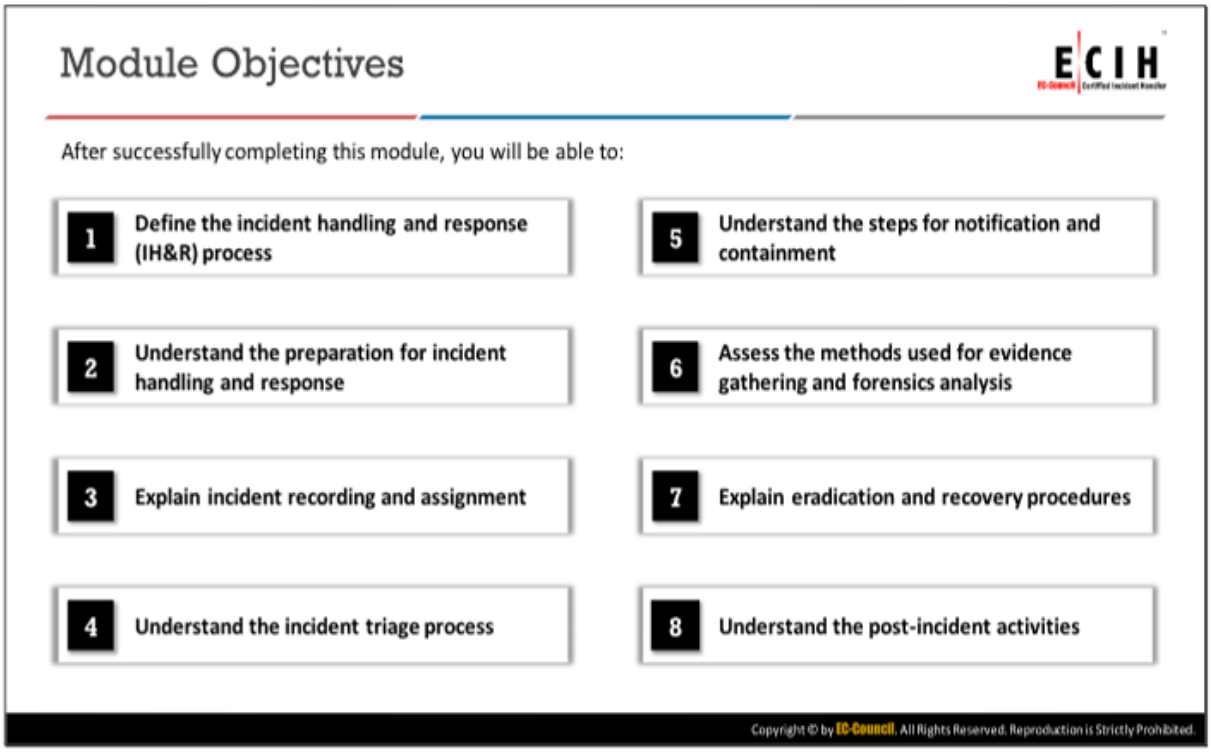
Module 02

Incident Handling and Response Process

This page is intentionally left blank.



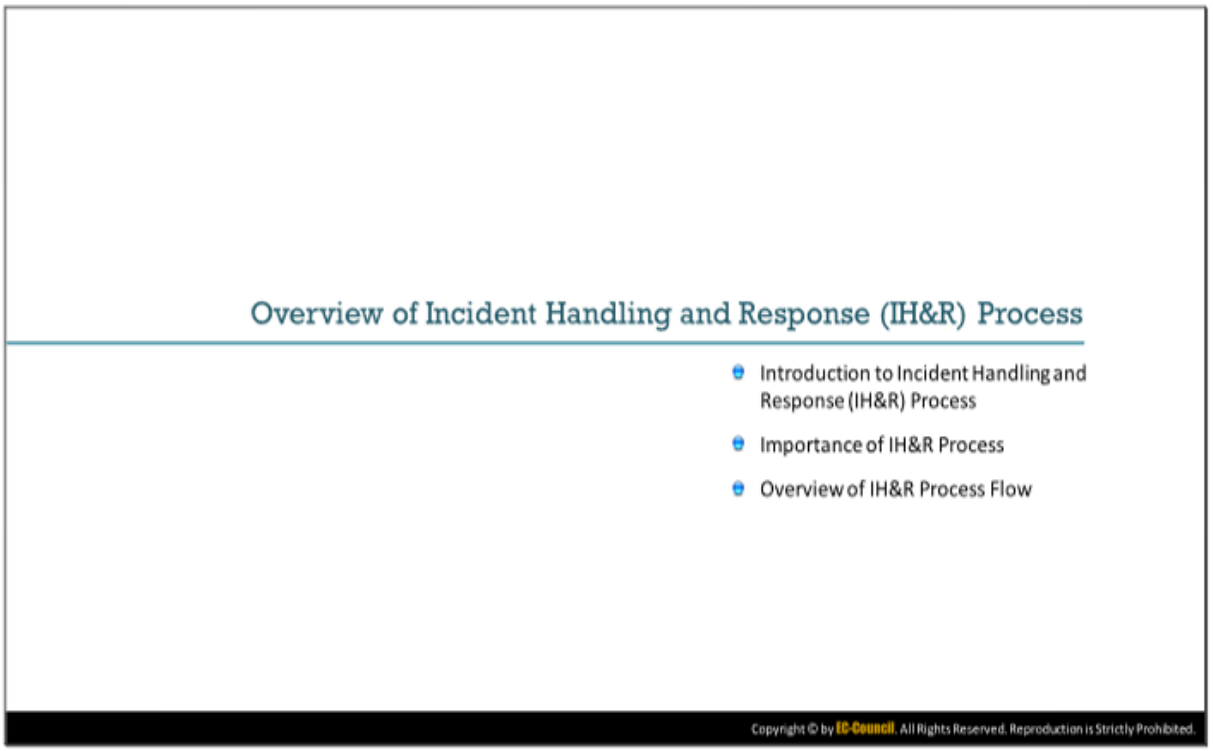
Module Objectives

Information security incidents have skyrocketed in recent years, owing to the adoption of digital technologies and the daily innovation of new technologies. In this environment, organizations are at risk of suffering huge losses related to data, trust, profits, systems, devices, and human resources. Therefore, it is crucial for organizations to be ready to battle—if not completely prevent—these incidents.

This module will help in understanding the complete incident handling and response process that organizations must institute to face, fight, and prevent different types of information-based attacks. This module also presents a framework that can be used to create a sound incident handling response for your organization.

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

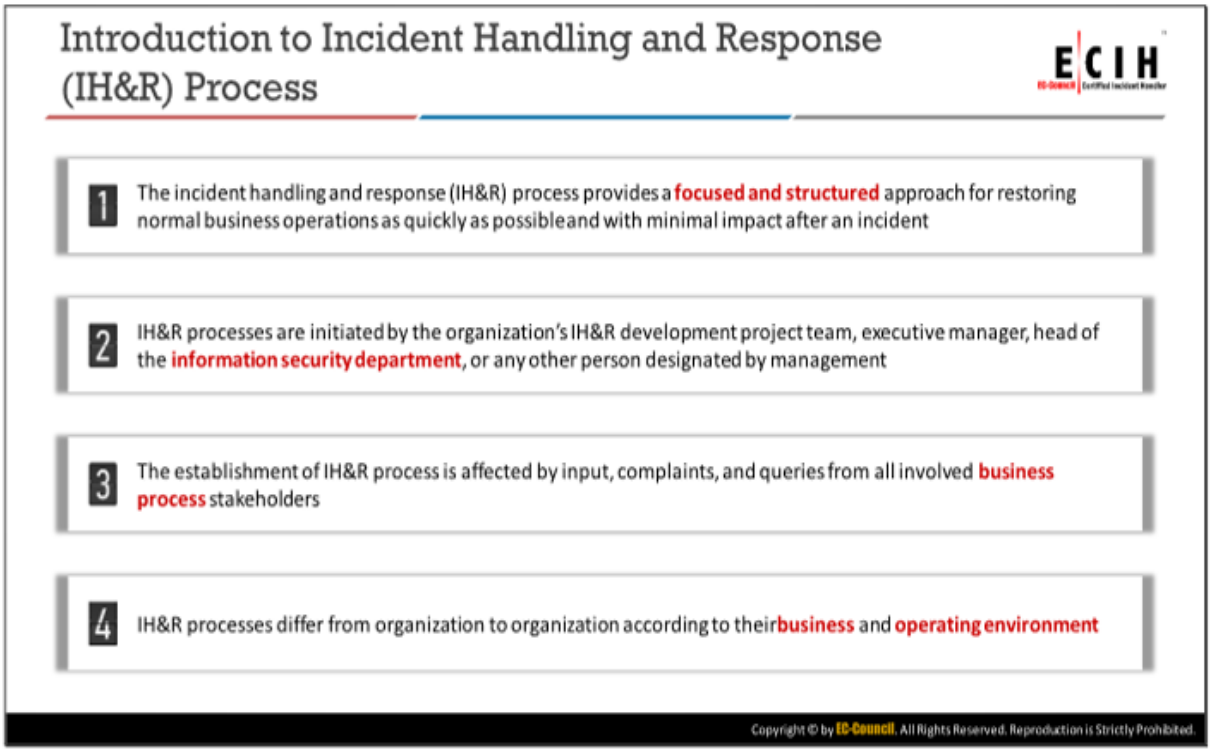
- Define the incident handling and response process
- Understand how to prepare for incident handling and response
- Explain incident recording and assignment
- Understand the incident triage process
- Understand the notification and containment steps of the process
- Assess different methods of evidence gathering and forensics analysis
- Explain the eradication and recovery procedures
- Understand post-incident activities



Overview of Incident Handling and Response (IH&R) Process

An "incident" refers to an event that disrupts the quality or productivity of a service or a system. An incident can be a computer threat, policy violation, or exploitation of a vulnerability that troubles the normal functioning of an information system. These violations can impact standard security practices, acceptable user policies, and computer security policies and can also result in security breaches. There are several different types of computer security incidents, such as improper usage, unauthorized access, malware attacks, and denial-of-service attacks.

