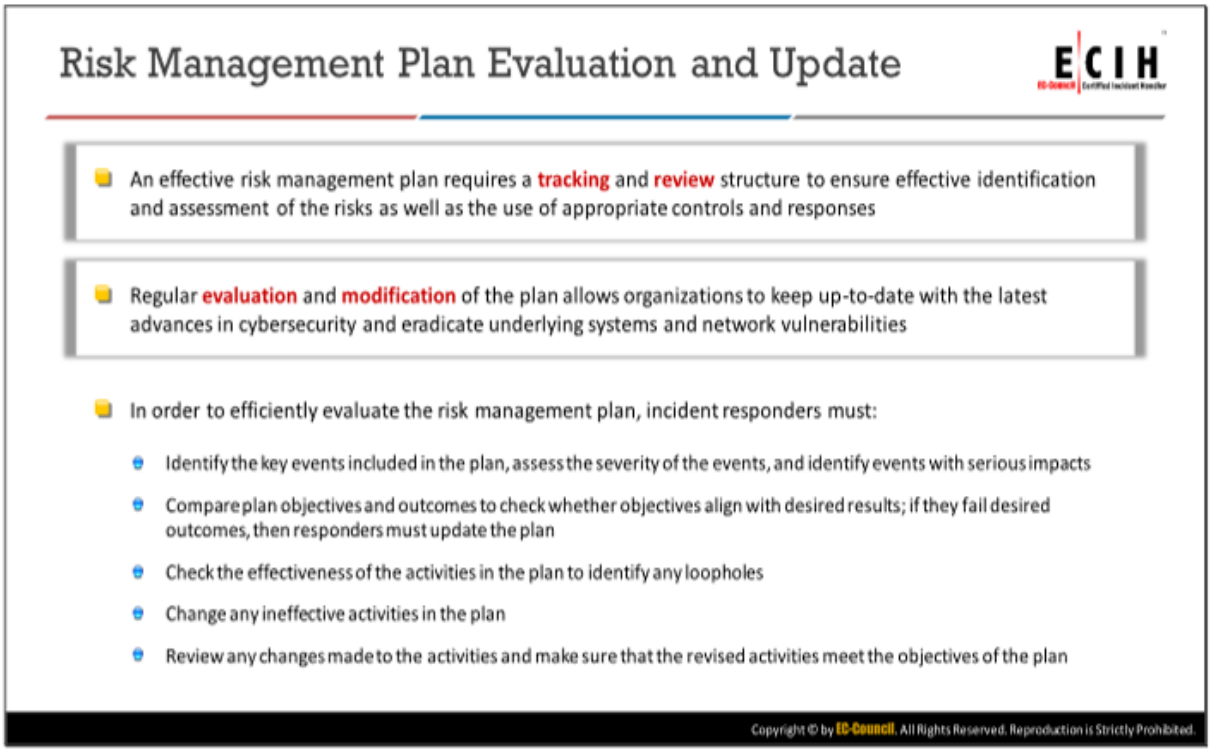
The following are some of the control measures that responders may implement to reduce risks:

- Impart security awareness to employees.
- Implement up-to-date hardware and software security solutions, such as IDS, firewall, honeypot, and DMZ.
- Strengthen network, account, application, device, and physical security across the organization.
- Implement strict access controls and security policies.
- Deploy encryption for all data transfers.
- Implement an appropriate incident handling and response plan.

- Implement safe password practices by changing passwords regularly and making sure that they include a combination of numbers, characters, and special characters.
- Raise employee awareness about phishing emails and messages that request personal or financial information.
- Raise employee awareness of not entering their password in a link from an unknown or malicious-looking email and never sending their password via email.
- Develop policies and raise awareness among employees, management, and vendors of the need to be cautious while opening attachments or downloading files from unfamiliar or unknown sources.
- Make sure that operating systems are up-to-date and all vulnerabilities are patched.
- Ensure installation of updated antivirus software and antispyware on every computer in the organization.
- Install a firewall on every employee's working system and on the whole organization's network.
- Secure Wi-Fi networks with passwords.
- Monitor the performance of systems and look after those systems that are taking a long time to reboot.
- Create a separate user account for each employee and only grant administrative privileges to trusted staff.
- Restrict employees from installing software without permission.
- Make it mandatory for all employees to change their account, system, and other passwords at regular intervals.

If the risk cannot be avoided or transferred, then it must be accepted, and incident responders must perform the following actions to minimize or eliminate the risk:

- Develop a risk control plan.
- Determine the impact of risk control on service delivery.
- Constraints required for risk control are identified and considered when completing the risk control plan.
- Implementation of risk control strategies.
- Uncontrollable risks.
- Client resistance to risk control.
- Communicate with support workers/other workers during risk control.
- Completely document the risk control plan as a part of the risk control process.



Risk Management Plan Evaluation and Update

A risk management plan is a process designed to identify, eliminate, or mitigate risks to the organizational network and systems. It contains predictions about various cyber risks, their impacts, and how to respond. Organizations must update their risk management plan on a regular basis, as risks can change due to changes in business strategies, policies, and operations. Therefore, reviewing a risk management plan regularly is necessary in order to identify new risks and to monitor the efficiency of risk treatment strategies employed by the organization.

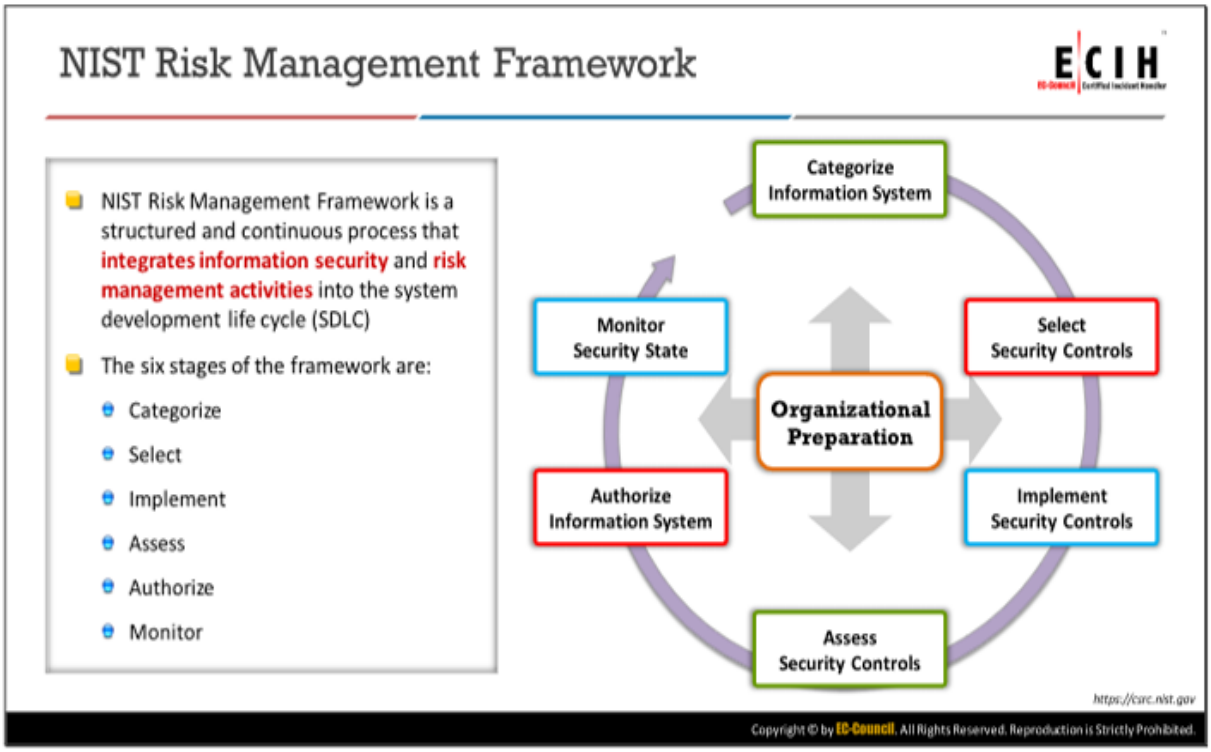
An effective risk management plan requires a tracking and review structure to ensure effective identification and assessment of risks as well as the use of appropriate controls and responses. Further, the monitoring process assures that there are appropriate controls in place for the organization's activities and that procedures are understood and followed.

Attackers can make use of various hacking techniques and tools to identify new loopholes in the organization's infrastructure and exploit vulnerabilities, thereby putting organizational networks at risk. The regular evaluation and modification of the plan allows organizations to identify and implement the latest updates in cybersecurity and eradicate underlying vulnerabilities in systems and networks more effectively.

In order to evaluate the risk management plan efficiently, incident responders must consider the following points:

- Identify the key events included in the plan, assess the severity of the events, and identify any events that are causing serious impact.
- Compare the objectives and outcomes of the plan to check whether the latter match the former. If not, then the responders must update the plan.

- Check the effectiveness of plan activities to identify weaknesses in the plan.
- Make changes to ineffective aspects of the plan.
- Review the changes being made to activities and make sure that they meet the objectives of the plan.



NIST Risk Management Framework

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

The NIST risk management framework is a structured, continuous process that integrates information security and risk management activities into the system development life cycle (SDLC). It follows a security life cycle which involves six stages.

Discussed below are the six stages of the framework:

- **Categorize Information System**

  This initial stage of the NIST framework involves defining the criticality or sensitivity of the information system according to the potential worst-case scenario. This reveals the adverse impact on the mission or the business.

- **Select Security Controls**

  Categorize the information system, and then select the baseline security controls under a NIST risk management framework. Apply tailored guidance and supplemental controls (if needed) based on risk assessment.

- **Implement Security Controls**

  Implement security controls within the enterprise architecture using sound system-engineering practices. Apply security configuration settings.

- **Assess Security Controls**

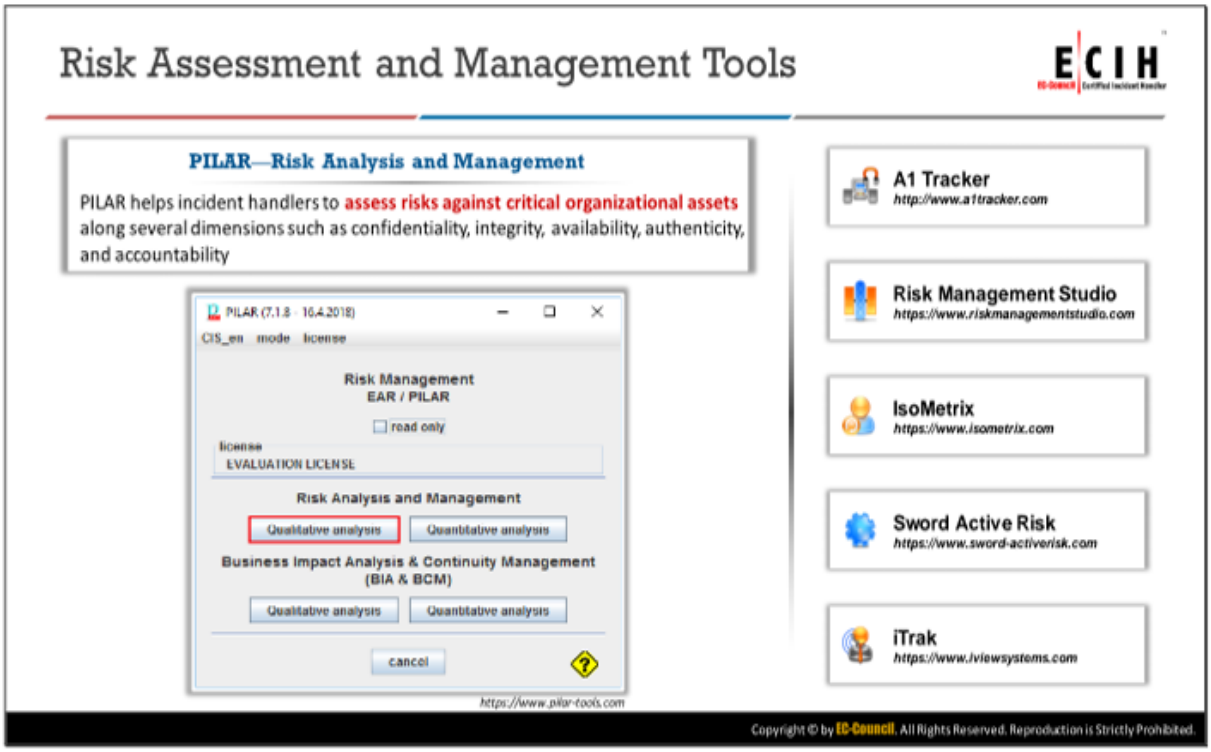
  Determine security control effectiveness by ensuring correct and effective implementation of the controls as per required operation and compliance with security requirements for the information system.

- **Authorize Information System**

  Determine risk to organizational operations and assets, individuals, other organizations, and the nation; if acceptable, authorize the operation.

- **Monitor Security State**

  Continuously track changes to the information system that may affect security controls, and reassess control effectiveness.



Risk Assessment and Management Tools

Risk assessment and management tools help incident handlers assess and prioritize risks to organizational assets by importance, based on the impact and likelihood of the risk. Discussed below are some of the key risk assessment and management tools:

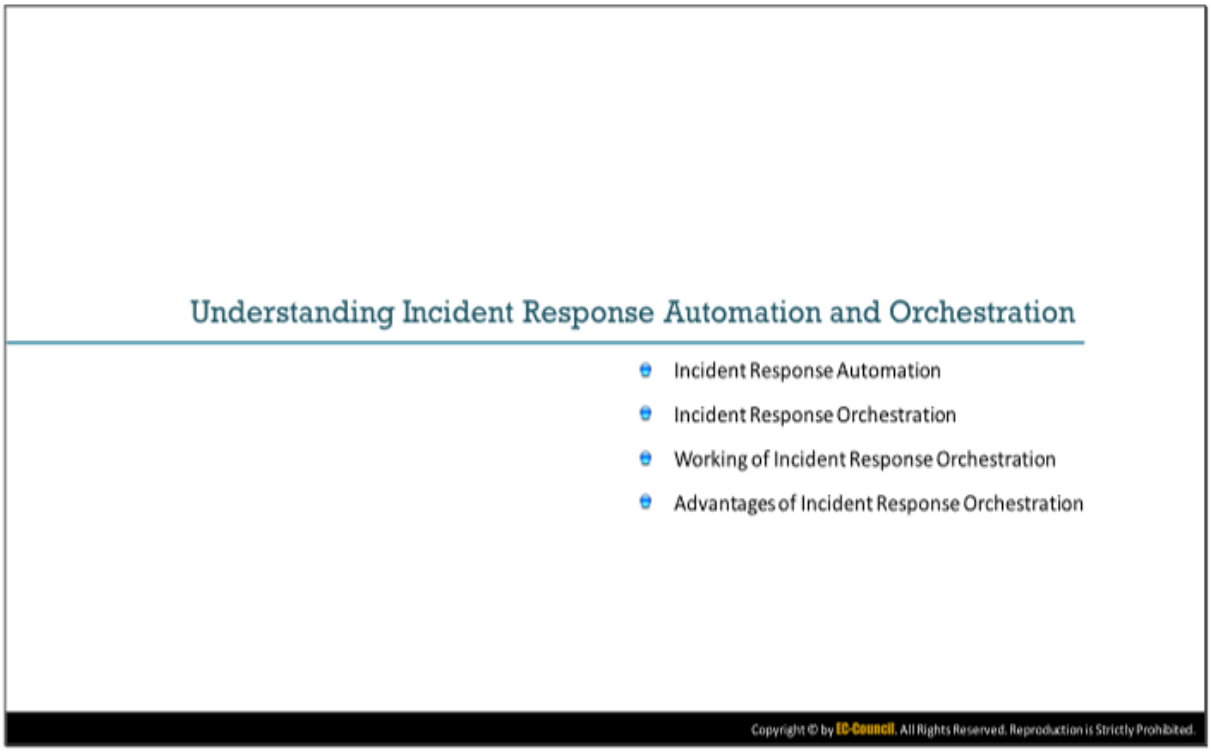
- **PILAR - Risk Analysis and Management Tool**

  Source: *https://www.pilar-tools.com*

  The PILAR tool helps incident handlers assess risks against critical assets of the organization in several dimensions, such as confidentiality, integrity, availability, authenticity, and accountability. It includes both qualitative and quantitative risk analysis. To eradicate the identified risks, you can implement various countermeasures and security policies. Using PILAR, you can generate risk assessment reports in RTF or HTML format.

Some additional risk assessment and management tools are listed below:

- A1 Tracker (*http://www.a1tracker.com*)
- Risk Management Studio (*https://www.riskmanagementstudio.com*)
- IsoMetrix (*https://www.isometrix.com*)
- Sword Active Risk (*https://www.sword-activerisk.com*)
- iTrak (*https://www.iviewsystems.com*)
- Certainty Software (*https://www.certaintysoftware.com*)
- Resolver's ERM software (*https://www.resolver.com*)
- Isolocity (*https://www.isolocity.com*)
- Enablon (*https://enablon.com*)

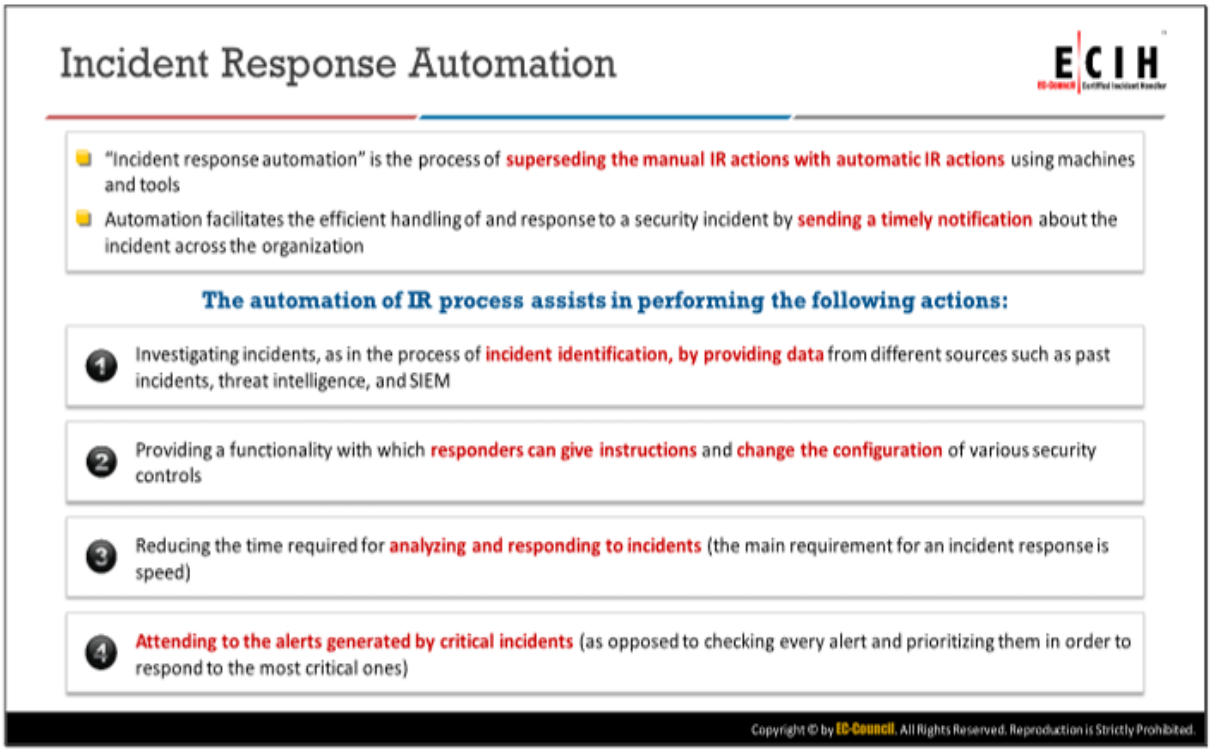


Understanding Incident Response Automation and Orchestration

Due to the increasing frequency of security incidents, organizations must rapidly identify and respond to them in a timely manner in order to handle them before they create any damage to the organizational assets. With security as a priority, organizations must adopt new ways to overcome this issue, while at the same time adding value to their existing security infrastructure and technologies, so as to enhance their incident response process and overall security operations.

Incident response automation and orchestration is a solution to this problem, as it helps organizations to quickly, correctly, and effectively identify critical security incidents, further notify responders, and communicate across different business units to address an issue quickly. Using this solution, an organization can simplify the process by reducing repetitive tasks and the number of individuals needed to complete tasks.

This section discusses incident response automation and incident response orchestration, including its workings and advantages.



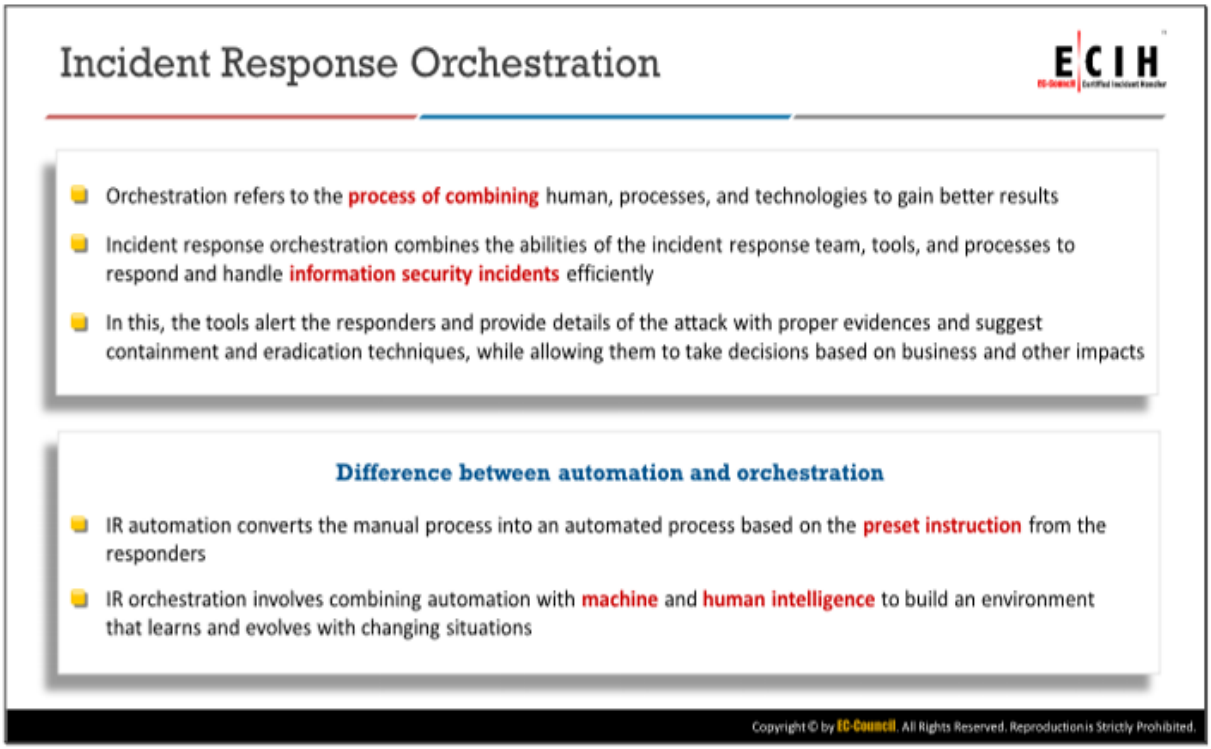
Incident Response Automation

Incident response automation is the process of superseding manual IR actions with automatic IR actions using machines and tools. In it, security teams define certain standardized response steps to the tools and conditions to perform them, based on alerts and warnings from different systems. When automated tools encounter these conditions, they perform the preset incident response functions.

Automation aids efficient handling and response to security incidents by sending timely notification about the incident across the organization or to relevant people. It also assists responders in quickly assessing the situation and performing containment and mitigation activities. IR automation has no set form or process; there are many ways to go on with it depending on the nature of the incident and the technical sophistication of implementation.

The automation of the IR process assists in performing the following actions:

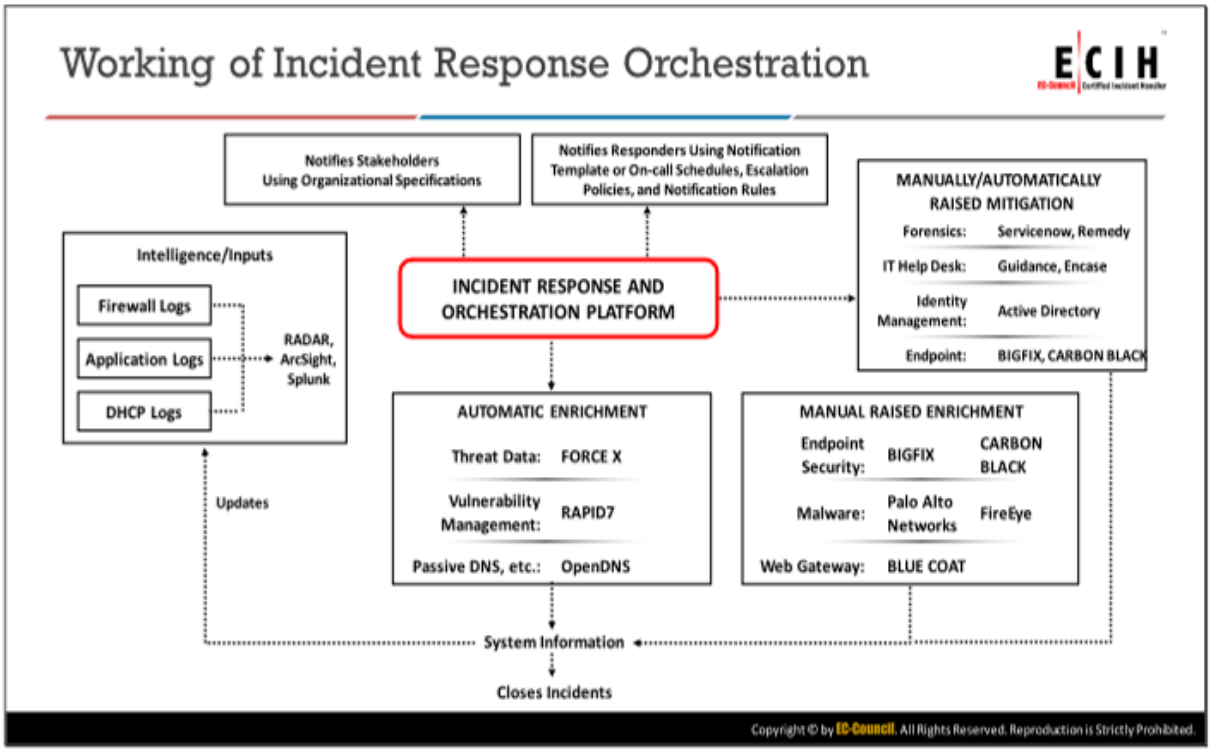
- It helps in investigating the incidents, for example in identifying them by providing and analyzing data from different sources, such as past incident information, threat intelligence, and SIEM.
- It provides functionality where responders can give instructions and change the configuration of various security controls.
- The main requirement for incident response is speed, and automation helps to achieve it, reducing the time taken to analyze incidents and respond to them efficiently.
- It enables responders to pay more attention to alerts generated by critical incidents rather than checking every alert.



Incident Response Orchestration

Orchestration is the process of combining human responses, processes, and technologies to gain better results. Incident response orchestration is an approach to security incidents that occur in an organization. The main aim of IR orchestration is to ensure that the response team knows exactly what process to follow in case of security incidents and has the required tools and strategy to act efficiently, correctly, and on time. Thus, incident response orchestration combines the abilities of the incident response team, tools, and processes to respond and handle information security incidents efficiently. The tools alert the responders, provide details of the attack with proper evidence, and suggest containment and eradication techniques, while allowing responders to take decisions based on business and other impacts. IR orchestration is organization specific, as it must map to the organization's unique IT systems, security controls, asset priorities, and threat landscape.

IR orchestration is different from IR automation in that the latter converts the manual process into an automated process based on preset instruction from responders, whereas the former involves combining automation with machine and human intelligence to build an environment that learns and evolves with changing situations. The integration of IR automation and orchestration can help responders address security incidents, drastically cutting down response time from days to mere minutes.

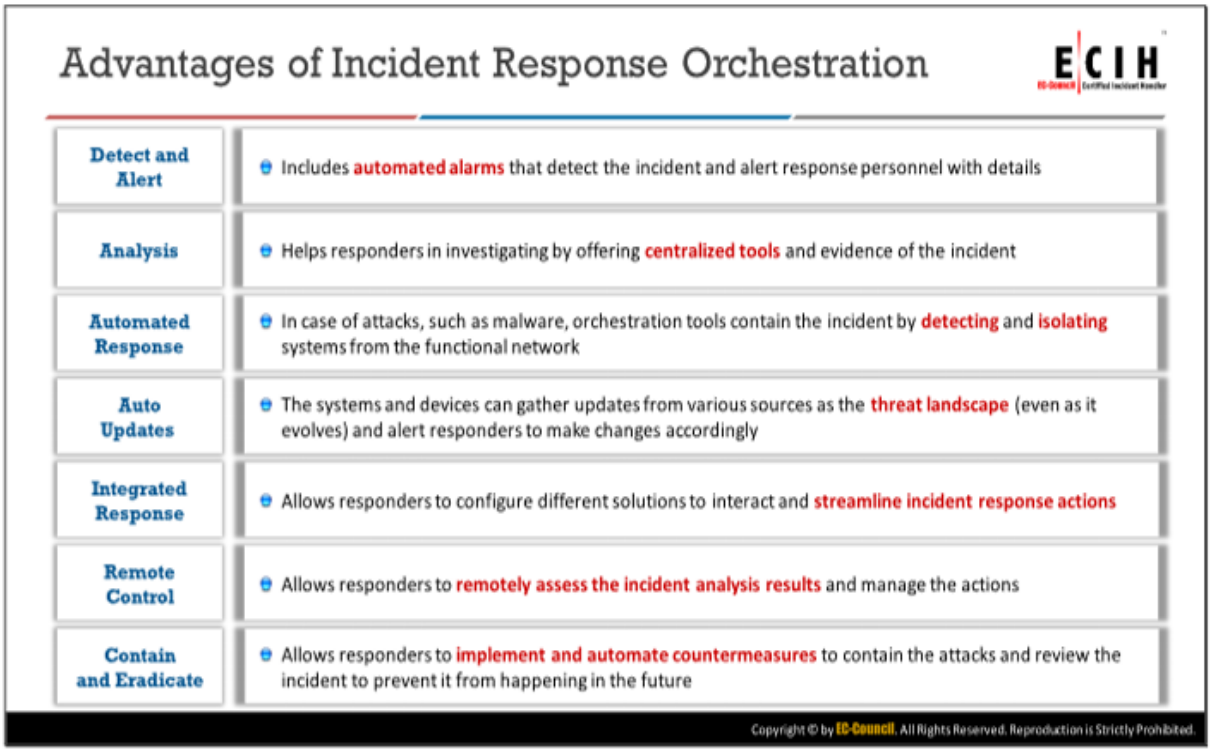


Working of Incident Response Orchestration

The diagram shown on the above slide illustrates the functioning of incident response orchestration as it is usually employed in organizations. As depicted in the diagram, orchestration plays a vital role in the security operations center (SOC), from escalation to security incident enrichment to mitigation strategies.

Incidents escalated from security alerts are stored automatically in the incident response platform (IRP) and are automatically gathered by the automatic enrichment platform, which performs analysis using built-in threat intelligence data and additional sources on the gathered incidents and delivers valuable incident information.

At this stage, security responders have critical information about incidents and can initiate mitigation strategies by notifying the IT help desk or by denying users access through identity management. The responders can further use additional features to manually take on certain actions regarded as critical and can gather additional information about the incident manually from other security tools.



Advantages of Incident Response Orchestration

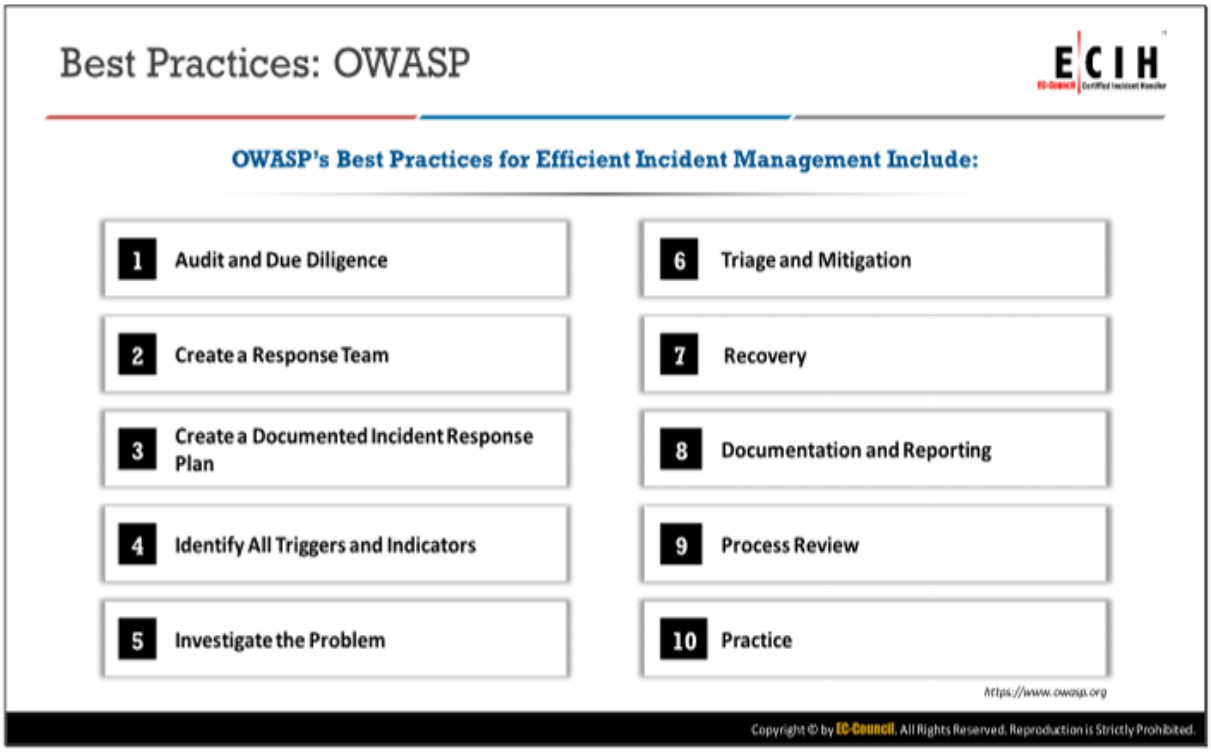
Discussed below are some of the important advantages of incident response orchestration:

- **Detect and Alert:** It automates alarms that detect the incident, alert the response personnel, with details, and suggest the required containment steps based on the nature of the attack and impacted resources.
- **Analysis:** It helps responders in their investigation by offering centralized tools and evidence of the incident. These tools also help in sorting and prioritizing the incidents.
- **Automated Response:** In case of attacks such as malware attacks, the orchestration tools will be able to contain the incident by detecting and isolating individual systems from the functional network. Responders can customize such automated responses based on their requirements.
- **Auto Updates:** Systems and devices can gather updates from various sources as the threat landscape evolves and alert the responders to make changes accordingly.
- **Integrated Response:** IR orchestration allows responders to configure different solutions to interact with and streamline incident response actions.
- **Remote Control:** It allows responders to remotely assess the incident analysis results and manage response actions.
- **Case Creation:** The process includes tools that create cases with a single click, integrating details of detection, containment, and eradication methods.
- **Contain and Eradicate:** IR orchestration allows responders to implement and automate countermeasures to contain attacks and review incidents to eradicate them from happening in the future.