"Incident handling and response" (IH&R) is the practice of managing the processes involved in responding to an incident—such as preparation, detection, containment, eradication, and recovery—to quickly and efficiently overcome the impact of an incident. This section introduces the IH&R process, including its importance and process flow.

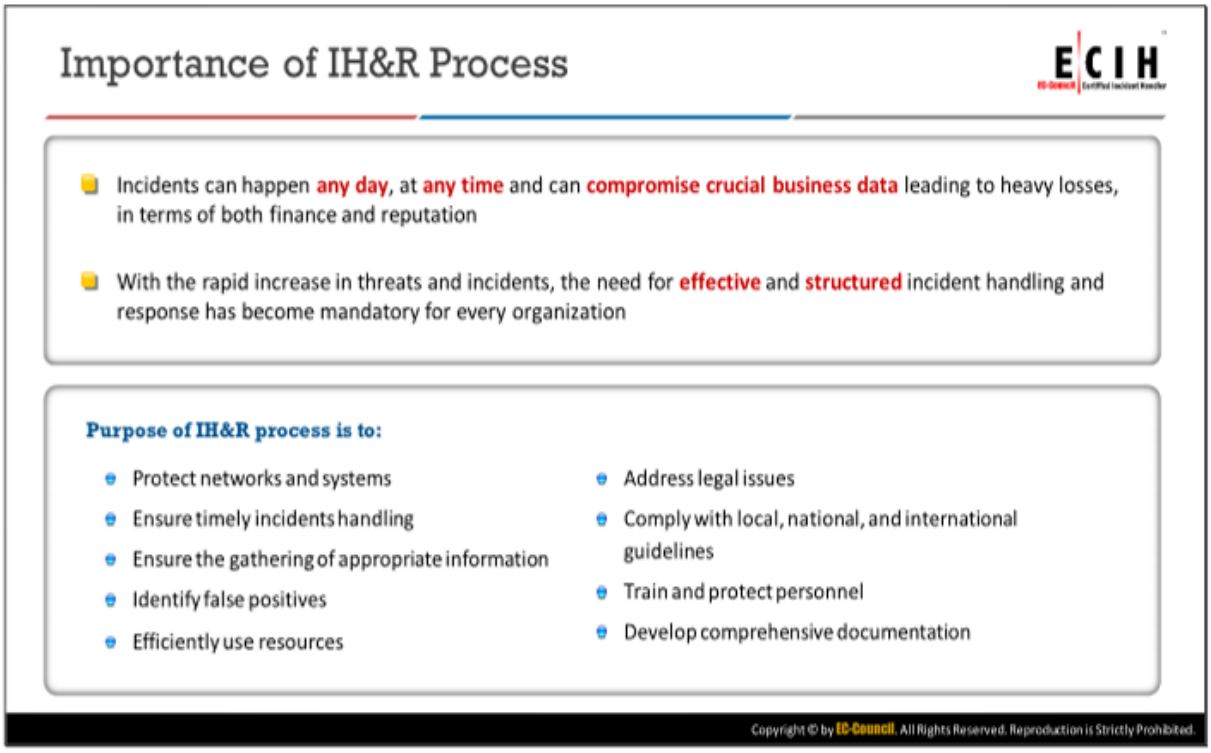


Introduction to Incident Handling and Response (IH&R) Process

The IH&R process involves uncovering an incident, the time at which it occurred, its impact, and its cause. The main objective of the IH&R process is to provide an organized, focused, and structured approach for combating security incidents, stop ongoing attacks, limit damage to the lowest possible level, keep services running, reduce recovery time, reduce costs, and deal with the aftermath of the incident. The process also helps incident examiners analyze the consequences of the incident and take appropriate measures to minimize damage and rapidly restore the disrupted sector.

Ultimately, then, IH&R processes facilitate a focused and structured approach to restoring normal business operations after an incident. For our purposes, it is important to note that the IH&R process involves defining user policies, developing protocols, building incident response (IR) teams, auditing organizational assets, planning IR procedures, getting management approvals, reporting incidents, prioritizing activities, and managing responses. Moreover, it also requires the establishment of proper communicative practices between responders as well as the establishment of guidelines to help responders detect, analyze, contain, recover from, and prevent incidents.

IH&R processes are initiated by an organization's IH&R Development Project Team, Executive Manager, Head of Information Security, and any other person exclusively designated by management. The decision to establish an IH&R process is affected by inputs, complaints, and queries from all stakeholders involved in an organization's business processes. To be sure, IH&R processes differ between organizations according to their business and operating environments.



Importance of IH&R Process

The exponentially rapid progress of technology for organizations has given rise to new technologies capable of serving diverse sectors. However, this technological diversity has notably intensified the frequency, diversity, severity, and approach of security threats, indicating the need for every organization to mandate effective and structured IH&R processes.

Incidents that can compromise crucial business data and cause heavy financial and reputational losses can happen on any day and at any time. To avoid such losses, organizations should prepare to efficiently handle any incidents.

Organizations therefore employ the IH&R process to:

- **Protect Networks and Systems**

  With technology continuously evolving, attackers are finding new ways to damage businesses. In such a scenario, it is difficult to completely secure systems and data even after instituting expensive high-level security features such as special access controls on various computing resources. The best strategy for securing computer systems and protecting networks is to quickly detect any indicators of compromise and recover from the security incident. An efficient IR procedure ensures the proper maintenance of all critical business operations during and after an incident.

- **Ensure Timely Incident Handling**

  During any incident situation, time is the most important factor: as time increases, damage increases. Therefore, IH&R processes should always encourage organizations to adopt various time management techniques and tools for detecting, validating, and containing incidents before it is too late.

- **Ensure the Gathering of Appropriate Information**

  The IH&R process ensures the gathering of appropriate and accurate information necessary for understanding a security incident, building an IH&R team from existing employees, clarifying standard security procedures, developing knowledge of required tools, and deploying the latest security measures to handle any future information security incidents.

- **Identify False Positives**

  Detecting an incident is an arduous process; however, it becomes even more difficult when it is necessary to identify false positives—even simple mistakes, such as application program errors, human errors, hardware failure errors, and system configuration errors, can generate alarms. IR processes crucially help organizations differentiate actual incidents from false alarms and advise best practices for handling both.

- **Efficiently Use Resources**

  The technical and managerial resources required for incident handling are often limited. The best way to use these resources is to respond to incidents as quickly as possible. Information gained during the incident handling process can help to prevent incidents or enhance an organization's ability to handle future incidents and implement strong security for systems and data.

- **Address Legal Issues**

  Organizations must abide by the laws of their jurisdictions when dealing with security incidents; otherwise, they may face legal issues. Sometimes, for example, incident handling requires the investigation of private information, and such processes can conflict with individual privacy rights—according to the U.S. Department of Justice, it is illegal for organizations to use certain monitoring techniques to identify an information security incident. To be sure, then, IH&R processes must comply with different laws and acts, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA). Moreover, IH&R processes should also be sure to advise incident responders to attain proper permissions and approvals from concerned authorities. In addition, IH&R processes may also define a strategy for identifying and prosecuting the perpetrators of security incidents. The key takeaway here is that aligning incident procedures with relevant laws fortifies an organization against legal and public liabilities.

- **Comply with Local, national, and International Guidelines**

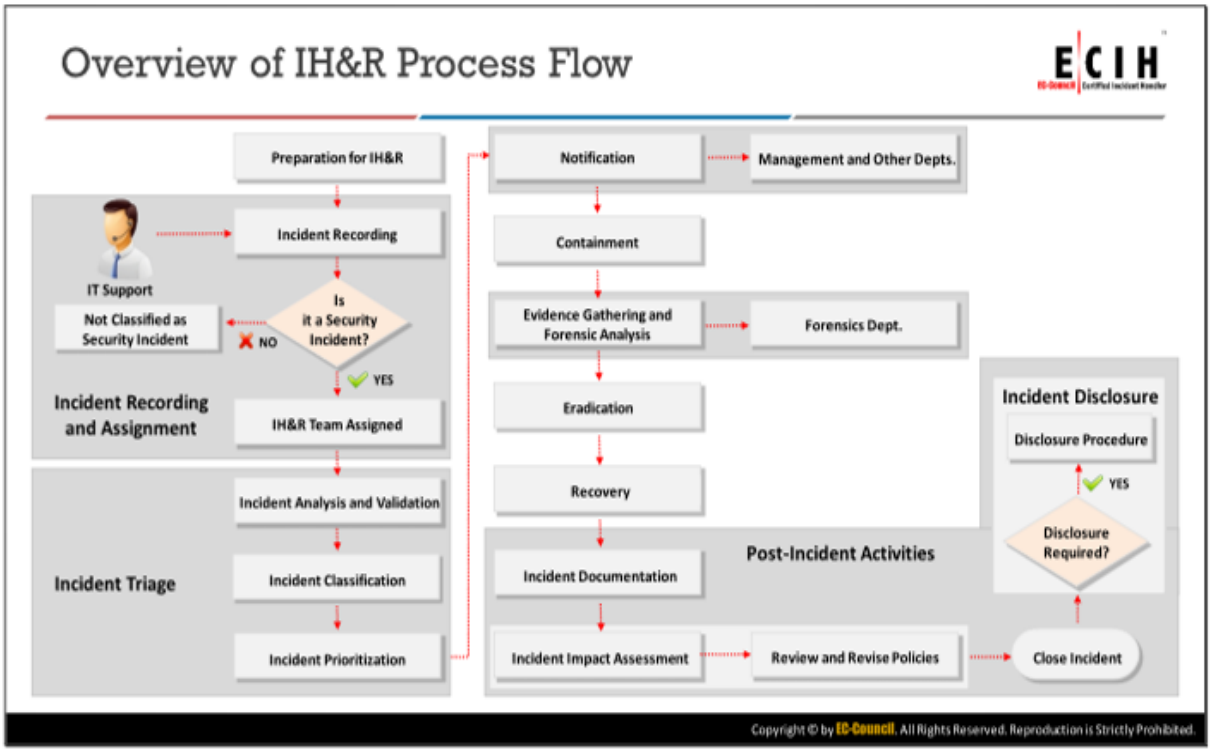
  An IH&R process can help an organization comply with local and international protocols, policies, control measures, and guidelines set by various Community Emergency Response Teams (CERTs), while at once enabling it to handle and recover from any type of information security incident.