Incident Handling and Response Best Practices

With the growing threat landscape, it has become essential for organizations to manage incidents rapidly and much more efficiently. Incident handlers should have sufficient knowledge about best practices for security incident management. Such practices should be carried out before as well as after the incident has occurred, so as to be sure that the problem is eradicated and services are completely recovered.

This section gives an overview of best practices provided by OWASP, ENISA, GPG18, and forensic readiness planning (SPF).



Best Practices: OWASP

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

Following are the best practices provided by OWASP to manage incidents efficiently:

1. **Audit and Due Diligence**

   Performing an audit will help to know how well prepared the organization is for incident response in terms of:

   - People
   - Process
   - Equipment and materials

2. **Create a Response Team**

   Preventing and managing attacks or incidents that can occur without prior notice is best done by experts who belong to an incident response team.

   Some important things to note when creating an incident response team:

   - Ensure that a competent team leader is in charge and that there is a clear chain of command.
   - Document the roles and responsibilities of the team members and communicate them clearly to all relevant stakeholders.

3. **Create a Documented Incident Response Plan**

   An organization should have a well-documented incident response plan to guide the incident response team during an incident. A comprehensive plan at minimum should

cover roles and responsibilities, investigation, triage and mitigation, recovery, and documentation process.

4. **Identify All Triggers and Indicators**

   It is important to clearly define what can trigger an incident in the organization. Some of these events include:

   - Loss or theft of equipment
   - Loss or theft of information
   - Attempts to gain unauthorized access to data, computers, or information storage devices

5. **Investigate the Problem**

   A thorough investigation will require input from the incident response team and might also require input from external resources. The investigation will document the incident details, including what to look for, who to involve, and how to document what is found.

6. **Triage and Mitigation**

   Investigation leads to the triage and resolution process. As the team identifies potential exposure, they should plan and execute effective mitigation accordingly.

   In summary, the triage process should cater to the following activities:

   - Classification of the incident
   - Incident prioritization
   - Assigning specific tasks to specific people

7. **Recovery**

   Recovery is a significant step for restoring whatever services or materials might have been affected during an incident: the transition from active incident to standard monitoring. The recovery procedure should include steps for transition given the specifics of the firm's environment and approach.

8. **Documentation and Reporting**

   Reporting and documentation are critical actions that must continuously occur, before, during, and after incident response. A comprehensive incident report is required, in keeping with best practices and with the incident response plan. The type of report that might be required might vary, but it should help manage and review incidents satisfactorily.

9. **Process Review**

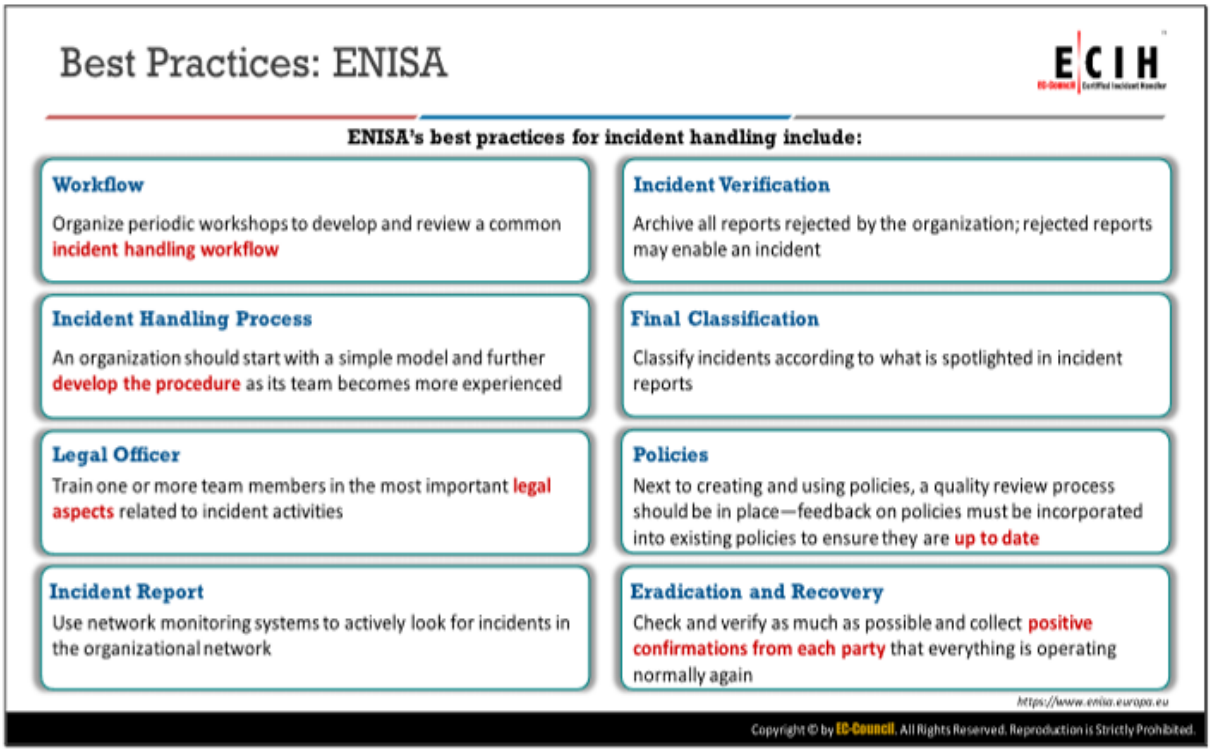
   It is imperative to continuously monitor an incident and the workload/performance of the team or incident handler.

   Process review can help the organization answer the following:

- Should the organization increase or decrease the number of incident handlers?
- Should the organization develop automated procedures for incident handling?
- What risks did the organization identify during the incident that need to be followed up for action and/or monitored closely?

10. Practice

Organizations should not wait for incidents to occur; rather, incident handling teams should always be prepared. It is important that the incident response team understands how important mock drills and practice are to the firm. Sometimes the team can practice the organization's plan by simulating a live scenario. This test can be as simple as dropping a thumb drive on the floor of the office and seeing what happens or as sophisticated as simulating a data breach or phishing attack.



Best Practices: ENISA

Source: *https://www.enisa.europa.eu*

The European Network and Information Security Agency (ENISA) provides, among many other activities related to IT security in the European Union, reference materials, good practice guides, and exercise material for cyber emergency response teams (CERTs). ENISA also regularly supports CERT training activities in Europe, such as TRANSITS.

Following are some of the good practices provided by ENISA for incident handling:

- **Workflow**

  It is good practice to organize periodic (for example, twice a year) workshops to develop and review common incident handling workflow.

- **Incident Handling Process**

  Organizations should start with a simple model and then, as the team becomes more experienced, develop the procedure further.

- **Legal Officer**

  It is good practice to train one or a few team members in the most important legal issues or procedures related to incident activities.

- **Incident Report**

  - Use network monitoring systems (for example, intrusion detection systems or any other threat monitoring systems) to actively look for incidents in organizational networks.

- Subscribe to services that provide information about compromised machines.
- Monitor blacklists for records from the location where the organization operates

- **Incident Verification**

  The CERT should answer with some explanation of what scanning or probing is, why incident handlers do not handle it, and what to do to avoid successful attacks on the network of the incident reporter. This can also be a good method for building incident awareness within the geographic location of an organization.

  Incident handlers should archive reports that are rejected by an organization, as any of the rejected reports could lead to an incident or provide useful information for other incidents.

  An incident report should be rejected when:

  - The incident has nothing to do with the constituency of the organization
  - An incident reporter expects services from the incident handler that can't be delivered
  - The occurrence is not an incident, or not one by the organizational definition at least

  It should be ignored when:

  - It has been reported anonymously or by an untrusted or unreliable party

- **Final Classification**
  - Classify incidents according to what is reported by incident reporters
  - Classify incidents according to what is recognized by incident handlers at the very beginning of the incident handling process

- **Policies**

  Alongside creating and using policies, a quality review process should be in place for them, with feedback incorporated into existing policies and policy revisions conducted accordingly.

- **Entry and Exit Procedures**

  As CERT personnel are hard to get, organizations should make sure that new people are brought up to speed quickly and have enough challenge and variety in their jobs to ensure that organizations can retain them. Organizations should also ensure that when CERT personnel leave, proper actions are taken.

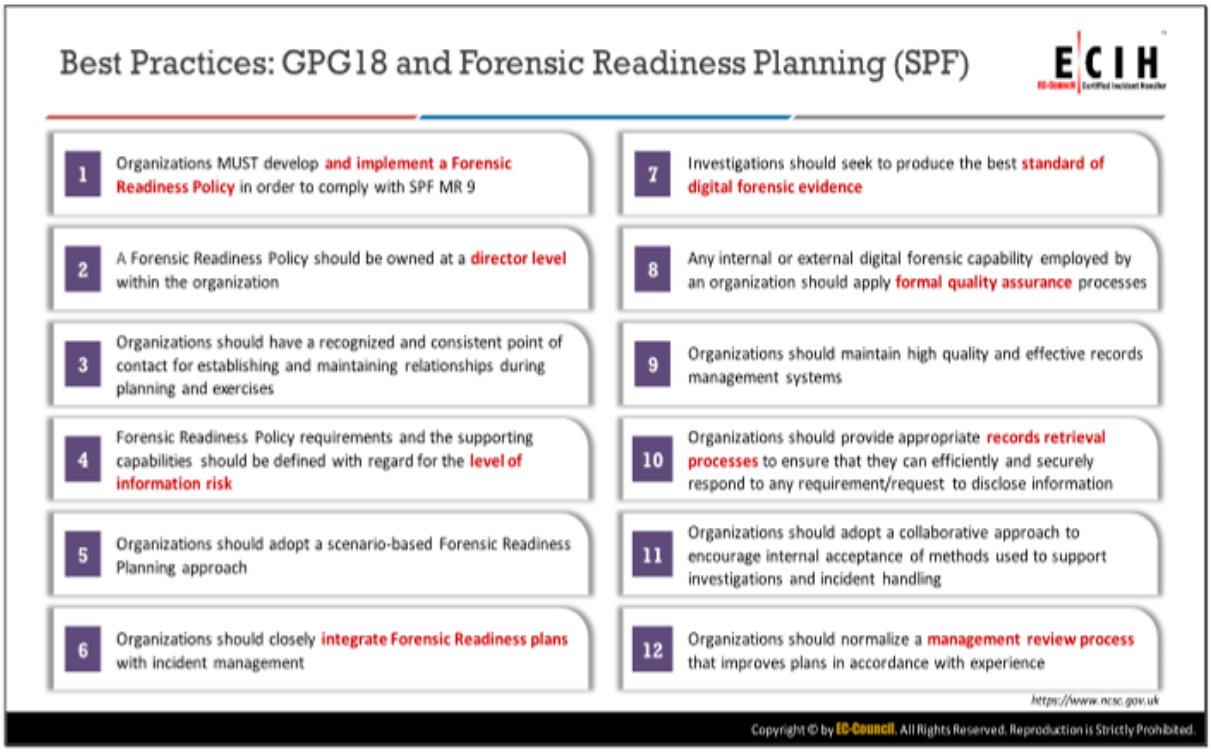
  Exit procedures should always be followed without question. They should aim at the following:

  - Removing the exiting employee's access to systems with confidential information (changing passwords, revoking certificates and keys, blocking accounts, and so on)
  - Logging the actions of the employee

- Backing up all his/her work
- Revoking his/her roles in incident management
- Conducting a handover interview for the incoming person
- Performing an exit interview with the exiting person to learn for the future
- Announcing the staffing change to constituents, the parent organization, and other teams

- **Eradication and Recovery**

  If there are doubts whether a problem is eradicated and service is recovered, it is good practice to check and verify to the degree possible and/or get positive confirmation from each party that in their opinion everything is operating normally again.



Best Practices: GPG18 and Forensic Readiness Planning (SPF)

Source: *https://www.ncsc.gov.uk*

The aim of the *Good Practice Guide* (GPG) is to provide advice on good practice that can help to define and implement an approach to the development of forensic readiness policy and associated planning and practice activities. The guidance provided is generic but includes information on how it can be applied to suit the requirements of individual organizations.

There are 12 significant principles that organizations should observe as part of adoption of forensic readiness policy, which are as follows:

- **Principle 1**

  Organizations must develop and implement a forensic readiness policy in order to comply with SPF MR 9. It is also strongly recommended that all other organizations within the wider public sector either develop or adopt and implement such a policy.

- **Principle 2**

  Forensic readiness policy should be owned at a director level within an organization.

- **Principle 3**

  Organizations should have a recognized, consistent point of contact to establish and maintain relationships during planning and exercises and to act as a focal point during crisis investigations and management. The point of contact should work closely with organizations' legal departments and other relevant stakeholders during each stage of each investigation.

- **Principle 4**

  Forensic readiness policy requirements and supporting capability should be defined with regard to the level of information risk or actual business need to undertake digital forensic investigations.

- **Principle 5**

  Organizations should adopt a scenario-based forensic readiness planning approach that learns from experience gained within the business.

- **Principle 6**

  Organizations should closely integrate forensic readiness plans with incident management and other related business planning activities.

- **Principle 7**

  Investigations should seek to produce the best standard of digital forensic evidence. Practitioners should adopt the principles published by the Association of Chief Police Officers (ACPO).

- **Principle 8**

  Any internal or external digital forensic capability employed by an organization should apply formal quality assurance processes, and all staff involved in handling evidence during investigations should have an appropriate degree of competence.

- **Principle 9**

  Organizations should maintain the quality and effectiveness of their records management systems in order that specific business records can be produced as evidence in court or to address any legal or regulatory requirement.

- **Principle 10**

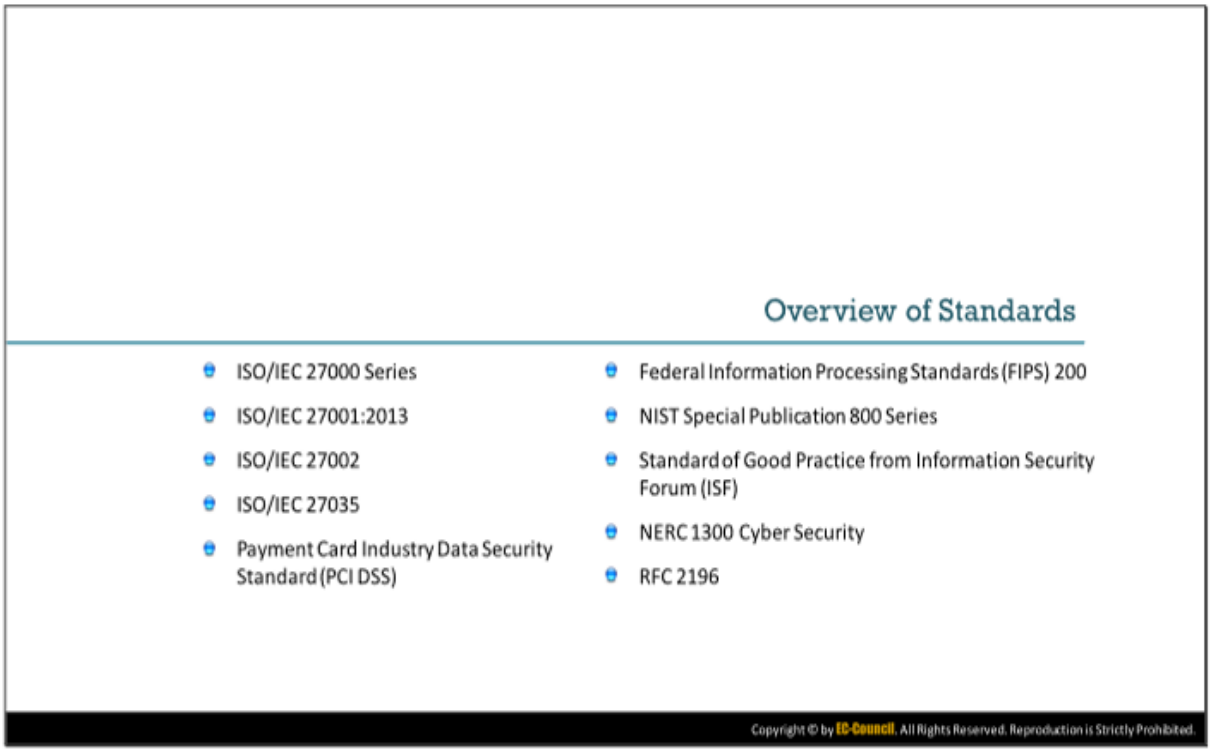
  Organizations should provide appropriate records retrieval processes and mechanisms in order that any requirement to disclose information can be efficiently and securely dealt with. Such disclosures must be handled in accordance with all relevant legislation and regulations.

- **Principle 11**

  An open and collaborative approach should be adopted within organizations, wherever possible, to help gain acceptance of methods used to support investigations and incident handling. All methods of investigation and detection of information security incidents must be lawful.

- **Principle 12**

  Organizations should have a management review process that improves plans in accordance with experience and new knowledge.



Overview of Standards

Information is the critical asset that organizations need to secure. To understand how to do so, it is essential to be aware of relevant standards.

This section discusses various standards pertaining to information security, such as ISO/IEC 27000 Series, NIST Special Publication 800 Series, Standard of Good Practice from Information Security Forum (ISF), NERC 1300, and RFC 2196.

ISO/IEC 27000 Series

- The ISO/IEC 27000 is the **information security standard** developed and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- The ISO/IEC 27000 provides a **global framework** for effective information security management for all types of organizations
- The ISO/IEC 27000:2018 is the latest revision of the standard; it addresses information technology, security techniques, information security management systems, overview, and vocabulary
- The ISO/IEC 27000 family contains many standards that define **information security management systems**

Standard	Description
ISO/IEC 27000	Overview and introduction of the information security management systems
ISO/IEC 27001	The information security management system (ISMS) requirements
ISO/IEC 27002	Code of practice for information security controls
ISO/IEC 27003	Information security management system implementation guidance
ISO/IEC 27004	Information security management
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for information security management systems auditing
ISO/IEC TR 27008	Guidance for auditors on ISMS controls
ISO/IEC 27009	Guidelines for those producing sector- or industry-specific ISO27k standards
ISO/IEC 27010	Information security management for inter-sector and inter-organizational communications

https://www.iso.org

ISO/IEC 27000 Series (Cont'd)

Standard	Description
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27013	Guidance on the joint implementation of both ISO/IEC 27001 (ISMS) and ISO/IEC 20000-1
ISO/IEC 27014	Offers guidance on the governance of information security
ISO/IEC TR 27015	Provides information security management guidelines for financial services
ISO/IEC TR 27016	Covers the economics of information security
ISO/IEC 27017	Covers information security controls for cloud services
ISO/IEC 27018	Code of practice for protection of personally identifiable information (PII) in public clouds
ISO/IEC TR 27019	Information security for process control in the energy industry
ISO/IEC 27031	Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032	Guideline for cybersecurity
ISO/IEC 27033	Network security

Standard	Description
ISO/IEC 27034	Application security
ISO/IEC 27035	Information security incident management
ISO/IEC 27036	Information security for supplier relationships
ISO/IEC 27037	Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038	Document redaction
ISO/IEC 27039	Intrusion prevention
ISO/IEC 27040	Storage security
ISO/IEC 27041	Investigation assurance
ISO/IEC 27042	Analyzing digital evidence
ISO/IEC 27043	Incident investigation
ISO/IEC 27050	Electronic discovery
ISO 27799	Guidelines for health industry organizations on protecting health information

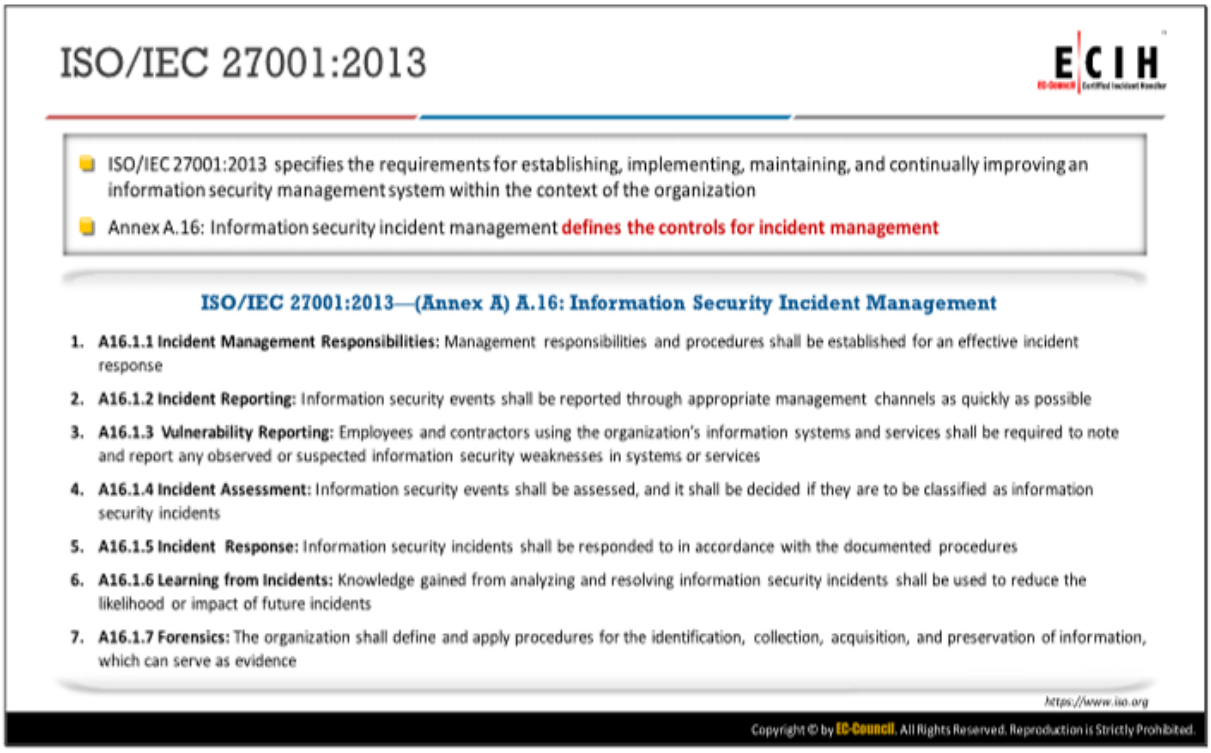
ISO/IEC 27000 Series

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

The ISO/IEC 27000 is the information security standard developed and published by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). It provides a global framework for effective information security management for all types of organizations. The ISO/IEC 27000:2018 is the latest revision, and

defines information technology, security techniques, information security management systems, and vocabulary, with an overview.

The ISO/IEC 27000 family contains many standards that define information security management systems as shown on the above slides.



ISO/IEC 27001:2013

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

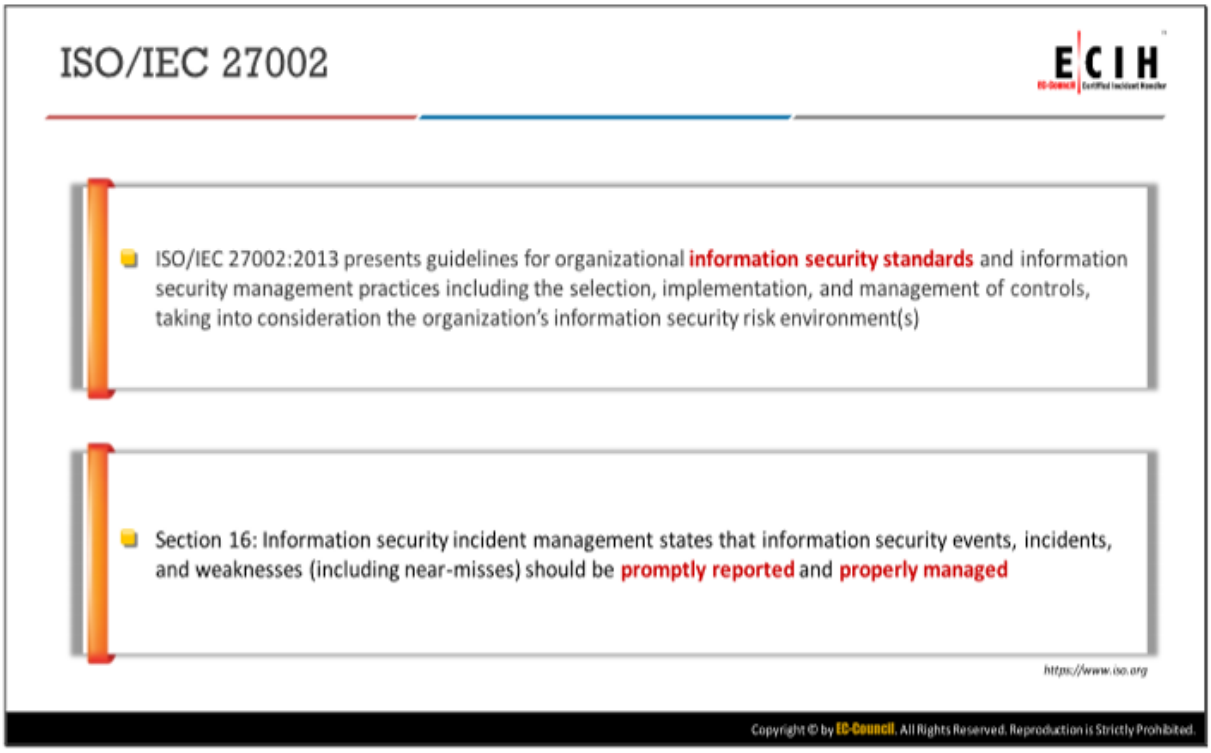
ISO/IEC 27001 is a standard framework for managing and protecting information systems and other network resources so that they remain safe and secure. An organization that implements this framework assures its customers, partners, and vendors that their information is safe and that it can handle information securely. ISO/IEC 27001:2013 is a revised version with enhanced support to secure information systems.

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. Annex A.16: Information Security Incident Management defines the controls for incident management.

ISO/IEC 27001:2013—(Annex A) A.16: Information Security Incident Management includes:

- **A16.1.1 Incident Management Responsibilities**: Management responsibilities and procedures shall be established for an effective incident response.
- **A16.1.2 Incident Reporting**: Information security events shall be reported through appropriate management channels as quickly as possible.
- **A16.1.3 Vulnerability Reporting**: Employees and contractors using an organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
- **A16.1.4 Incident Assessment**: Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.

- **A16.1.5 Incident Response:** Information security incidents shall be responded to in accordance with the documented procedures.
- **A16.1.6 Learning from Incidents:** Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
- **A16.1.7 Forensics**: An organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.



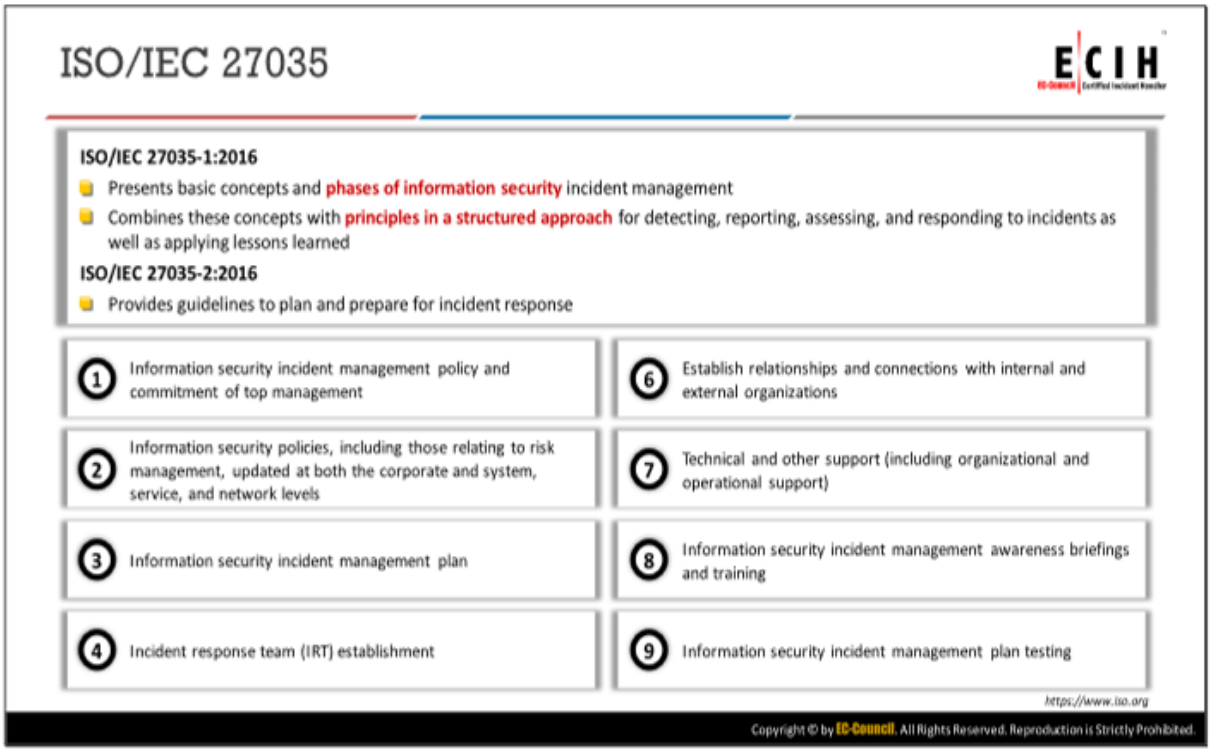
ISO/IEC 27002

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

ISO/IEC 27002 is a standard framework that provides recommendations for implementing information security controls for organizations that initiate, implement, or maintain information security management systems (ISMSs).

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices, including the selection, implementation, and management of controls taking into consideration the organization's information security risk environment(s).

In this standard, section 16 defines "information security incident management" and subsection 16.1 defines "management of information security incidents and improvements." According to ISO/IEC 27002, there should be responsibilities and procedures to manage (report, assess, respond to, and learn from) information security events, incidents, and weaknesses consistently and effectively and to collect forensic evidence.



ISO/IEC 27035

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

ISO/IEC 27035 is a standard for dealing with "Information Security Incident Management," and defines recommendations and best practices for developing an efficient incident management plan and allows organizations to prepare for the incidents. This standard is divided into three parts:

- ISO/IEC 27035-1:2016 Principles of incident management
- ISO/IEC 27035-2:2016 Guidelines to plan and prepare for incident response
- ISO/IEC 27035-3 Guidelines for incident response operations (draft)

These standards are discussed below:

- **ISO/IEC 27035-1:2016**

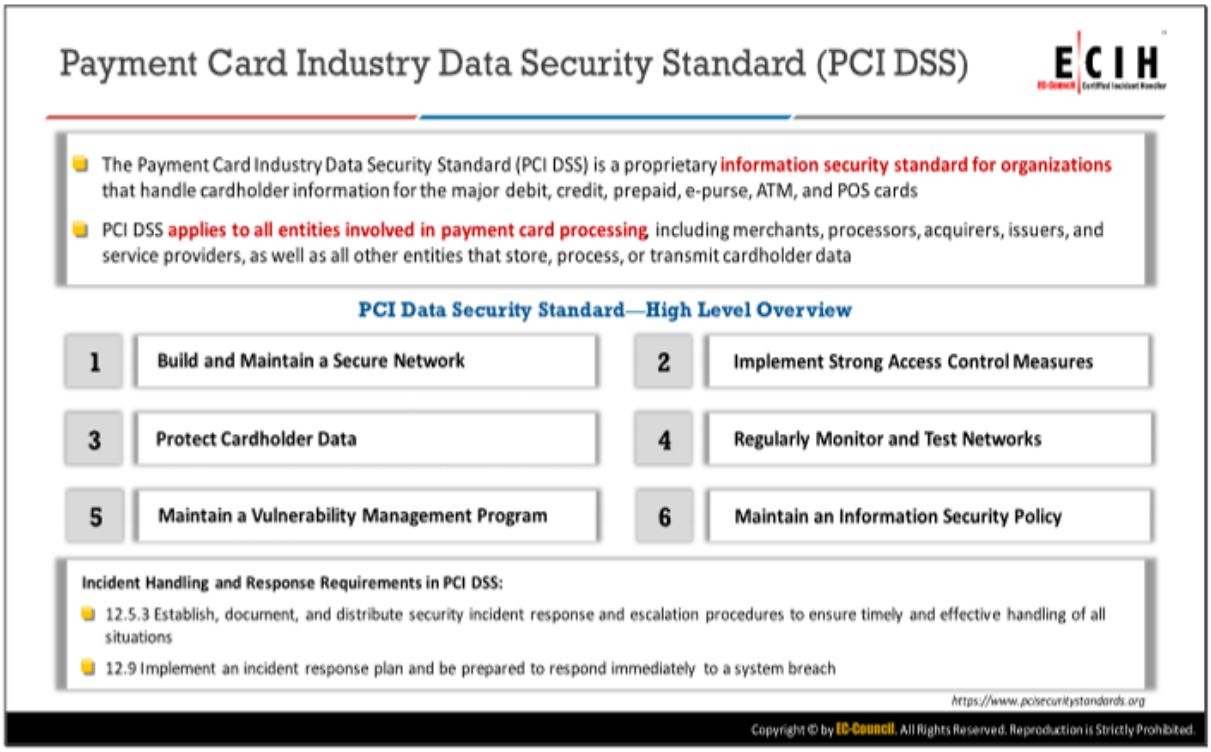
  This presents basic concepts and phases of information security incident management. It combines these concepts with principles in a structured approach for detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.

- **ISO/IEC 27035-2:2016**

  This provides guidelines to plan and prepare for incident response:

  - Information security incident management policy and commitment of top management
  - Information security policies, including those relating to risk management, updated at the corporate level as well as system, service, and network levels

- Information security incident management plan
- Incident response team (IRT) establishment
- Establishing relationships and connections with internal and external organizations
- Technical and other support (including organizational and operational support)
- Information security incident management awareness briefings and training
- Information security incident management plan testing



Payment Card Industry Data Security Standard (PCI DSS)

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

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and point of sale (POS) cards. It 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. A high-level overview of the PCI DSS requirements is developed and maintained by the Payment Card Industry (PCI) Security Standards Council.