- **Train and Protect Personnel**

  A good IH&R process requires an organization to build a good team capable of accelerating analysis, limiting damage to a minimal level, completely eradicating the incident, and restoring operations. This team will also help the organization learn from the incident and implement such knowledge to improve network safety. A swift IR helps to protect an organization's human resources from any physical consequences of a workplace incident.

- **Develop Comprehensive Documentation**

  IH&R processes must advise the documentation of the whole scenario starting from the alert generation to the identification of the best solution to the incident. This documentation will serve as a reference for analyzing the mistakes, threats, or vulnerabilities that paved the way for the incident and will thus offer insights helpful for future prevention, especially when they inform which advanced security measures may best prevent future attacks.



Overview of IH&R Process Flow

IH&R combines various cybersecurity processes under a single procedure for combating incidents, quickening responses, improving controls and management processes, easing communication, improving resource use, evenly distributing tasks, efficiently reporting incidents and responses, and so on. Incident handling is like fighting a war, but on the cyber front.

- **Step 1: Preparation for IH&R**

  The first phase of IH&R is to prepare to face the security issue(s). Preparation includes auditing the resources and assets to determine the purpose of the security response; defining the rules, policies, and procedures that drive the IH&R process; building and training an IR team; defining incident readiness procedures; gathering required tools; and training employees to secure their systems and accounts.

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

  The preparation phase is followed by an incident recording and assignment phase that involves the initial reporting and recording of the incident. This phase includes identifying the incident and defining a proper incident communication plan for employees—notably, this latter element can include normalizing communication methods that involve informing IT support personnel or raising an appropriate ticket. When a user or an employee reports any suspicious behavior on his or her system to IT support staff, a ticket or token is created about the irregular behavior and a member from the IR team is assigned to analyze the issue. Based on the ticket or the IT professional's intimation, the IH&R team will look into the issue and, if the issue qualifies as an incident, an IH&R team will be assigned to handle the incident, with the

compromised device sent to the IH&R team for further investigation. Otherwise, the issue will be considered resolved and the ticket will be closed.

- **Step 3: Incident Triage**

  In this phase, the incident will be analyzed, validated, categorized, and prioritized. The IH&R team will further analyze the compromised device to find incident details, such as the attack's type, severity, target, impact, and method of propagation as well as the vulnerabilities the attacker exploited. These details help the IH&R team to scale its impact and determine what other targets were involved in the incident, what techniques it must apply to contain the incident, and what it must prioritize to solve the incident.

- **Step 4: Notification**

  The notification phase involves the release of incident information to various stakeholders, including management, third-party vendors, and clients. The notification phase occurs as soon as the incident is confirmed and validated, with the incident handlers first communicating the issue to management to gain necessary approvals and permissions.

- **Step 5: Containment**

  The containment phase—which occurs at the same time as the notification phase—involves the IH&R team's containment of the incident. Crucially, the containment phase must be performed to stop the infection from spreading to other organizational assets. Along these lines, the important take away here is that the containment phase helps an organization stop a live attack from spreading and reduce damage and losses.

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

  The evidence gathering phase occurs after the containment phase and involves the IH&R team collecting evidence. In this phase, the team will accumulate all possible evidence related to an incident and submit it to the forensic department for investigation. Such evidence may include details related to the method of attack as well as the vulnerabilities exploited, security mechanisms averted, network devices infected, and applications compromised that may have acted as pathways in the attack. Collecting and analyzing this information helps the IH&R team to block propagation methods to eradicate the incident and prevent it from reoccurring in the future.

- **Step 7: Eradication**

  The eradication phase involves the IH&R team removing or eliminating the root cause of an incident and closing all attack vectors to prevent similar incidents in future. Eradication methods may include patching vulnerabilities, replacing malfunctioning devices, and installing better security mechanisms, including those that scan for malware signatures.

- **Step 8: Recovery**

  After eliminating the causes of an incident, the IH&R team is responsible for restoring the affected systems, services, resources, and data through a recovery process. It is the

responsibility of the IR team to ensure—to the extent possible—that the incident does not disrupt the organization's operations. Therefore, the IH&R team may need to recover compromised devices, applications, systems, or terminals as soon as possible by either replacing them or quickly fixing the issue.

- **Step 9: Post-Incident Activities**

  This stage occurs only after the incident has been contained and the systems recovered. All tasks performed by IH&R personnel after this stage—such as incident documentation, incident impact analysis, policy review and revision, and incident disclosure—qualify as "post-incident activities."

  - **Incident Documentation**

    Incident responders must document the complete IH&R process from detection to recovery. Such documentation will serve as a future reference to facilitate understanding of the practices employed to handle the incident. Notably, handlers should present the report to legal counsel; submit it to management; and use it to assess loss, review policies, change security norms, and reframe user protocols to improve network security.

  - **Incident Impact Assessment**

    After completing the formal IH&R process from incident recording through documentation, the IH&R team will analyze all information available to perform an incident impact analysis that assesses the impact of the damages or losses the organization suffered as a result of the incident.

  - **Policy Review and Revision**

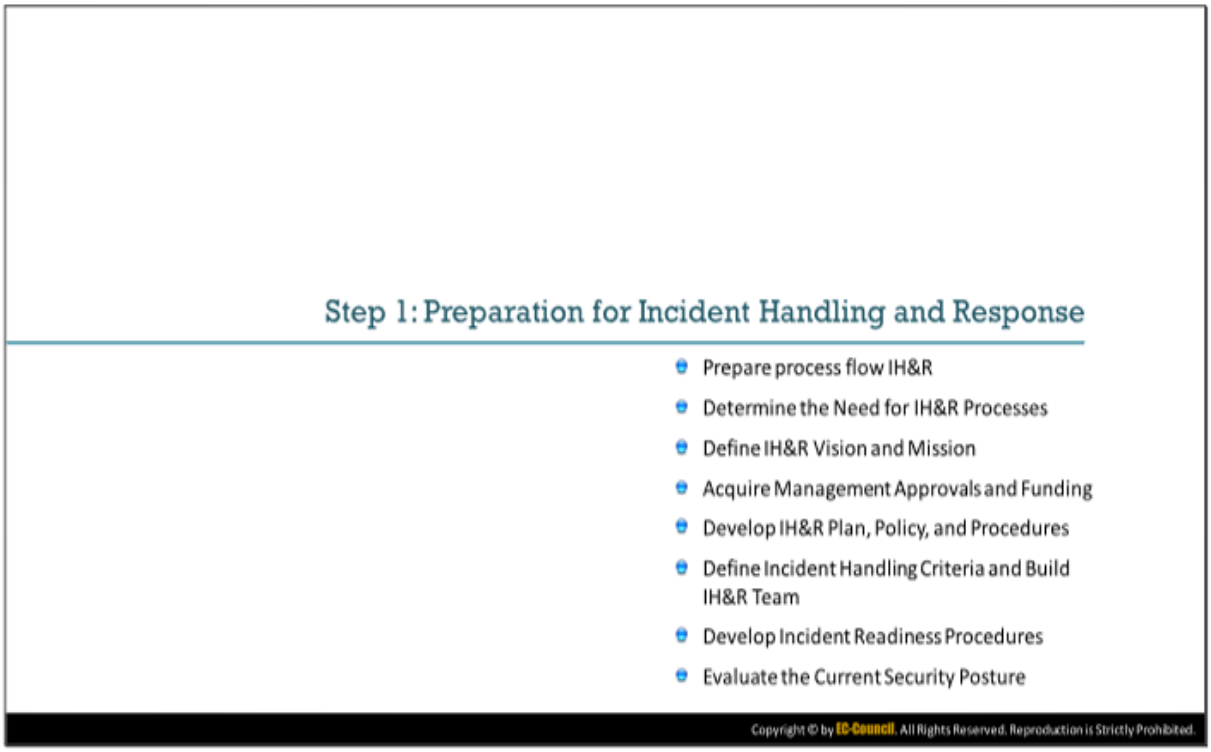
    After assessing the incident's impact, the IH&R team will review and revise the organization's policies, preparation and protection procedures, and security controls to prevent future incidents. They will also share the identified threat information with threat intelligence teams.

  - **Closing the Investigation**

    By this phase, the incident will have been thoroughly investigated and documented and appropriate policies will have been reviewed and revised. This phase involves the official termination of the investigation and the planning of the implementation of the incident evidence retention policy.

  - **Incident Disclosure**

    After formally closing the incident, the organization's IH&R team and management will discuss whether to disclose the incident's details to the public (e.g., customers, media, industry intelligence). Additionally, the incident handlers are also responsible for communicating the issue to other departments in the organization (e.g., legal, human resources, forensics).

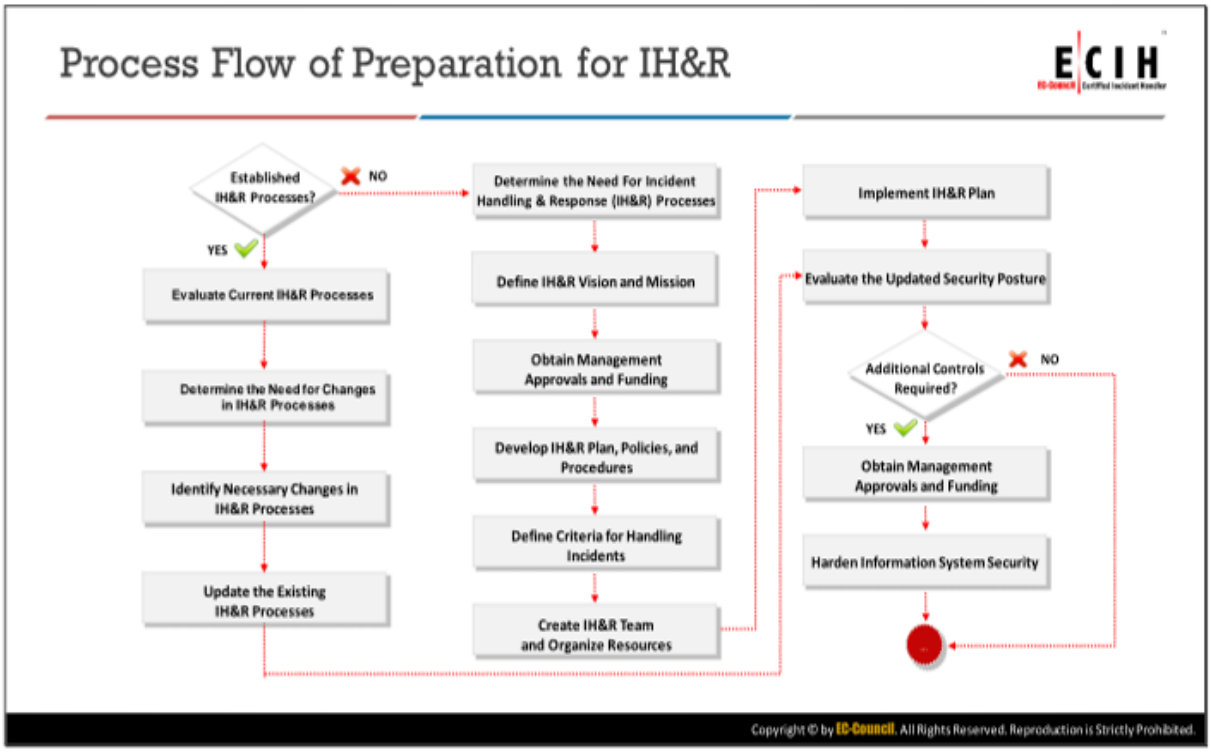


Step 1: Preparation for Incident Handling and Response

Preparation is the first and most important phase in the incident handling process; it enables an organization to establish an efficient IR process. In this stage, the organization will assess its assets, organizational structure, security policies, services, requirements for incident procedures, and other crucial elements of incident handling. Crucially, this stage enables organizations to take precautionary measures before an incident occurs; thus, the success of an IR process depends on the preparation phase.

In this stage, the organization will define the mission, vision, and scope of IH&R; obtain management approvals and funding; develop and implement security policies; build an IR team (a team of experts capable of handling any computer security incidents); gather systems, hardware, and software tools required for IR; prioritize assets and services; and create a plan for smooth communication during the incident.

This section discusses about various concepts involved in preparation for IH&R including defining vision, mission, and scope; developing the IH&R project plan, project management and time management, policies and procedures; building and training IH&R teams; and evaluating the current security posture of an organization.



Process Flow of Preparation for IH&R

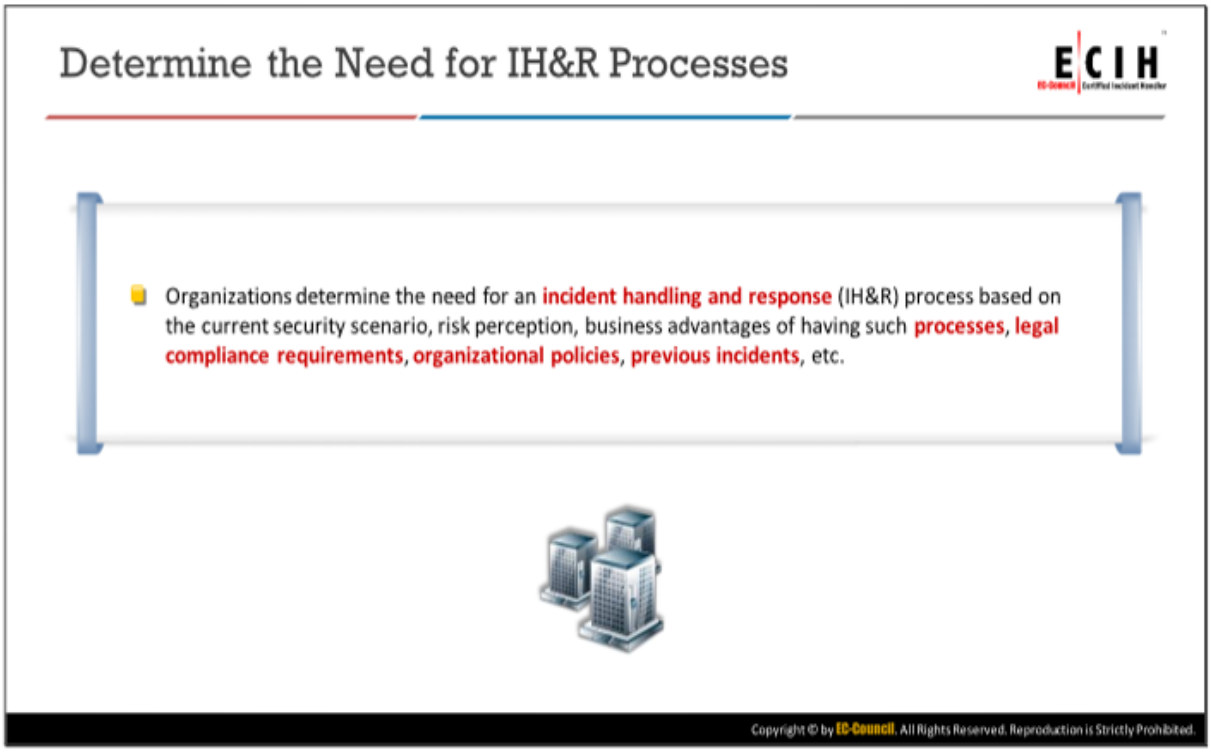
Preparing for an incident is always a precautionary measure that provides organizations, at the very least, with a defense mechanism, even against a zero-day attack. A state of preparedness is always advisable to limit damage in cases of intrusion, security breaches, or data breaches.

Preparation involves preparing guidelines for employees as a contingency plan in case of an attack. Preparation and planning can eliminate the ambiguity often faced during the peak hours of an attack and help in finding an appropriate response. Moreover, sometimes dry runs and mock drills can help spotlight loopholes in the network by highlighting different ways of penetrating an organization's information systems.

To be sure, proper permission is required before initiating IR processes, as this process includes gathering all parts of information, both personal and professional, from a victim's devices in an organization that led to the breach of privacy—of course, such work will always have legal implications. Therefore, incident handlers should be sure to align with regulations in ways that allow them to handle devices and data during an incident or in ways that can help their organization avoid an incident. Moreover, organizations should also develop fair usage policies for all employees.

It is important to note that adequate preparation will yield financial and safety benefits for an organization. For example, clients are more interested in doing business with an organization that can efficiently handle an incident. Preparation will also help an organization develop a documentation and reporting procedure; process for investigating an attack; policies and procedures for backup and recovery processes; training programs to make staff and users aware of incidents and reporting processes; and training for the IR team in successful forensics, investigations, and remediation.

The process flow for the preparation phase is detailed in the figure shown on the above slide.

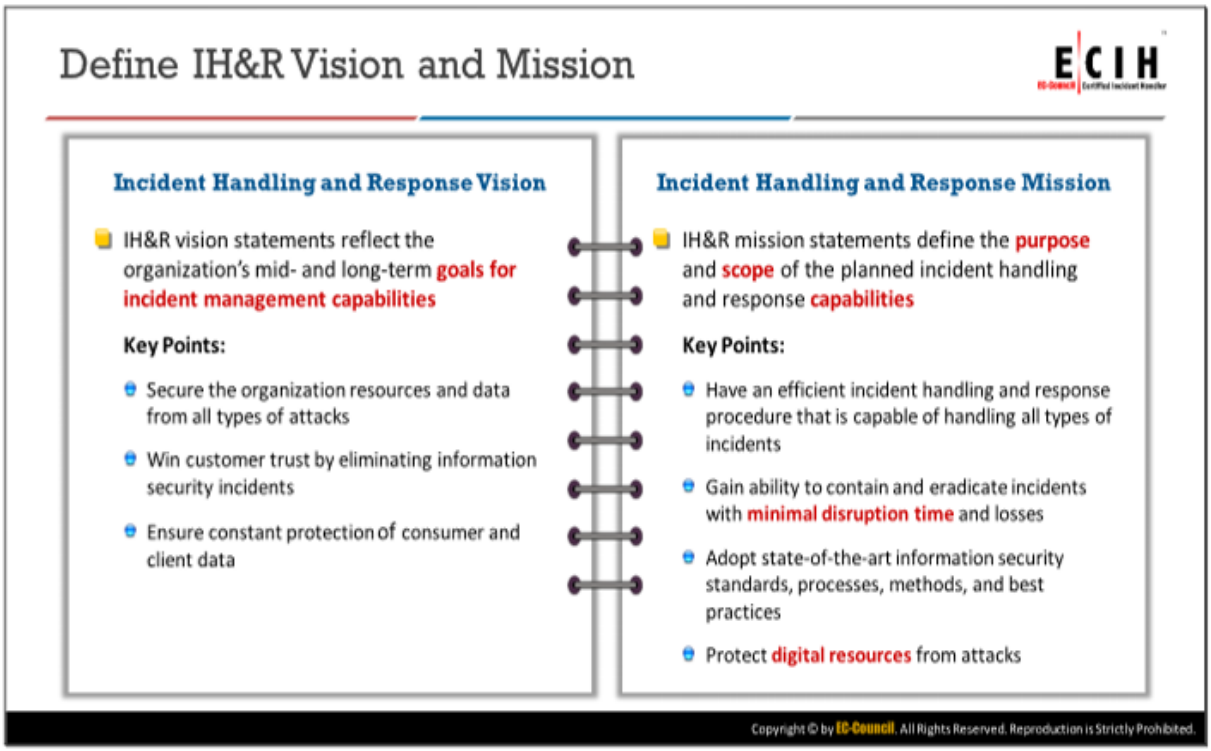


Determine the Need for IH&R Processes

An organization determines its need for an IH&R process based on its current security scenario, risk perception, legal compliance requirements, organizational policies, and previous incidents as well as the business advantages of having such processes. Factors impacting the IH&R process plan include the types of the organization's assets, services, storage devices, servers, and networking devices.