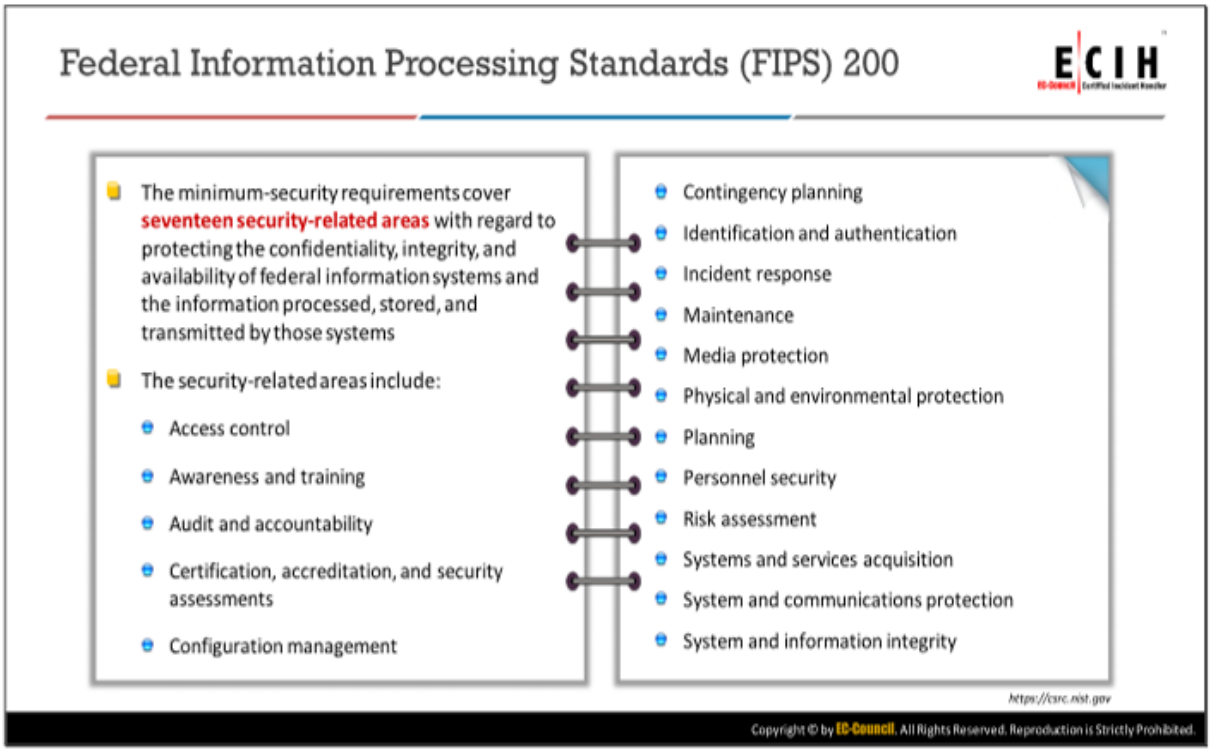
PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network	▪ Install and maintain a firewall configuration to protect cardholder data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	▪ Protect stored cardholder 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 1.1: Table Showing the PCI Data Security Standard - High Level Overview

Incident Handling and Response Requirements in PCI DSS:

- 12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

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



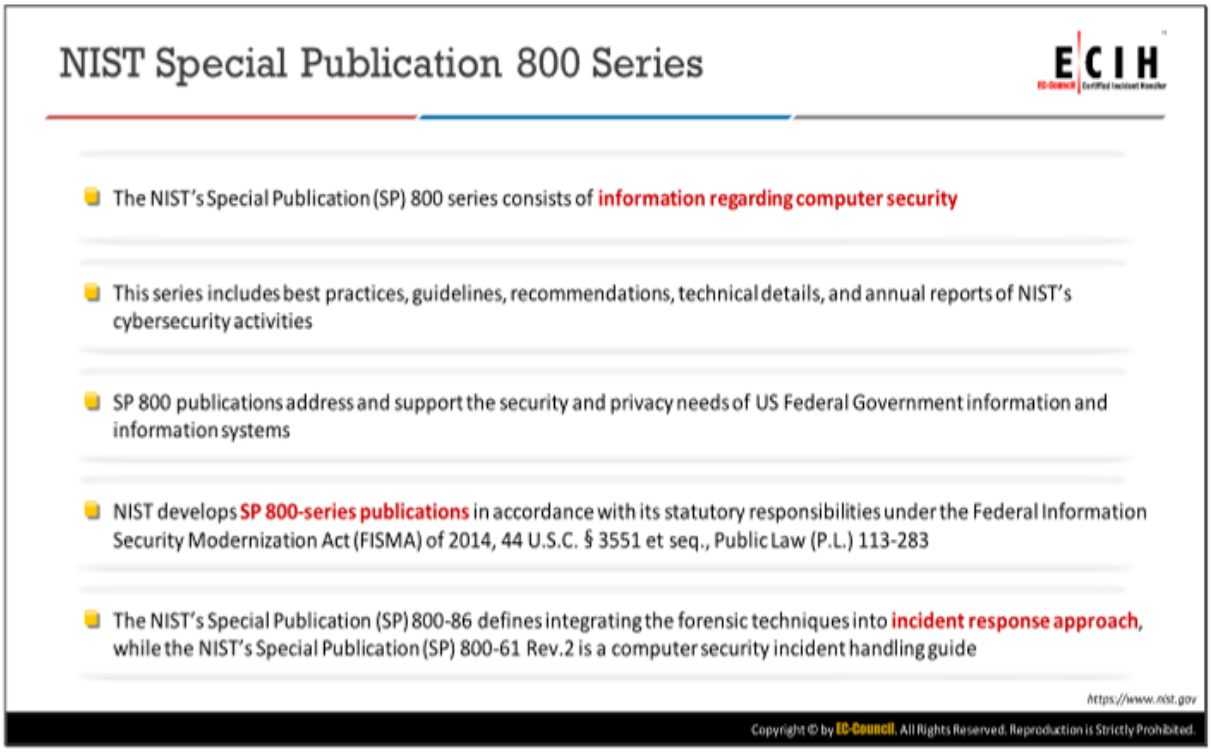
Federal Information Processing Standards (FIPS) 200

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

The NIST has published this standard, which defines computer systems usage for the US federal government. The minimum security requirements cover seventeen security-related areas about protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.

The security-related areas include:

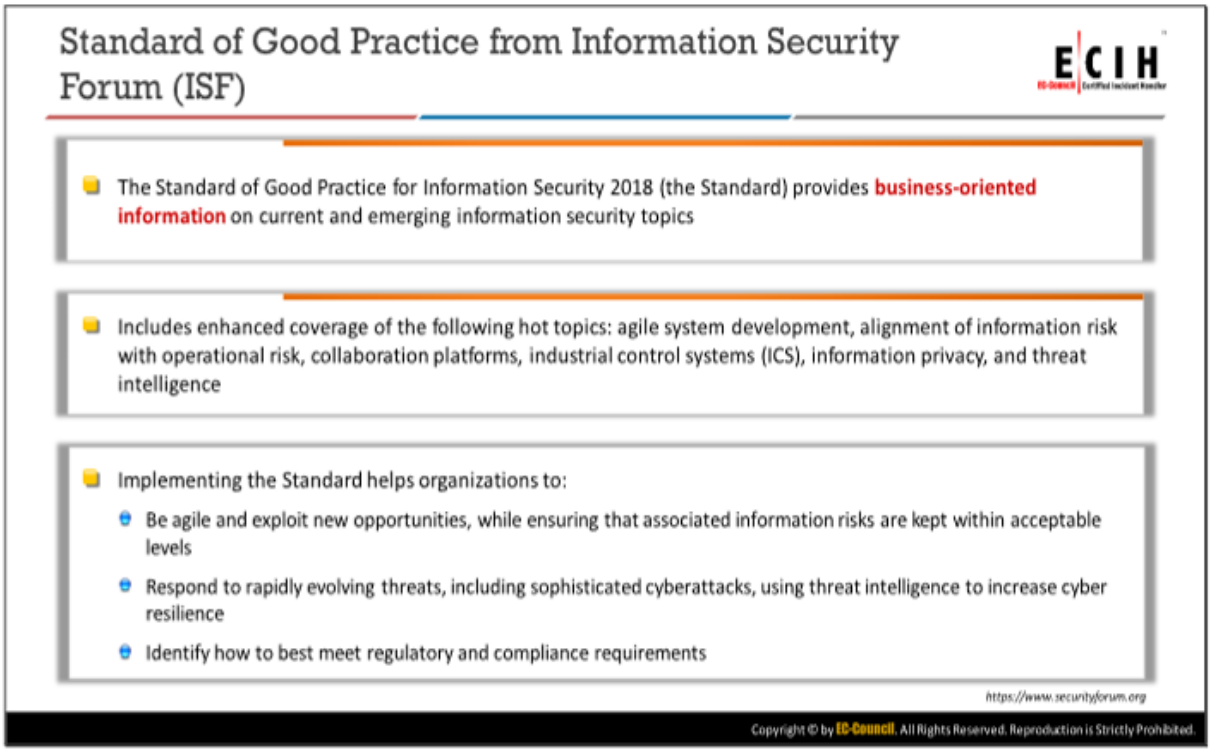
- Access control
- Awareness and training
- Audit and accountability
- Certification, accreditation, and security assessments
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Physical and environmental protection
- Planning
- Personnel security
- Risk assessment
- Systems and services acquisition
- System and communications protection
- System and information integrity



NIST Special Publication 800 Series

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

The NIST's Special Publication (SP) 800 series consists of information regarding computer security: best practices, guidelines, recommendations, technical details, and annual reports of NIST's cybersecurity activities. SP 800 publications address and support the security and privacy needs of US federal government information and information systems. NIST develops SP 800-series publications in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. The NIST's Special Publication (SP) 800-86 defines integrating the forensic techniques into incident response approach, while the NIST's Special Publication (SP) 800-61 Rev.2 is a computer security incident handling guide.



Standard of Good Practice from Information Security Forum (ISF)

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

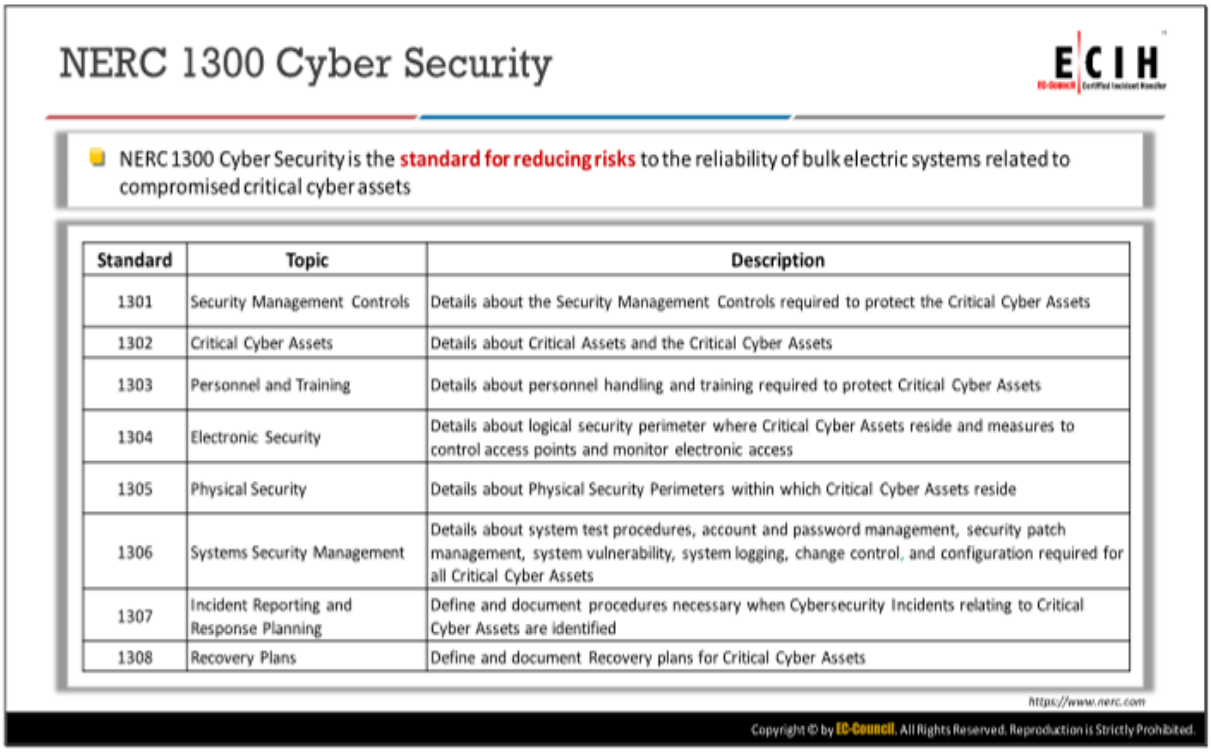
The Standard of Good Practice for Information Security 2018 (the Standard) provides business-orientated focus on current and emerging information security topics. This includes enhanced coverage of the following hot topics: agile system development, alignment of information risk with operational risk, collaboration platforms, industrial control systems (ICS), information privacy, and threat intelligence.

With its comprehensive coverage of information security controls and information risk-related guidance, it provides business leaders and their teams with an internationally recognized set of good practices.

Implementing this standard helps organizations to

- Be agile and exploit new opportunities, while ensuring that associated information risks are kept within acceptable levels
- Respond to rapidly evolving threats, including sophisticated cyberattacks, using threat intelligence to increase cyber resilience
- Identify how regulatory and compliance requirements can best be met

The standard, along with the ISF Benchmark, the ISF's comprehensive security control assessment tool, provide complete coverage of the topics set out in ISO/IEC 27002:2013, NIST Cybersecurity Framework, CIS Top 20, PCI DSS, and COBIT 5 for Information Security.

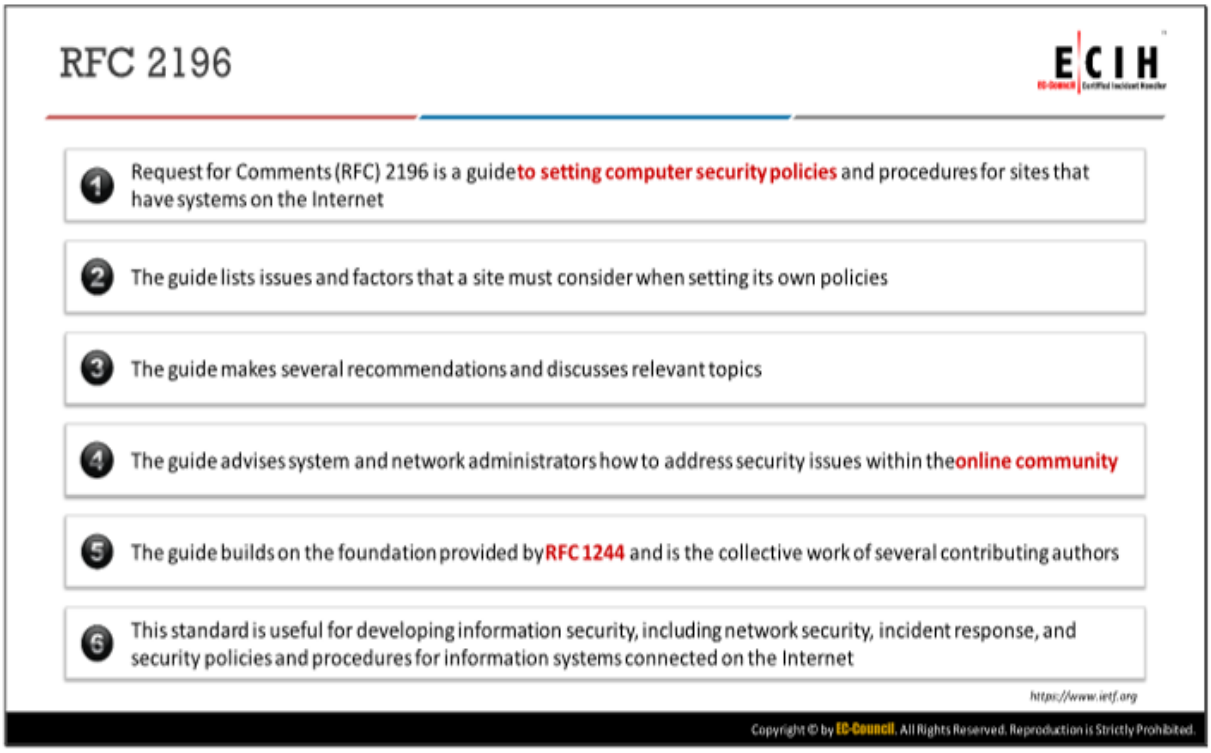


NERC 1300 Cyber Security

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

NERC 1300 Cyber Security is the standard to reduce risks to the reliability of bulk electric systems from any compromise of their critical cyber assets. This cybersecurity standard applies to entities performing Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity.

The table on the above slide shows NERC 1300 Cyber Security standard series.