Inputs, complaints, approvals, permissions, and queries from all the stakeholders involved in the organization's business processes along with standard protocols, policies, local, and regional laws influence the establishment of the IH&R process. An organization's IH&R Development Project Team, Executive Manager, Head of Information Security, and any other person exclusively designated by management may initiate the IH&R processes.

If the organization already has an established IH&R process, then determine the ability of the process to stop and handle the incidents. More specifically, determine the flaws and drawbacks of the process and suggest changes to it depending on the above-mentioned dynamics. Update the existing IH&R process according to the recommended changes and report the new policies to stakeholders, management, network and system administrators, employees, clients, and customers.



Define IH&R Vision and Mission

Any organization, whether big or small, will have to design an IH&R process to serve its particular purposes. To perfect its IH&R process, an organization should create an IH&R vision and mission.

An IH&R vision statement reflects an organization's mid-term and long-term goals for its incident management capabilities. Put differently, an IH&R vision is a measured plan that defines the requirements, scope, and purpose of an IH&R process after evaluating the assets, devices, and data it must secure. To determine an optimal IH&R process for their organization, incident handlers need to audit all relevant systems, devices, networks, storage media, applications, policies, protocols, services, previous attacks, and other business aspects.

Meanwhile, an IH&R mission statement defines the purpose and scope of an organization's planned IH&R capabilities.

The key elements in an IH&R mission statement include:

- What IH&R capability is it aiming to protect?
- What are the short- and long-term goals of the IH&R team?
- What services will the IR team offer?
- How will the organization's IH&R capabilities ensure business continuity?
- What resources are required and how can their cost be justified with an effective return on investment?

The assessment will help in understanding the attacks, vulnerabilities, attack methodologies, and threats to which an organization is susceptible. After appropriate approvals, a detailed

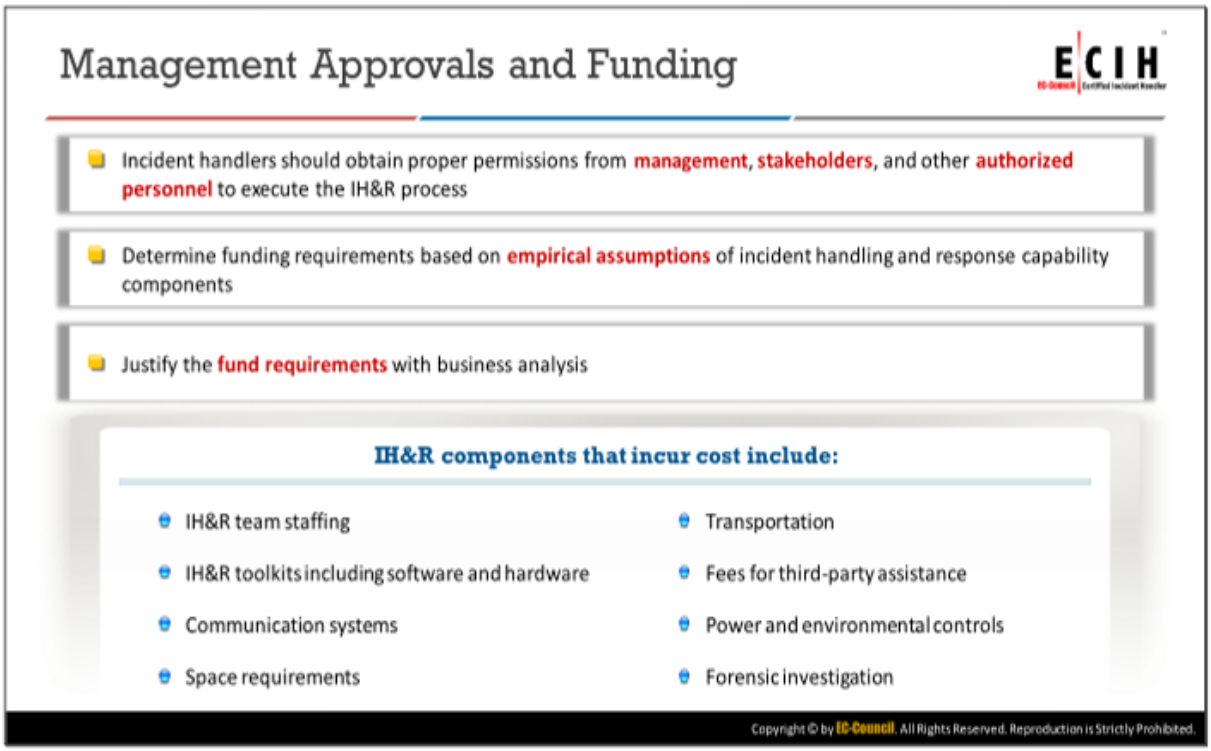
report of the vision and mission statements should be communicated to all stakeholders with supporting documents and should be published in easily accessible repository.

IH&R Vision

An organization's IH&R vision outlines how the organization plans to secure itself against all types of incidents to prevent business disruption and information loss. It also details how the organization seeks to win customer trust by implementing processes to eliminate information security hiccups to minimize the loss of life and property, prevent the occurrence of such incidents in future, and swiftly recover from security incidents. Ultimately, the organization's vision reflects its sense of how its IH&R process will ensure the safety of consumer and client data.

IH&R Mission

An organization's IH&R mission establishes its desire to have an efficient IH&R procedure capable of handling all types of incidents. Crucially, organizations often seek to gain the ability to quickly and efficiently overcome the impact of an incident with minimal disruption time and losses by performing all IR processes, such as preparation, detection, containment, eradication, and recovery. Along these lines, organizations strive to adopt state-of-the-art information security standards, processes, methods, and best practices to improve and update their IH&R processes to protect their digital resources, such as databases, network devices, and sensitive information, from attacks.



Management Approvals and Funding

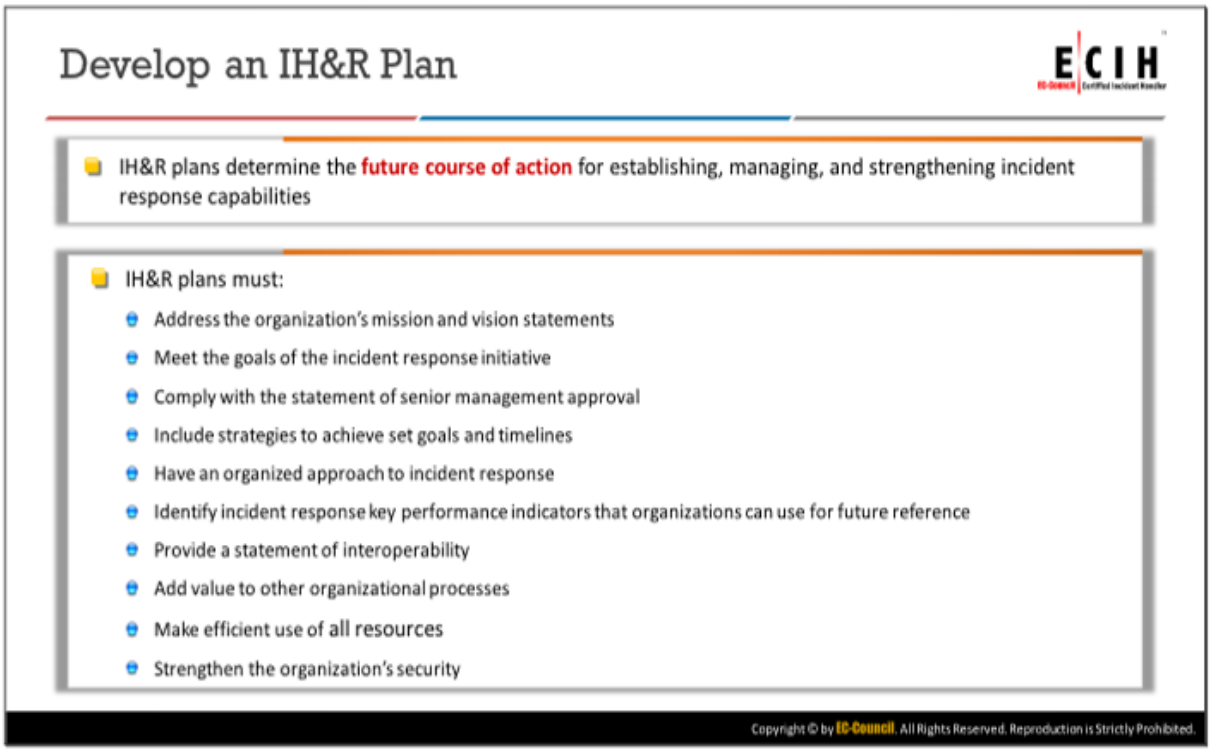
IH&R involves various tasks that require access to sensitive information and that can hinder the business functionality. Therefore, incident handlers should obtain proper permissions from management, stakeholders, and other authorized personnel to perform the IH&R process. More specifically, the IH&R process may require approvals related to using resources, analyzing data, disabling certain services, modifying authentication details, removing privileges, and disabling accounts. Incident handlers need to enlist all processes that require approvals, assign the task of seeking the proper approvals to an IH&R team member, and ensure that the approval is in a proper format.

Moreover, incident handlers need to assess the funding required for their process based on empirical assumptions about various components related to IH&R capability. Next, they must obtain management's approval for such a funding scheme by preparing a detailed document about the funding requirements and justifying their necessity with business analysis.

IH&R components that incur costs include:

- IH&R team staff, including full-time and part-time employees and a third-party IR service team that comes to the rescue when an event occurs. Related costs are incurred for recruitment, training, salaries, and so on.
- IH&R toolkits, including software and hardware components that help the team efficiently execute tasks. The expenses for creating toolkits include purchasing costs, updating costs, maintenance costs, upgrade costs, and replacement costs.
- Communication systems required during the IH&R process, including mobile phones, landlines, incident reporting mechanisms, encryption software, and issue tracking systems, along with their related service and maintenance charges.

- Environmental needs for IH&R team staff, including physical security, CCTV cameras, storage facility, air conditioning, lighting, and access.
- Transportation, including expenses related to moving evidence, storing media, team members, and other equipment to and from the incident site.
- Third-party assistance with the incident—this is only required sometimes, and the necessity is often short-lived. These expenses include the third-party assistance fee.
- Power controls, including transformers, generators, UPS, and other power supply equipment required to maintain a healthy power supply throughout the IH&R process (this is a basic requirement).
- Forensic investigation, that is, the process of finding the method of attack, finding the perpetrator, collecting evidence, proving the perpetrator is at fault, and attaining proper legal justice from a court of law. These tasks all require additional effort, a forensics team, tools, a legal team, equipment, and the use of a facility. When articulating these costs in a funding scheme for management, be sure to compare the cost of hiring an external forensics team against that of creating an internal forensics team to allow management decide their preference.
- Insurance, that is, the cost of the insurance policies the organization requires to protect itself against possible incidents.

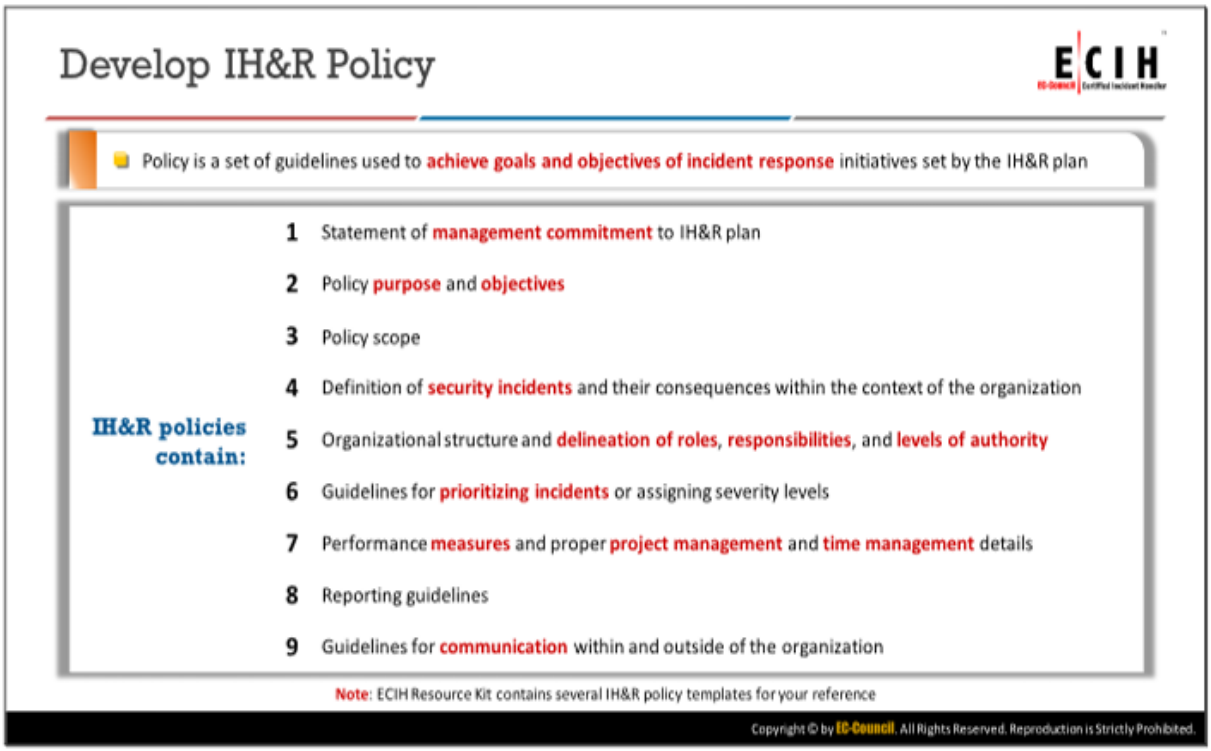


Develop an IH&R Plan

An IH&R plan refers to a set of instructions the IR team needs to follow to minimize the damage caused by an incident, efficiently use resources, and reduce its response duration. Incident handlers should associate with an organization's security personnel and management to develop a proficient IH&R plan that determines a future course of action for establishing, managing, and strengthening IR capabilities.

An IH&R plan must:

- Address the IH&R mission and vision statements
- Meet the goals of the IR initiative
- Comply with senior management's approval statement
- Include strategies to achieve set goals and timelines
- Have an organized approach to IR
- Identify key IR performance indicators that the organization can use for future reference
- Provide a statement of interoperability
- Add value to other organizational processes
- Make efficient use of all resources
- Strengthen the organization's security



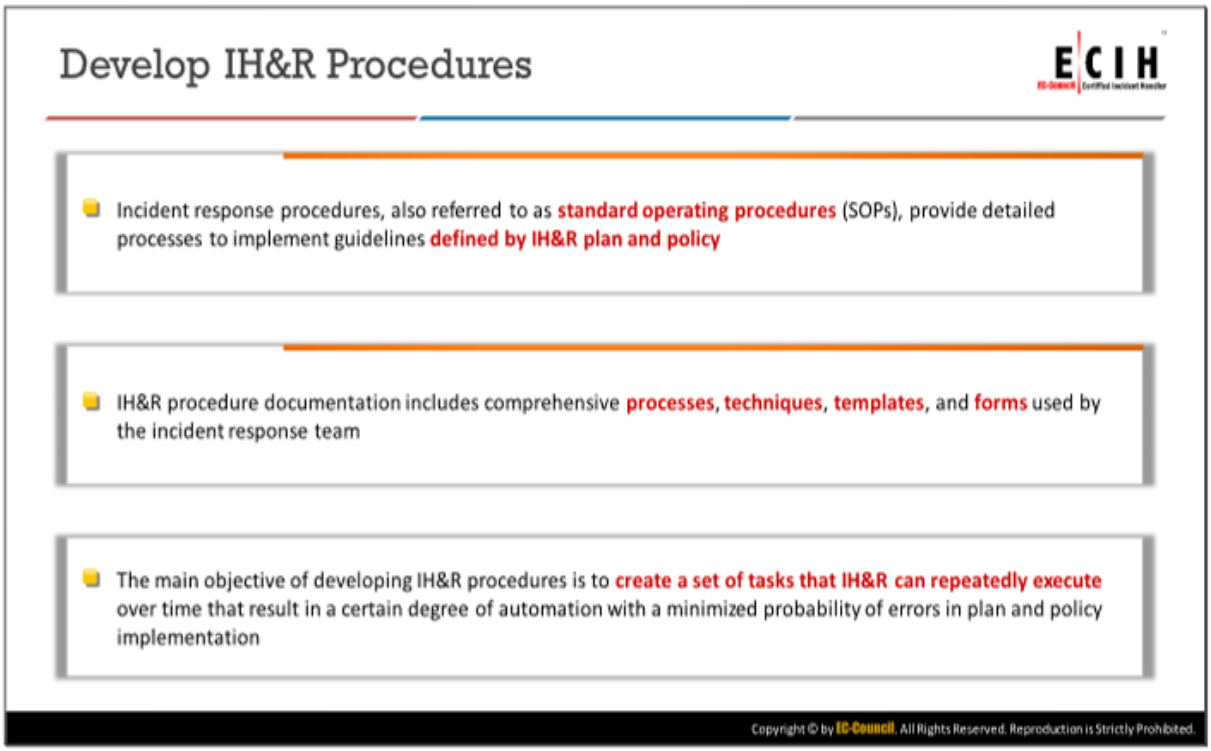
Develop IH&R Policy

An IH&R policy is a set of guidelines used to achieve the goals and objectives of the IR initiative set by the IH&R plan.

IH&R policies must contain the following:

- A statement of management's commitment to the IH&R plan, including the organization's IH&R vision and mission statements, which will help in understanding the organization's rationale for creating its IH&R procedure
- Purpose and objectives of the policy, such as the goals of its IR
- Scope of the policy, including the resources, regions, offices, and departments that the IH&R policy covers
- A definition of computer security incidents and a sense of their consequences within the context of the organization
- Delineations of the organization's structure, including the roles, responsibilities, and levels of authority within it
- Guidelines for prioritization or the assignment of severity levels
- Performance measures and proper project management and time management details
- Reporting guidelines, including the preferred formatting of reports and the persons to whom the response team must report
- Guidelines for communication within and outside of the organization

Note: The ECIH Resource Kit contains several IH&R policy templates for your reference.