RFC 2196

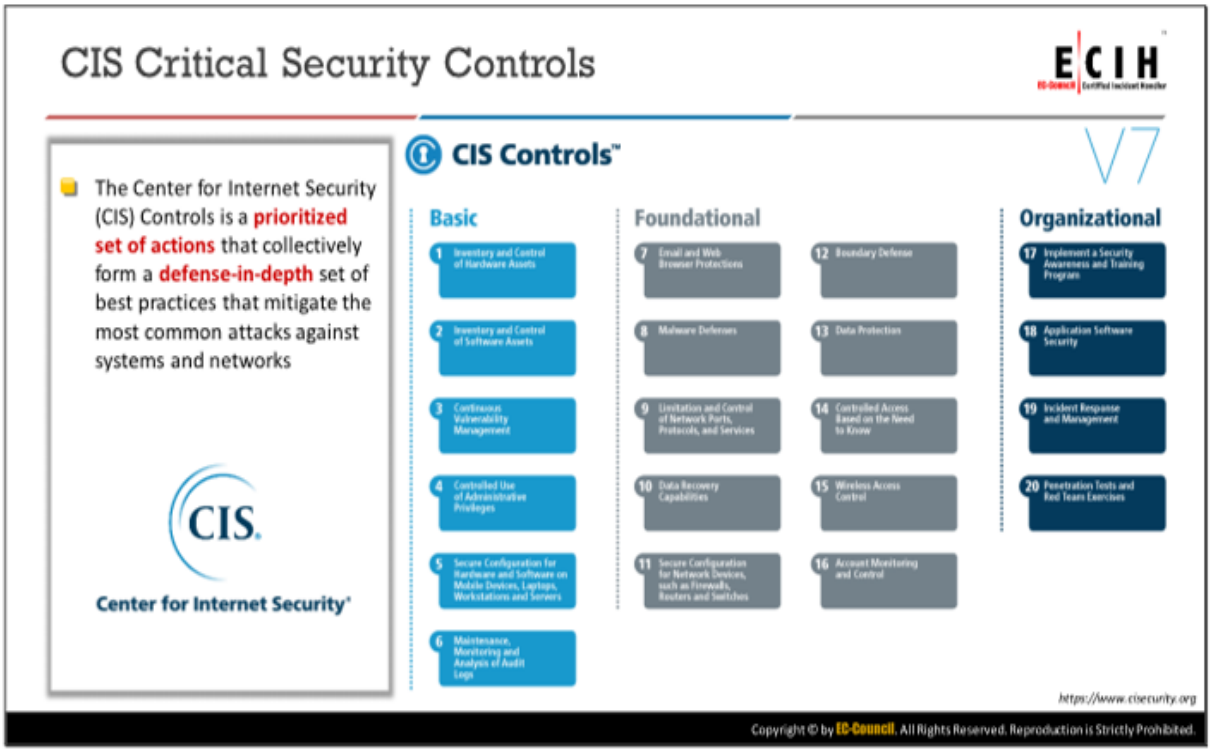
Source: *https://www.ietf.org*

Request for Comments (RFC) 2196 is a guide to setting computer security policies and procedures for sites that have systems on the internet. This guide lists issues and factors that a site must consider when setting their own policies. It makes several recommendations and provides discussions of relevant areas. This document provides guidance to system and network administrators on how to address security issues within the internet community. It builds on the foundation provided in RFC 1244 and is the collective work of several contributing authors. This standard is useful for developing information security, including network security, incident response, and security policies and procedures for information systems connected on the internet.

Overview of Cybersecurity Frameworks

Cybersecurity frameworks are incorporated into existing cybersecurity programs to help organizations take effective cybersecurity measures to safeguard crucial data and assets. These frameworks provide a systematic approach to assessing cybersecurity incidents in the organization.

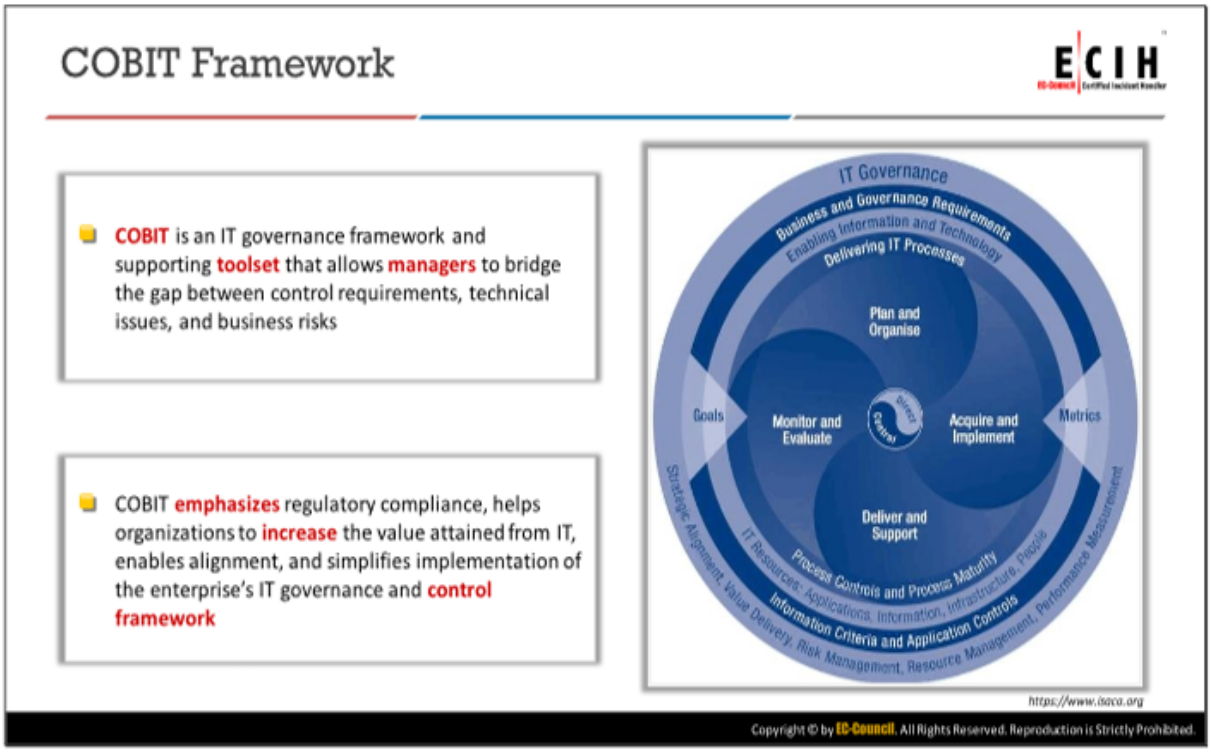
This section discusses various important cybersecurity frameworks, such as CIS Critical Security Controls, COBIT Framework, and NIST Special Publication 800-61.



CIS Critical Security Controls

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

Center for Internet Security (CIS) Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. CIS Controls are a relatively short list of high-priority, highly effective defensive actions that provide a "must-do, do-first" starting point for every enterprise seeking to improve its cyber defense. CIS Controls are developed by a community of IT experts who apply their firsthand experience as cyber defenders to create these globally accepted security best practices. These experts come from a wide range of sectors, including, retail, manufacturing, healthcare, education, government, defense, and others.



COBIT Framework

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

COBIT is a business framework for IT governance and management toolset enabling managers to bridge the gap between control requirements, technical issues, and business risks. The framework offers globally accepted principles, practices, analytical tools, and models to help increase trust in and value from information systems.

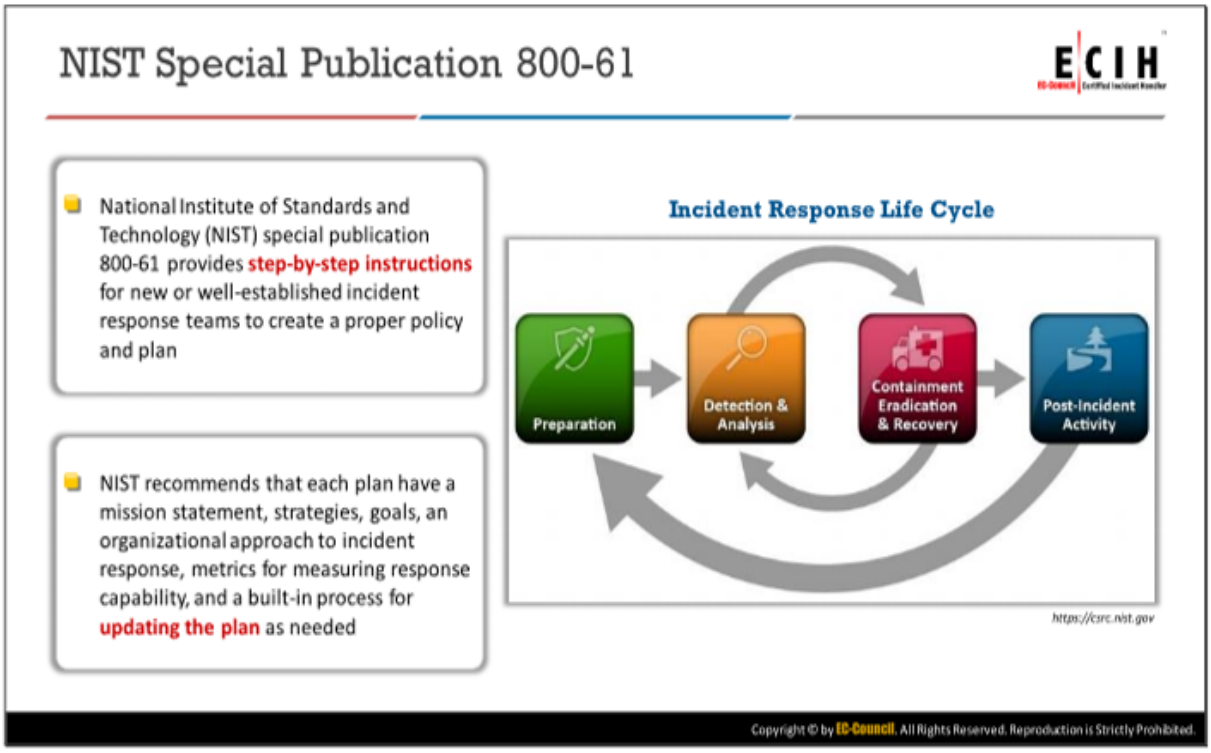
COBIT emphasizes regulatory compliance, helping organizations increase the value attained from IT, enables alignment, and simplifies the implementation of an enterprise's IT governance and control framework.

COBIT helps enterprises of all sizes to:

- Maintain high-quality information to support business decisions
- Achieve strategic goals and realize business benefits through the effective and innovative use of IT
- Achieve operational excellence through reliable and efficient application of technology
- Maintain IT-related risk at an acceptable level
- Optimize the cost of IT services and technology
- Support compliance with relevant laws, regulations, contractual agreements, and policies

The COBIT Framework is based on five key principles for the governance and management of enterprise IT:

- Meeting stakeholder needs
- Covering the enterprise end-to-end
- Applying a single, integrated framework
- Enabling a holistic approach
- Separating governance from management



NIST Special Publication 800-61

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

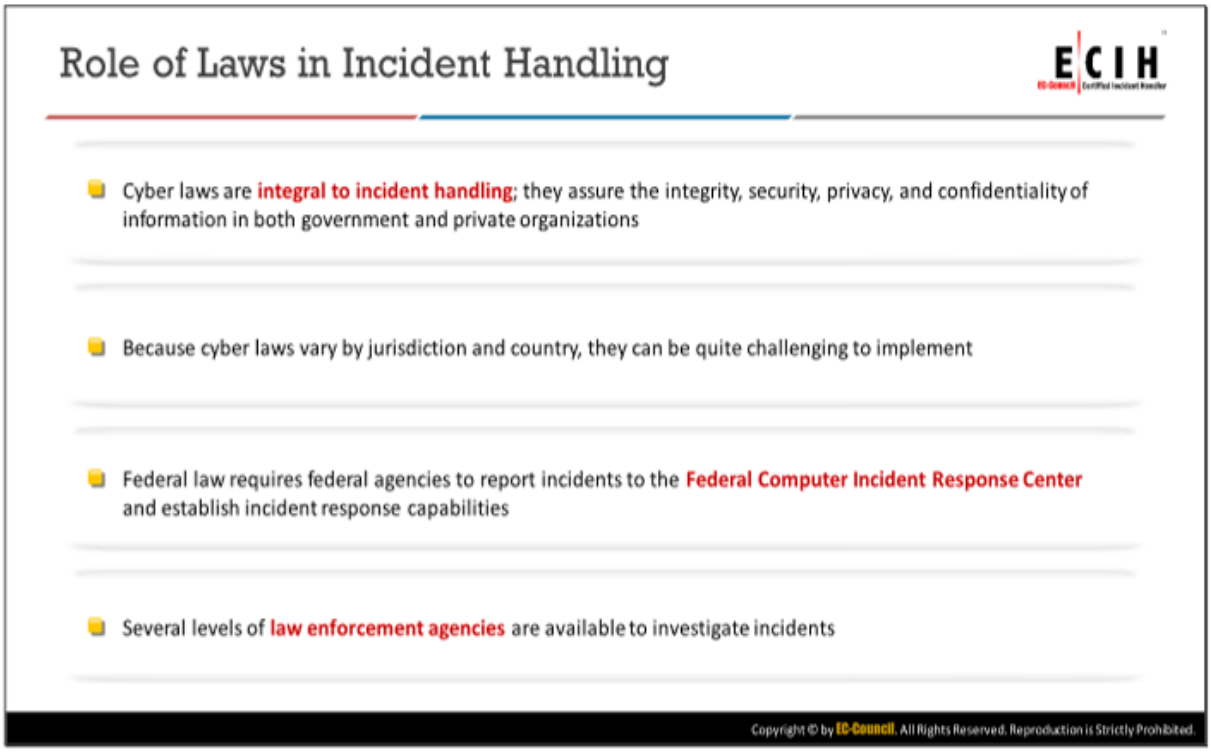
National Institute of Standards and Technology (NIST) special publication 800-61 provides step-by-step instructions for new or well-established incident response teams to create a proper policy and plan. NIST recommends that each plan should have a mission statement, strategies and goals, an organizational approach to incident response, metrics for measuring the response capability, and a built-in process for updating the plan as needed. The guide recommends reviewing each incident to prepare for future attacks and to provide stronger protections of systems and data. It includes a life cycle for incident handling and response that contains several phases:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity

Importance of Laws in Incident Handling

Cybersecurity incidents victimizing by an organization may have severe consequences for the organization's business operations. It is vital to report cybersecurity incidents in order to ensure safe security infrastructure in an organization. In such a scenario, laws function as a system of rules and guidelines enforced by a particular country or community to govern behavior.

This section discusses the role of laws in incident handling along with the legal and jurisdictional issues that may be encountered by an organization while dealing with an incident.



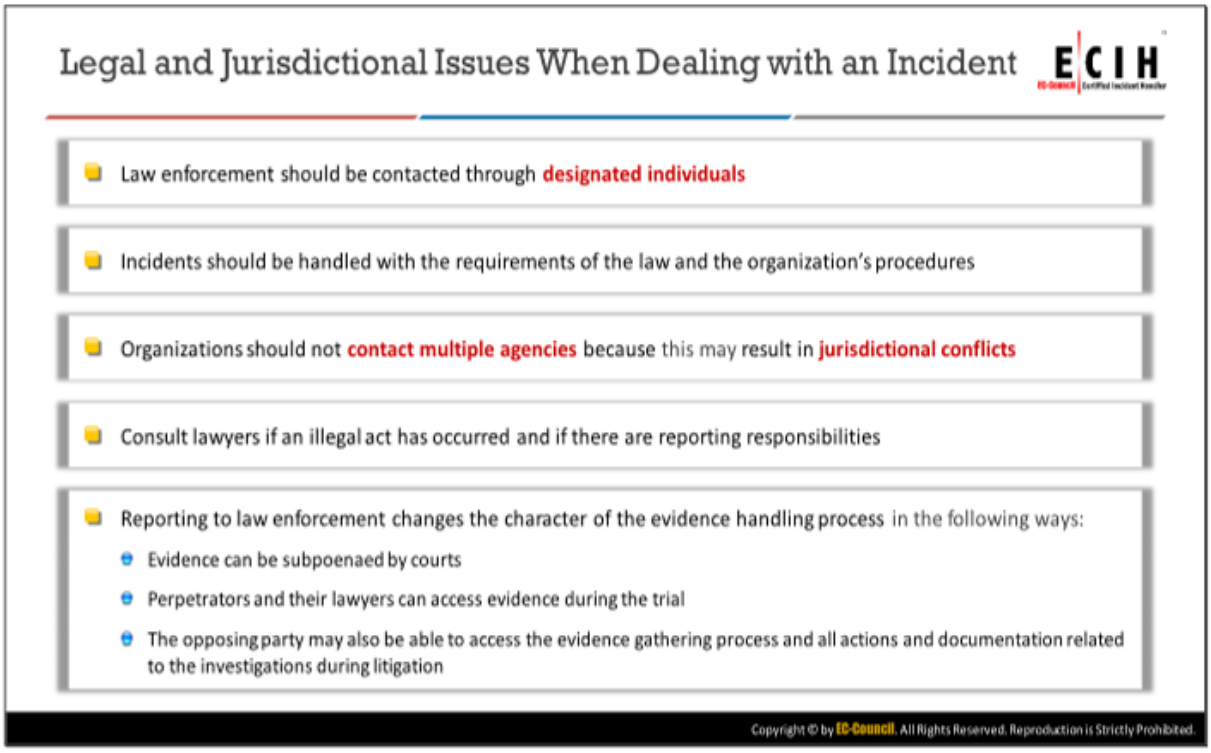
Role of Laws in Incident Handling

Cyber laws are integral to incident handling as they provide 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 internet use all over the world. Cyber laws vary by jurisdiction and country, so implementing these laws is quite challenging. Violating these laws may result in punishments ranging from fines to imprisonment.

Federal law requires federal agencies to report incidents to the Federal Computer Incident Response Center. It requires federal agencies to establish incident response capabilities. Similarly, various laws in different countries mandate organizations to build incident handling capabilities. The incident response team is responsible for reporting any incidents occurring inside an organization. It should be familiar with the reporting procedures for all relevant law enforcement agencies and be well prepared to recommend suitable agency and contact details.

Several levels of law enforcement agencies are available to investigate incidents. Law enforcement agencies start investigation based on the severity of the incident. They provide technical assistance in recovering from the incident and preventing it from happening in future. Necessary criminal and civil actions are taken up by law enforcement agencies. Usually in any country, law is enforced by:

- Federal investigative agencies (for example, in the United States, the FBI and the US Secret Service)
- District attorney offices
- State law enforcement
- Local law enforcement



Legal and Jurisdictional Issues when Dealing with an Incident

An organization can be subjected to different jurisdictions as per the locations where it operates. It is essential for organizations to stay alert about data breach notifications from each jurisdiction in which they function and to have internal policies with applicable laws to deal with such scenarios. Each jurisdiction enforces data protection standards in context to the time and process in which organizations should or must inform customers or other related individuals about the data breaches. This helps the concerned individuals to take required actions in case of severe consequences, such as financial losses or identity theft.