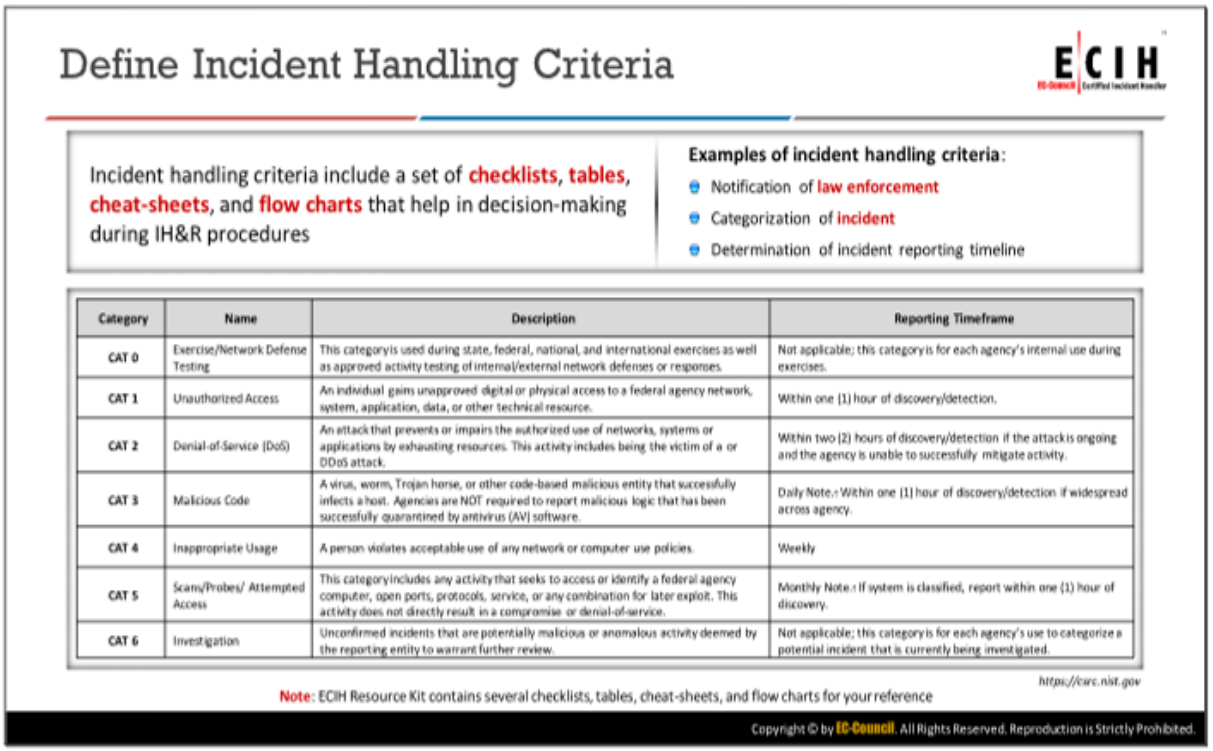


Develop IH&R Procedures

IH&R procedures, also referred to as standard operating procedures (SOPs), provide detailed step-by-step processes for implementing an IH&R plan and policy. The procedure discusses the roles and responsibilities of the incident handling team in the event of an attack to avoid confusion, minimize damages, and reduce response time.

The procedure should include the implementation of a complete IH&R process lifecycle, including detection, containment, eradication, and reporting. It should also detail the process of performing each task; the techniques involved; the tools required, the persons to contact in case of emergency; the authorities who can provide approvals; instructions for documenting the process, preserving evidence, and reporting the process; and best approaches for the usage of different templates and forms available to the IR team for reporting an incident.

The main objective of developing IH&R procedures is to create a set of tasks that IH&R can repeatedly execute with a certain degree of automation to minimize the probability of errors in plan and policy implementation.



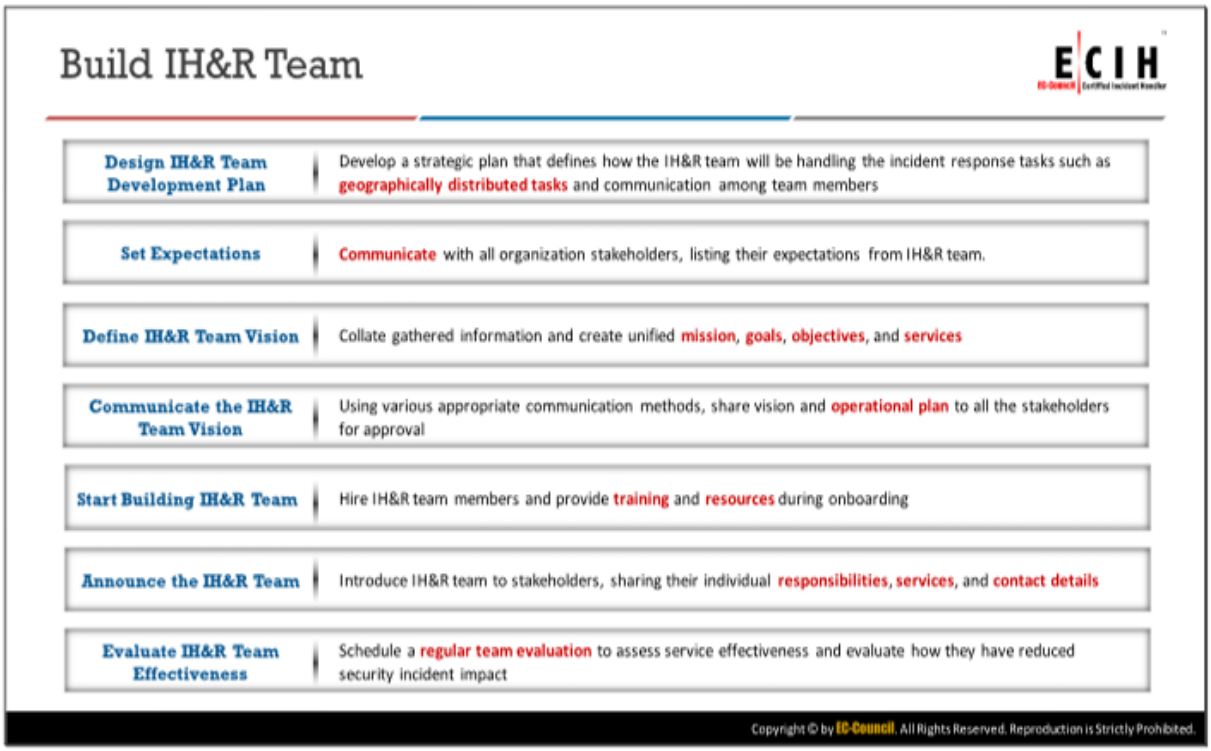
Define Incident Handling Criteria

Incident handling criteria include checklists, tables, cheat-sheets, and flow charts that facilitate decision-making during IH&R procedures. The table from NIST, as shown on the above slide, categorizes incidents based on their type, description, and reporting duration.

Incident handlers and responders must define incident handling criteria based on the organization's requirements, the type of incident, the incident's impact, and any business disruptions. Examples of incident handling criteria include:

- Criteria for notifying law enforcement
- Criteria for incident categorization
- Criteria for determining incident reporting time
- Criteria for taking appropriate actions while handling incidents
- Criteria to prevent evidence corruption

Note: The ECIH Resource Kit contains several checklists, tables, cheat-sheets, and flow charts for your reference.



Build IH&R Team

An IH&R team is a group of technically skilled people capable of carrying out various functions, such as threat intelligence, evidence analysis, and user investigations. Having a trained IH&R team in an organization reduces not only the losses caused by incidents, but also response time the probability of similar attacks occurring in the future.

A centralized IH&R team managed by an incident handler will perform vulnerability analysis, establish well-defined security policies, detect indicators of compromise, handle legal issues, manage public relations, and provide proper reports regarding the incident.

Incident handlers should perform the following tasks to build an IH&R team:

- **Design an IH&R Team Development Plan**

  Clearly mention the skills and expertise the IH&R team should have to perform IR tasks and the processes involved in recruitment, training, and deployment. The IH&R team strategy planning phase helps in dealing with administrative and management issues—if not managed properly, the IH&R team will fail. Thus, it is important to develop a strategic plan that details for the IH&R team the best practices for handling IR tasks, such as geographically distributed tasks and communication among the team members.

- **Set Expectations**

  Communicate with all the stakeholders of the organization and create a list of their expectations for the IH&R team—this will inform the setting of expectations for the IH&R team. Clearly define the roles and responsibilities of the IH&R team, ensuring that they comply with the security policies and standards of the organization. The best way to inform the organization of the IH&R team's duties is by sending a memorandum from the CIO, CEO, or other top-level manager to all stakeholders with information about the

development of the IH&R project. This will help stakeholders feel like they are a part of the design process and can contribute to the project.

- **Define an IH&R Team Vision**

  Incident handlers should always convey the IH&R team's mission, goals, objectives, services, and constituency to its members and ensure that the IH&R team is able to achieve its goals (e.g., the IH&R stages of preparation, detection, containment, and eradication) in as short a duration as possible. Along these lines, incident handlers should also ensure that tasks are properly allocated to team members in accordance with their styles of experience and expertise.

- **Communicate the IH&R Team Vision**

  Communicating the vision beforehand can ease the identification process and assist in determining organizational problems before implementing the IH&R process. Along these lines, this approach allows people to understand any developments in the plan and facilitate their ability to give feedback that can help in making any final modifications to the IH&R team's organizational structure and processes. Moreover, this process can reduce errors during the evidence gathering process.

- **Start Building an IH&R Team**

  Incident handlers may build an IH&R team using current employees with the required skills as well as by recruiting new ones. To be sure, they must gather the required tools and systems and provide proper training to all team members, including the use practice sessions and mock IR drills to check team efficiency.

  Building an IH&R team involves the following tasks:

  - Appointing the preliminary IH&R team and training team members
  - Developing the network infrastructure by purchasing equipment to support the team
  - Developing the IH&R team policies and procedures necessary to support its mandatory services
  - Identifying the specifications required to develop an incident tracking system
  - Developing incident reporting forms and guidelines for the constituency

- **Announce the IH&R Team**

  Inform stakeholders, management, and other employees about the members of the IH&R team; their responsibilities, services, contact details and processes, hours of operation, and methods of operation; and the availability of the incident reporting guidelines. Moreover, it is also crucial at this stage to acquire the proper permissions necessary for the team to work on sensitive organizational data. Consider distributing brochures and using open house to announce the operational IH&R team.

- **Evaluate the IH&R Team's Effectiveness**

  Regularly conduct tests and mock drill sessions with the team to evaluate its effectiveness, that is, to analyze the ability of the IR team to handle security incidents, including their speed of and success at protecting organizational assets.