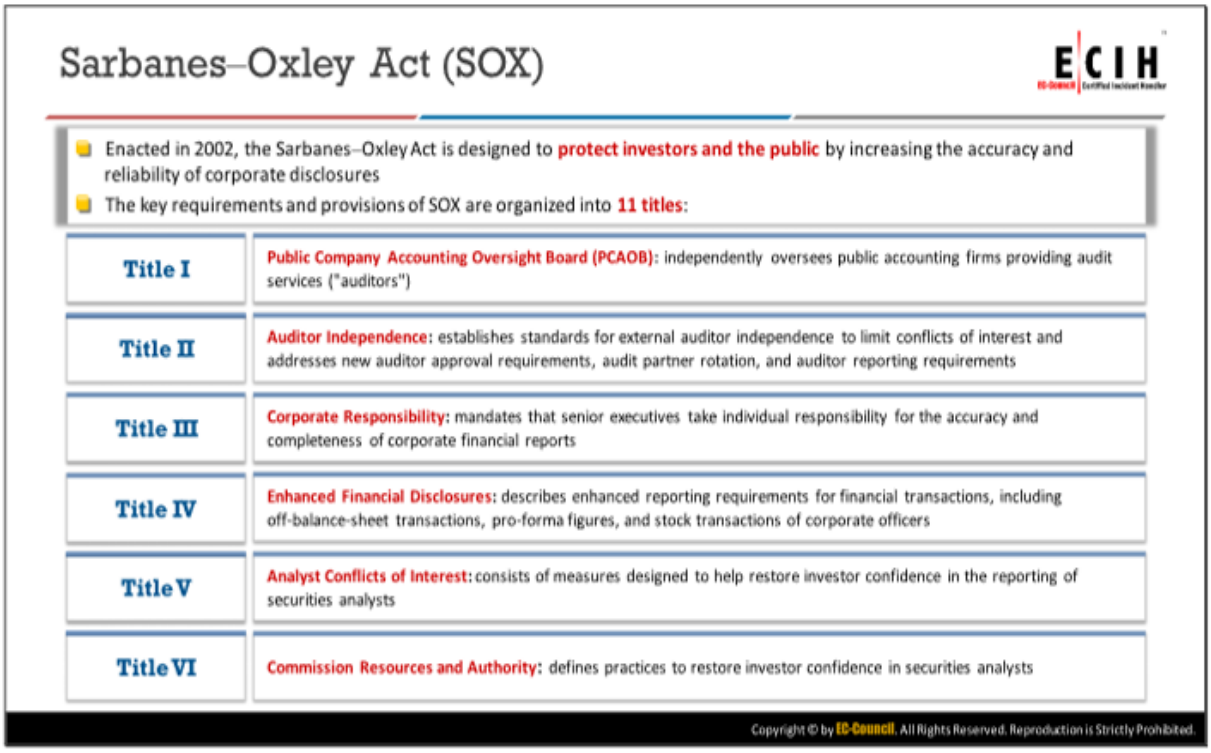
Following are ways to handle legal and jurisdictional issues when dealing with an incident:

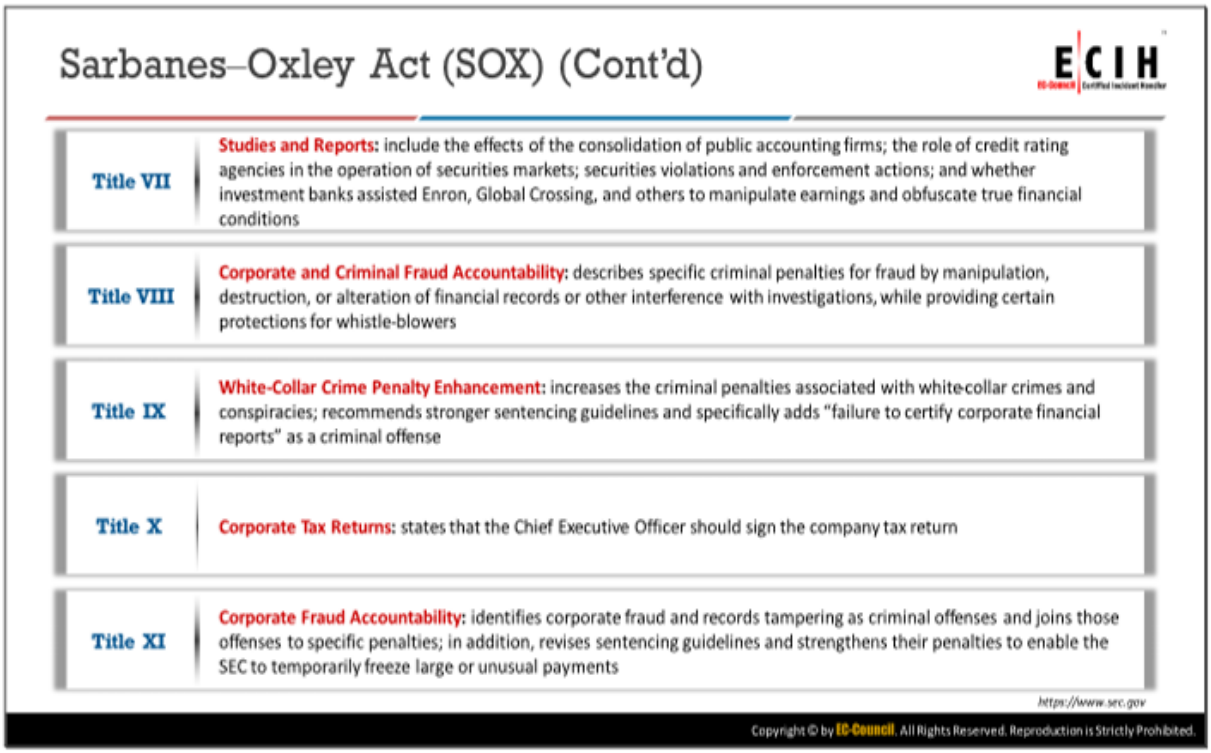
- Law enforcement agencies should be contacted through designated individuals.
- Incidents should be handled within the requirements of the law and the organization's procedures.
- Organizations should not contact multiple agencies because it might result in jurisdictional conflicts.
- Consult lawyers if an illegal act has occurred and there are reporting responsibilities.
- Reporting to law enforcement changes the character of the evidence handling process; for instance:
  - Evidence can be subpoenaed by courts.
  - Perpetrators and their lawyers can get access to it in the trial.
  - Evidence-gathering process and all actions and documentation pertaining to the investigation may also be accessible to the other party during litigation.

Incident Handling and Legal Compliance

Incident handling and legal compliance play a major role in handling security incidents more efficiently, helping organizations manage legal consequences arising from critical security incidents. Legal compliances ensure that any evidence collected is admissible in a court of law to help an organization recover from financial loss due to an incident.

This section discusses legal compliance and laws such as HIPAA, SOX, FISMA (see below), and General Data Protection Regulation (GDPR) that are essential while handling security incidents.





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 does describe the records the 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 (for example, 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 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 the financial condition and specific enhanced reviews by the Securities and Exchange Commission (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 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 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 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**

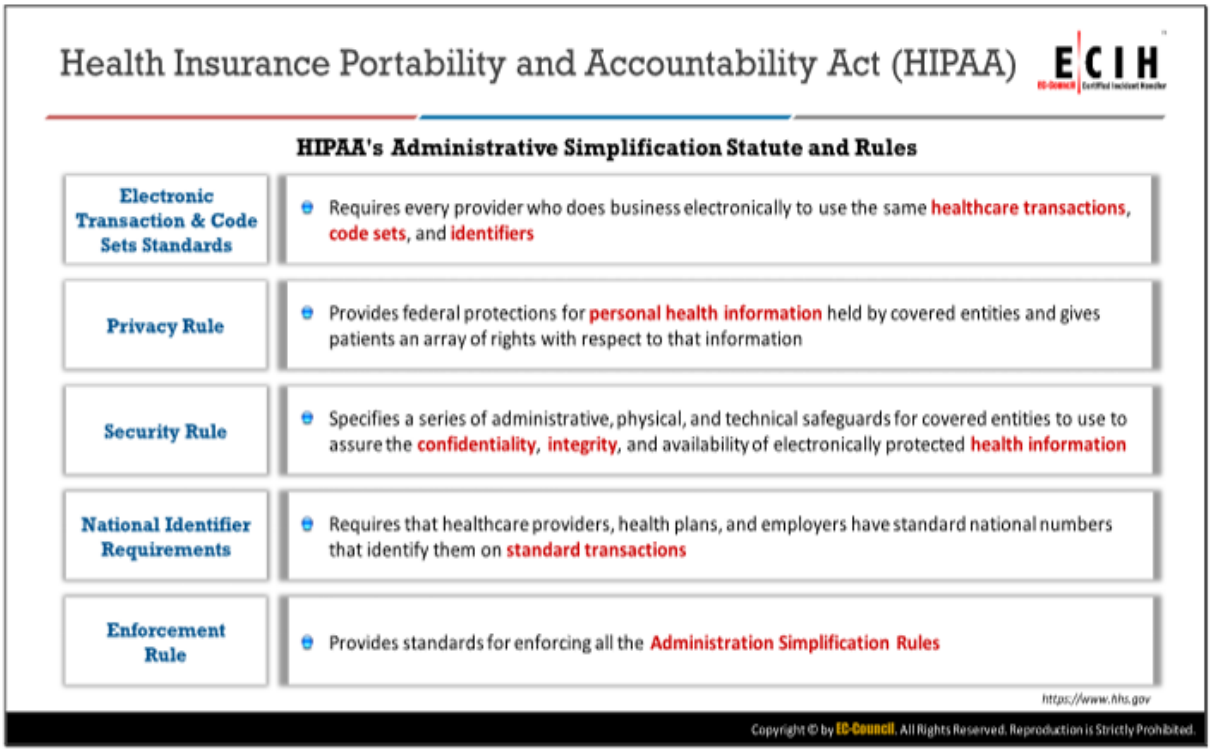
  Title IX, also known as the "White Collar Crime Penalty Enhancement Act of 2002," consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate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



Health Insurance Portability and Accountability Act (HIPAA)

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

The Health Insurance Portability and Accountability Act (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, healthcare clearinghouses, and certain healthcare providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for Electronic Data Interchange (EDI) of healthcare data, namely, 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. These standards require every provider, who does business electronically to use the same healthcare 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, healthcare clearinghouses, and those healthcare providers who conduct certain healthcare transactions electronically. It 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 the 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 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**

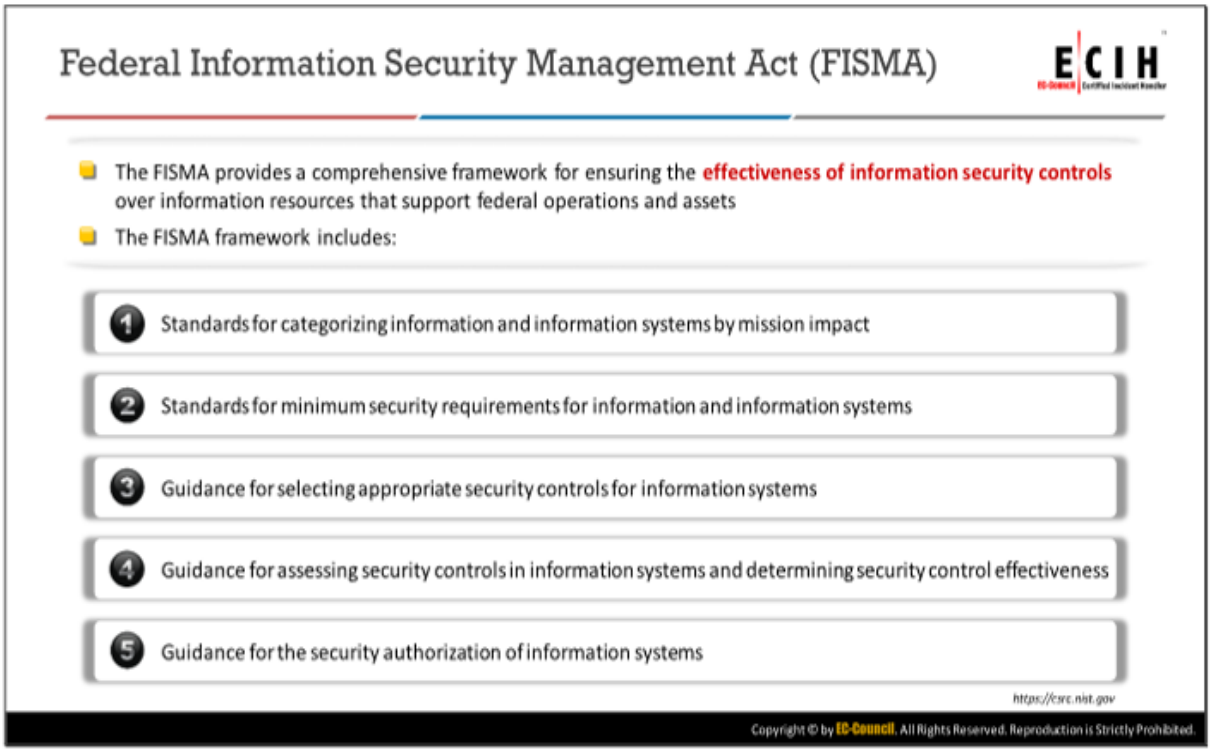
  The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that employers have standard national numbers that identify them on standard transactions.

- **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 healthcare providers. Covered healthcare providers and all health plans and healthcare clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a ten-position, intelligence-free numeric identifier (ten-digit number) that does 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.



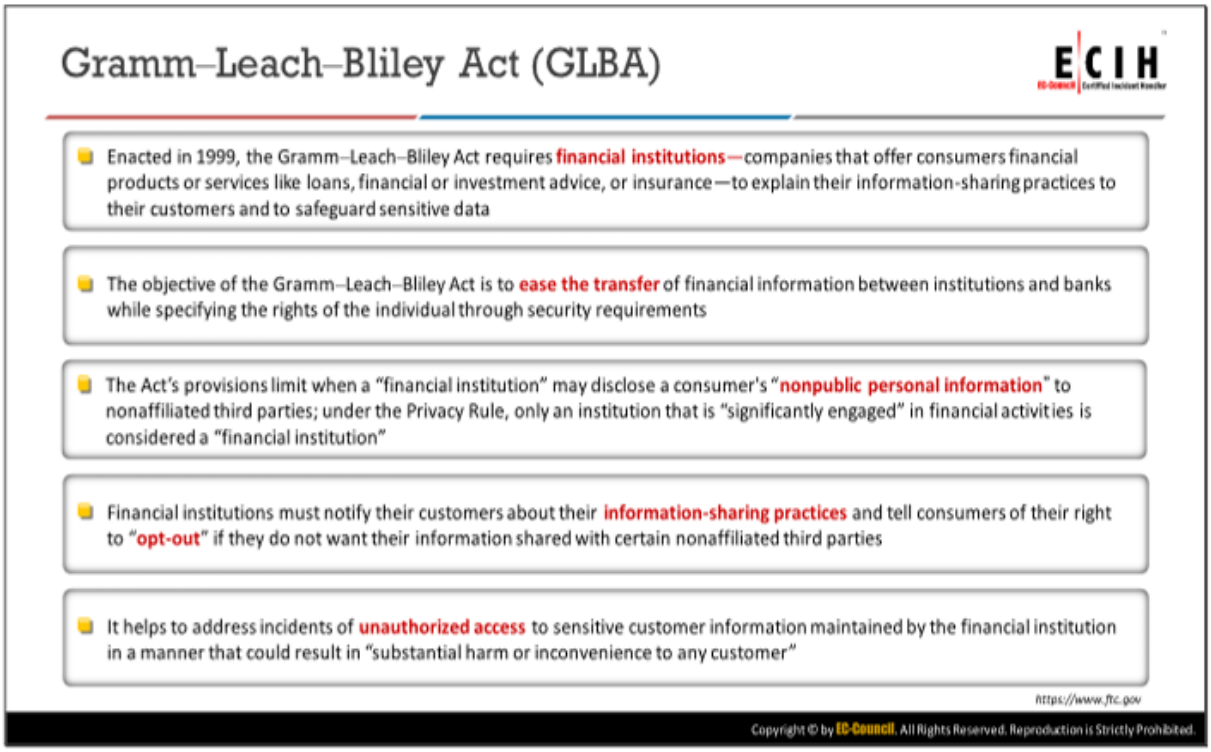
Federal Information Security Management Act (FISMA)

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

The Federal Information Security Management Act of 2002 (FISMA) concerns several key required security standards and guidelines. It 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



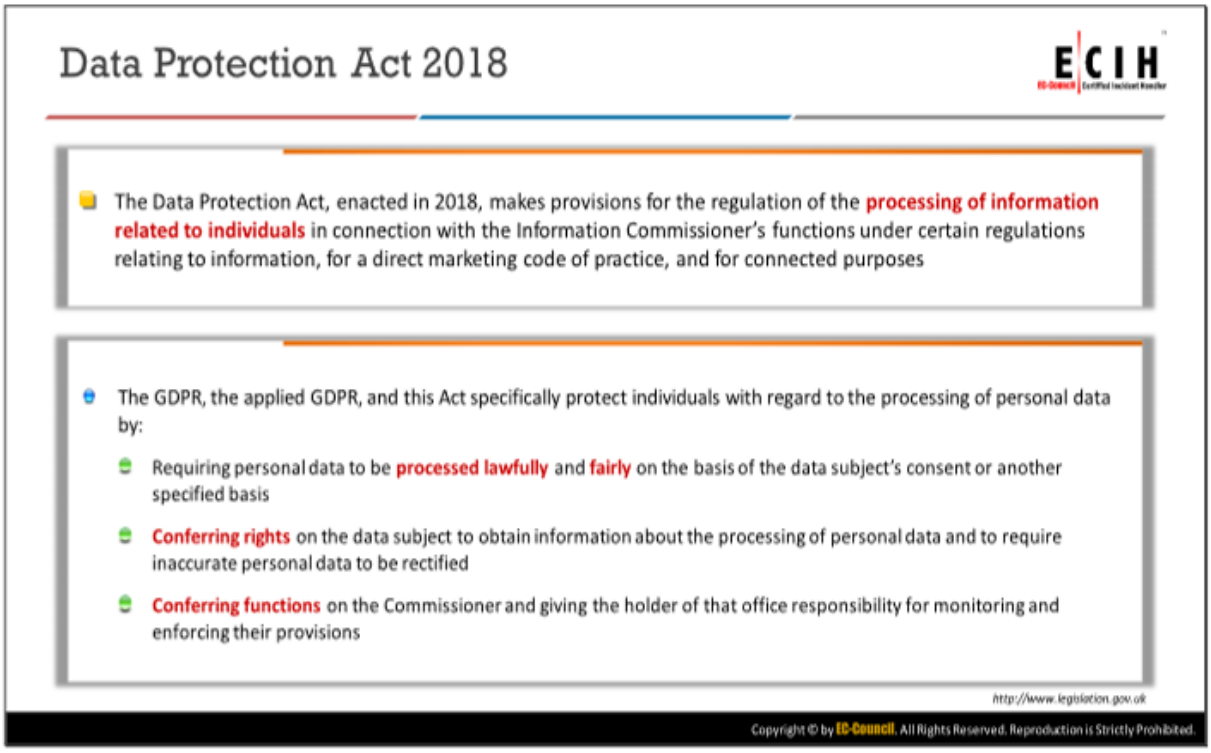
Gramm–Leach–Bliley Act (GLBA)

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

Enacted in 1999, Gramm–Leach–Bliley Act (GLBA) requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data. The objective of the Gramm–Leach–Bliley Act is to ease the transfer of financial information between institutions and banks while more explicitly addressing the rights of the individual through security requirements.

Its provisions limit when a "financial institution" may disclose a consumer's "nonpublic personal information" to nonaffiliated third parties. The law covers a broad range of financial institutions, including many companies not traditionally considered to be financial institutions but still engaged in certain "financial activities." Under the Privacy Rule, an institution that is "significantly engaged" in financial activities is considered a financial institution.

It is essential for the financial institutions to notify their customers about their information-sharing practices and tell consumers of their right to opt-out if they don't want their information shared with certain nonaffiliated third parties. In addition, any entity that receives consumer financial information from a financial institution is restricted in its reuse and re-disclosure of that information. This helps to address incidents of unauthorized access to sensitive customer information maintained by the financial institution in a manner that could result in "substantial harm or inconvenience to any customer."



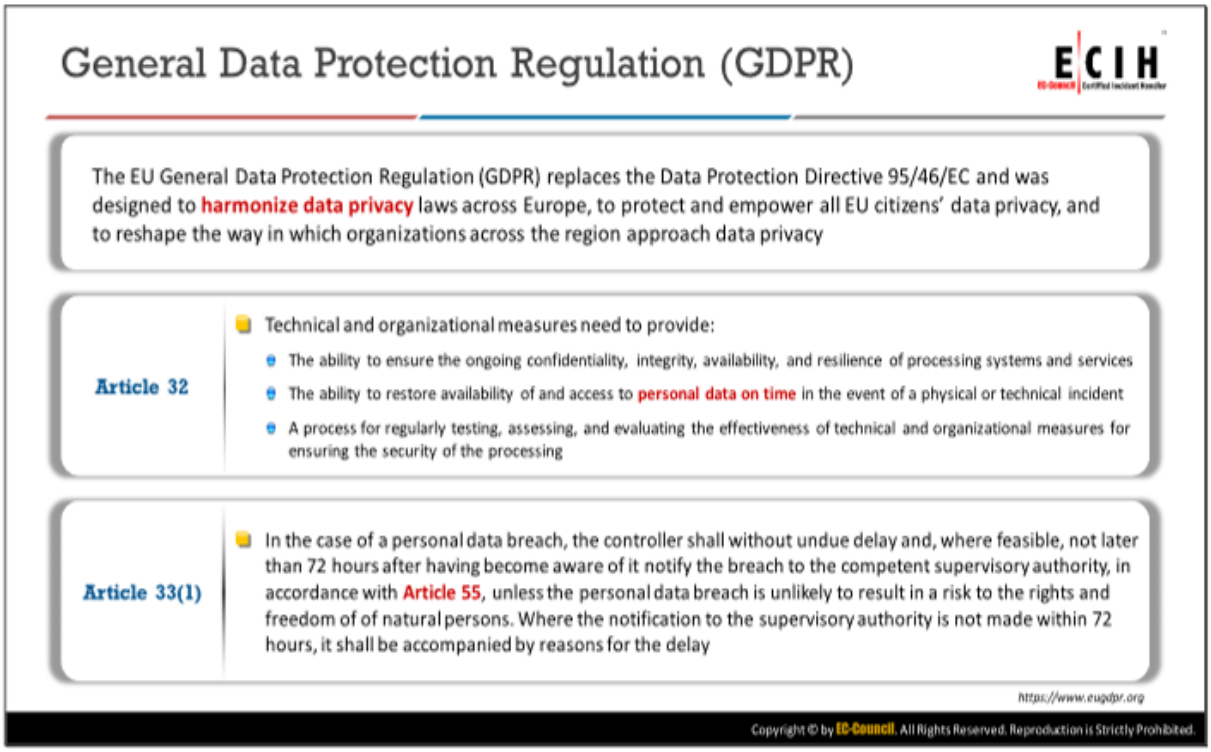
Data Protection Act 2018

Source: *http://www.legislation.gov.uk*

The Data Protection Act, enacted in 2018, makes provision for the regulation of the processing of information relating to individuals in connection with the Information Commissioner's functions under certain regulations relating to information, for a direct marketing code of practice, and for connected purposes.

It provides protection of personal data in the following way:

- The GDPR, the applied GDPR (see below), and this Act protect individuals with regard to the processing of personal data, in particular by:
  - Requiring personal data to be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis
  - Conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified
  - Conferring functions on the Commissioner, giving the holder of that office responsibility for monitoring and enforcing the Act's provisions
- When carrying out functions under the GDPR, the applied GDPR, and this Act, the Commissioner must have regard for the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers, and others, and matters of general public interest.



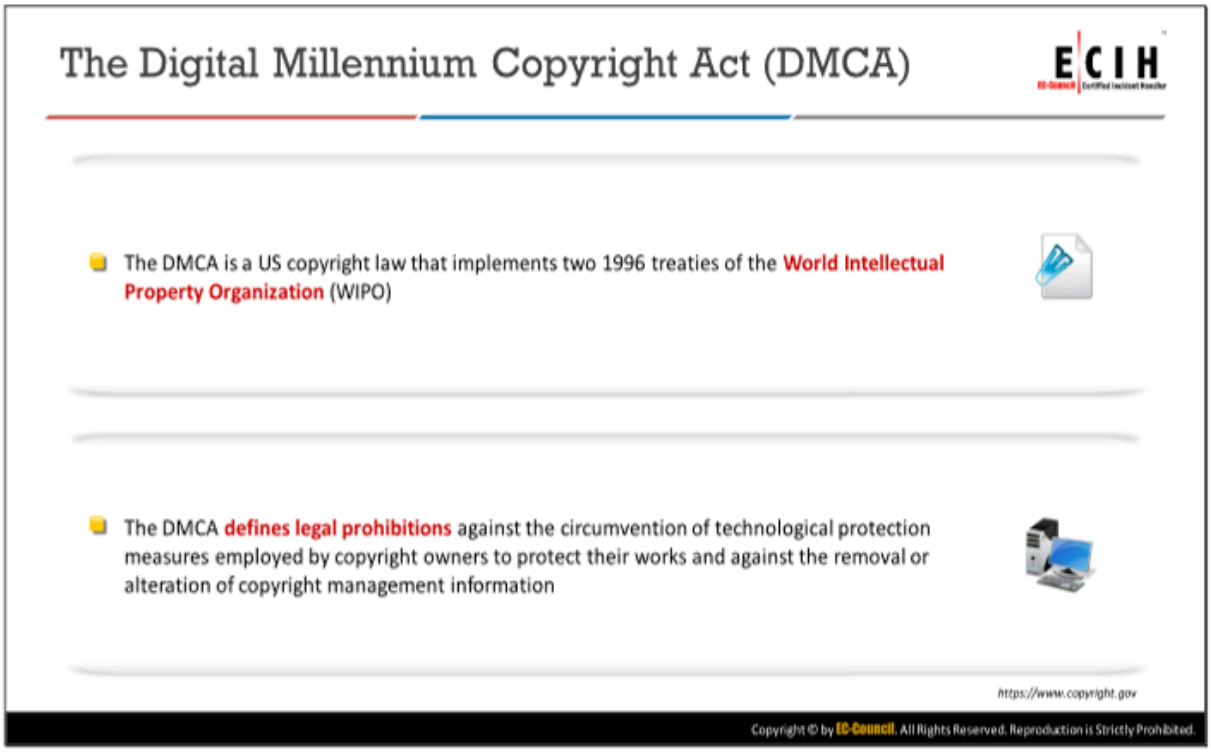
General Data Protection Regulation (GDPR)

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

The EU General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

- **Article 32: Technical and organizational measures need to provide:**
  - The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services
  - The ability to restore availability of and access to personal data on time in the event of a physical or technical incident
  - A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing
- **Article 33(1):**

  In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, give notification of the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.



The Digital Millennium Copyright Act (DMCA)

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

The Digital Millennium Copyright Act (DMCA) is a US 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 US 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 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

The 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 grants exemption for the making of "ephemeral recordings," the third promotes distance education study, the fourth provides exemption for nonprofit libraries and archives, the fifth allows webcasting amendments to the digital performance rights in sound recordings, and the sixth 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**

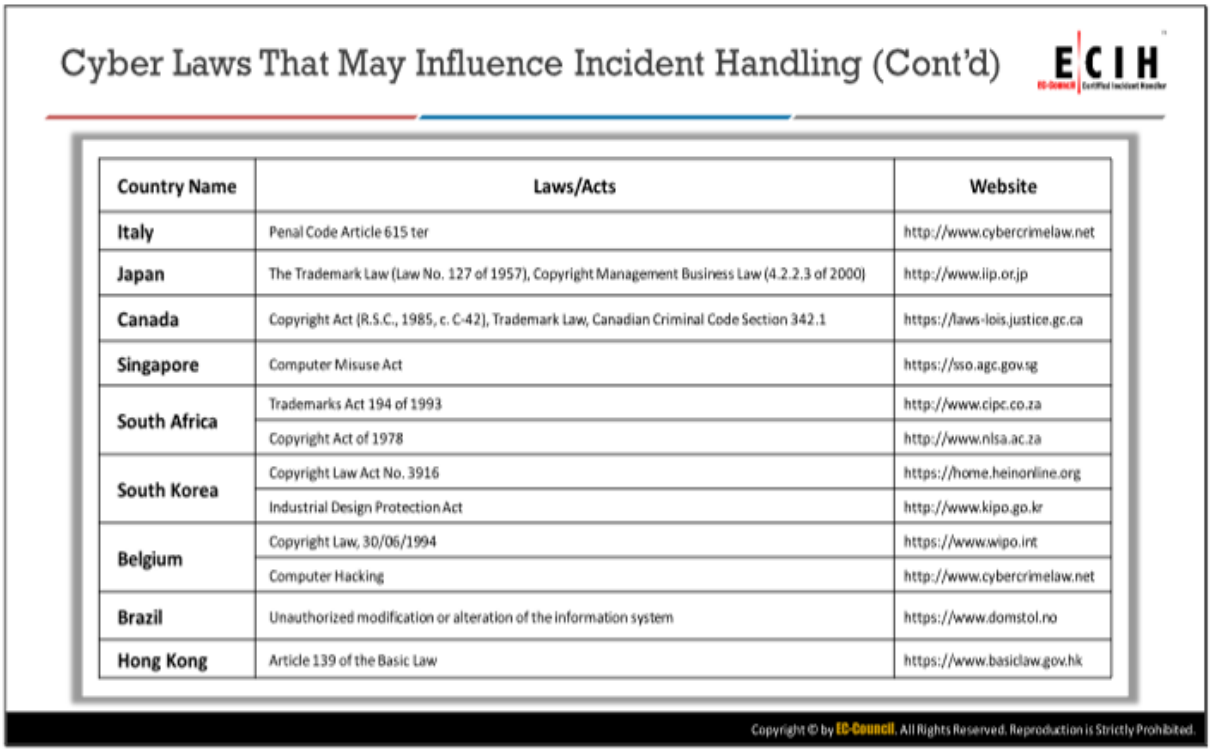
  Title V of the DMCA is titled the Vessel Hull Design Protection Act (VHDPA). It creates a new system for protecting original designs of certain useful articles that make them attractive or distinctive in appearance. For the purposes of the VHDPA, "useful articles" are limited to the hulls (including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

Cyber Laws That May Influence Incident Handling

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	https://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://www.energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov

Cyber Laws That May Influence Incident Handling (Cont'd)

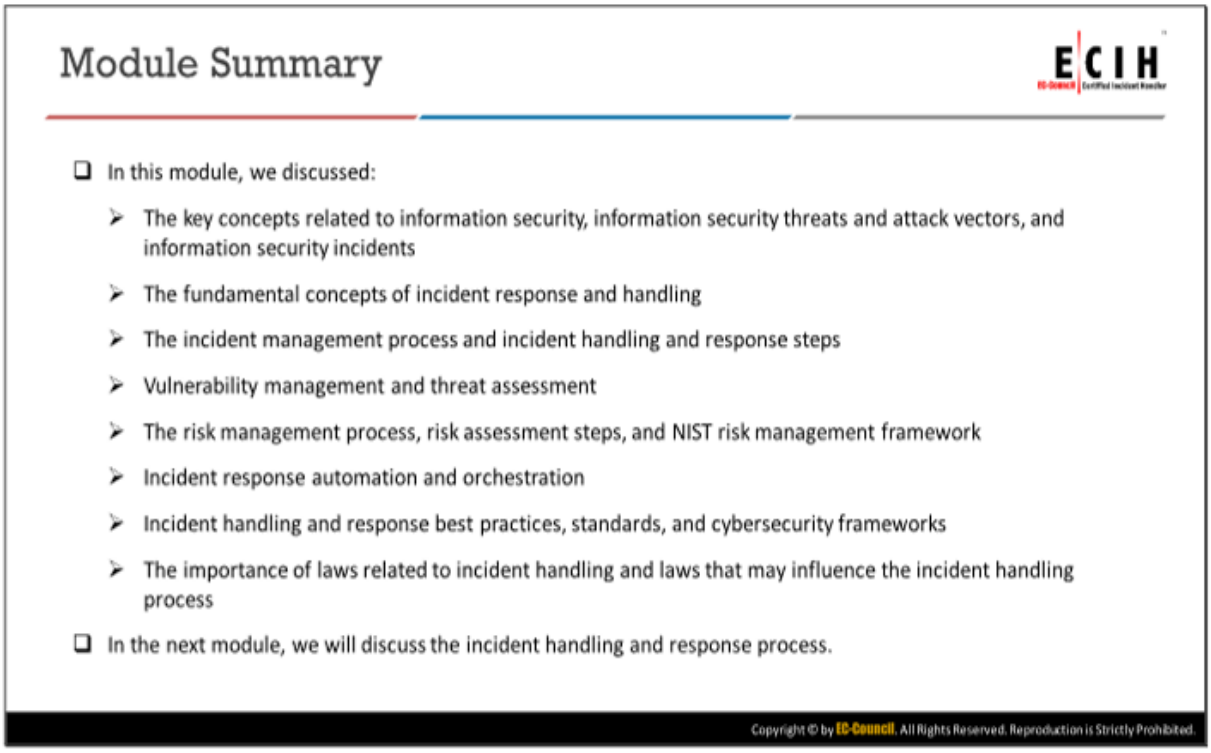
Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, etc. and Trademarks (Offenses And Enforcement) Act 2002	http://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Regulation of Investigatory Powers Act 2000	
	Police and Justice Act 2006	
	Criminal Justice Act 2008	
	Financial Services Act 2012	
	Protection of Children Act 1978	
China	Copyright Law of People's Republic of China (Amended on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amended on October 27, 2001)	http://samr.saic.gov.cn
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net



Cyber Laws That May Influence Incident Handling

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.

The tables shown on the above slides lists different cyber laws that may influence incident handling.



Module Summary

In this module, we have discussed key information security concepts, threats and attack vectors, and aspects of information security incidents, such as signs and cost. This module provides an overview of incident response and handling and discusses the incident management process and incident handling and response steps along with the advantages of incident handling and response. Besides discussing in detail vulnerability management and threat assessment, the risk management process, risk assessment steps, NIST risk management framework, and incident response automation and orchestration, it gave an overview of incident handling and response best practices, standards, and cybersecurity frameworks. This module ends with a discussion of the importance of laws in incident handling and the various laws that may influence the incident handling process.

In the next module, we will discuss in detail the incident handling and response process along with the various steps involved in the process.