  Various mechanisms for calculating IH&R team efficiency include:

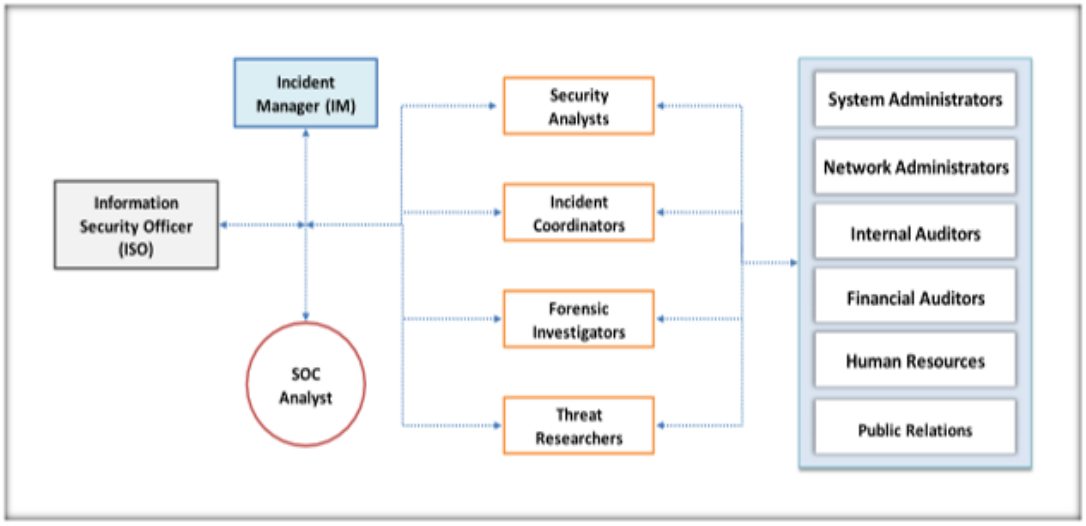
  - Comparison with other benchmarked IH&R teams
  - Conducting discussions with representatives of a constituency
  - Surveying constituency members on a periodic basis
  - Evaluating the team based on third-party criteria or an audit

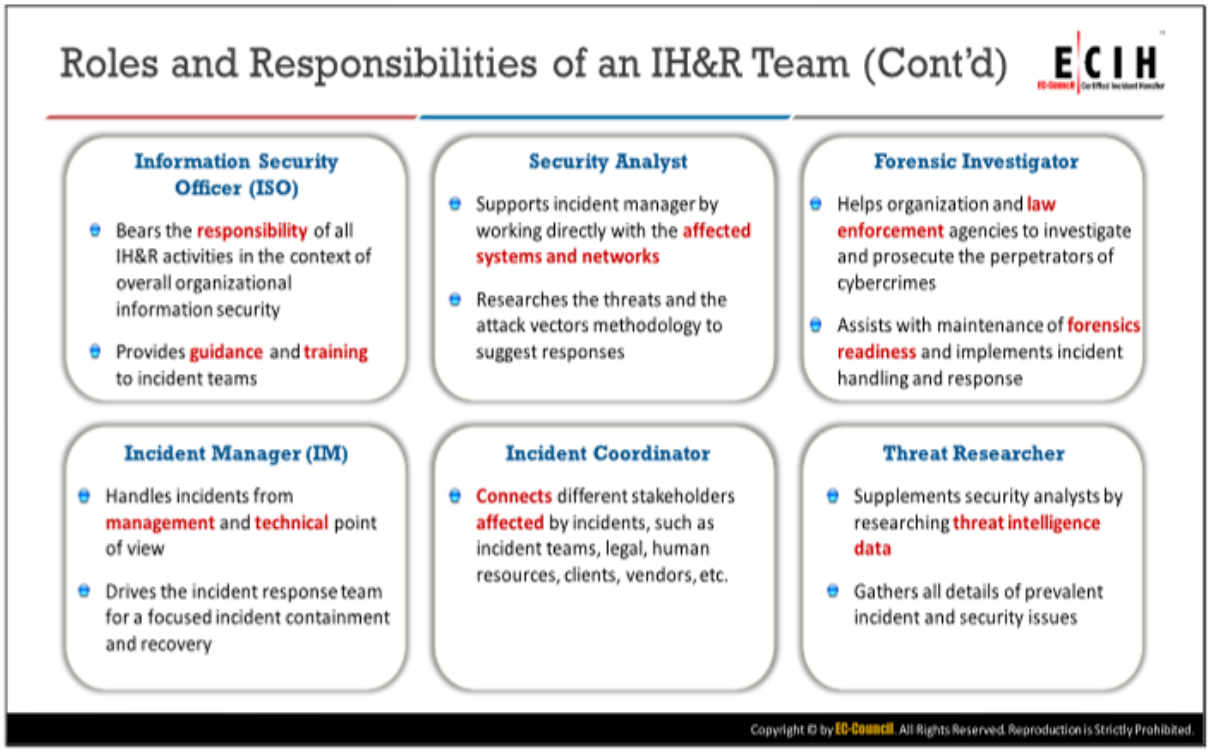
  In reviewing information gathered during an evaluation, it is important to note that it can serve as a baseline for planning the IR process.

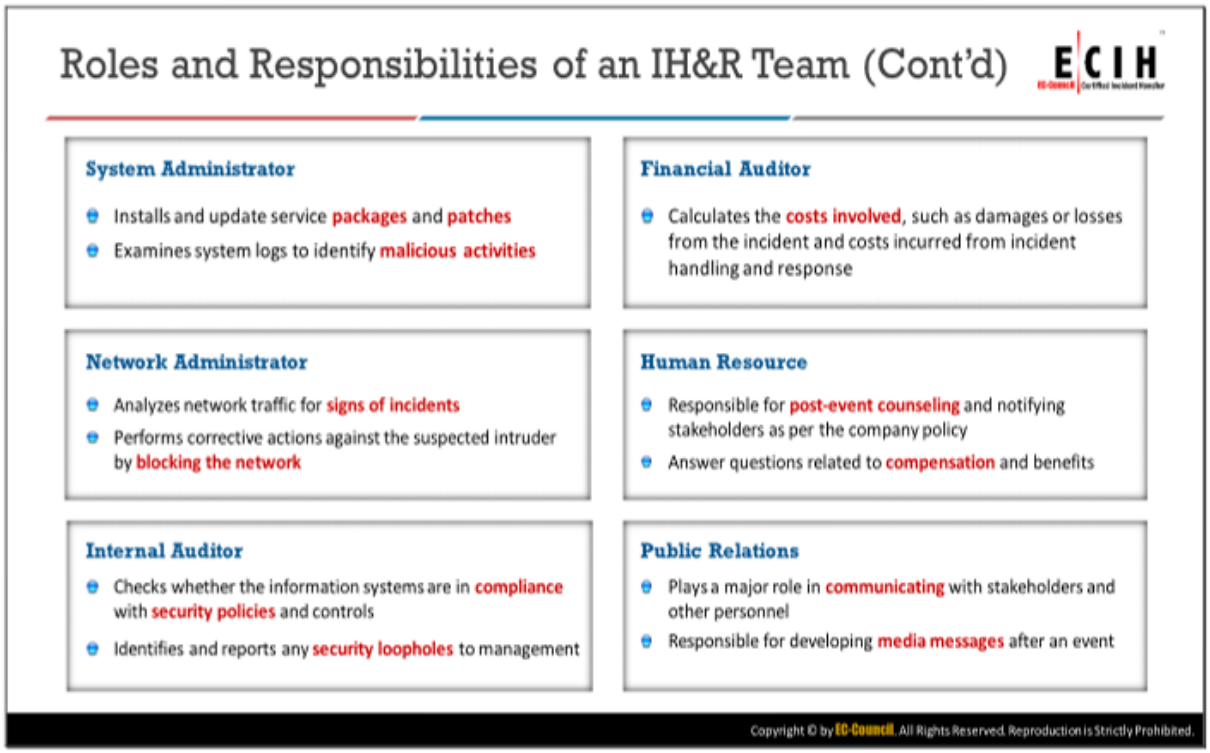
Roles and Responsibilities of an IH&R Team

- Manage security issues by taking a **proactive approach** toward security vulnerabilities and responding effectively to potential information security incidents
- **Develop** and **review** the processes and procedures that must be followed in response to an incident
- Manage the incident response and ensure that all procedures are followed correctly in order to **minimize and control the damage**
- Identify and analyze **what has happened** during an incident, including the impact and threat
- Review changes in **legal and regulatory requirements** to ensure that all processes and procedures are up-to-date
- Review **existing controls** and recommend steps and technology to prevent future **security incidents**
- **Establish relationships** with local law enforcement agencies, government agencies, key partners, and suppliers

Roles and Responsibilities of an IH&R Team (Cont'd)







Roles and Responsibilities of an IH&R Team

An IH&R team must manage security issues by taking a proactive approach toward security vulnerabilities and by responding effectively to potential information security incidents. As noted above, the team should develop and review the processes and procedures it must follow in response to an incident, must manage its response to an incident, must follow all procedures correctly to minimize and control damage, and must identify all incidents and analyze their impact on various organizational resources and information.

It is the responsibility of the team to provide a single point of contact for the reporting of security incidents and issues. Moreover, it is also important to remember that the team is also responsible, as stated above, for obtaining the proper permissions for performing its IR processes. It must always be aware of any changes in legal and regulatory requirements to ensure that all processes and procedures are valid and compliant. It must also regularly review existing controls to evaluate its strength and ability to detect and stop attacks. In addition, the team must recommend steps, procedures, and technologies that can help the organization to prevent future security incidents. It should also establish good relationship with local law enforcement agencies, government agencies, key partners, suppliers, and IH&R teams at other companies—this will keep it up-to-date on current incident trends, threat intelligence, incident data, and security trends.

In addition, the IR team is responsible for performing the following:

- Issuing alerts and warnings about attacks, security vulnerabilities, and malware to authorities, security teams, stakeholders, clients, and customers.
- Gathering information about hardware and software vulnerabilities and devising methods for fixing these vulnerabilities.
- Performing first response procedures and handling the artifacts at the incident site.
- Conducting deep analyses of any incidents to identify attackers and attack vectors.

As the figure on the above slide demonstrates, an IR team must include particular members able to perform their responsibilities in ways that efficiently respond to any incidents:

- **Information Security Officer (ISO)**

  An ISO governs the security posture of an organization and bears responsibility for all IH&R activities in the context of overall organizational information security. The officer is responsible for setting IH&R goals, approving the process, granting permissions, and contacting the stakeholders and other management authorities of the organization.

  The ISO must head all the members of the IH&R team, including the incident manager and incident handler. The officer is also responsible for providing incident handling guidance and training to security team members across the organization, evaluating their actions and consequences, and suggesting corrective actions to perfect incident handling.

- **Incident Manager (IM)**

  The IM is responsible for managing all IH&R activities. The IM must be a technical expert with a clear understanding of and experience with handling security issues. The IM will focus on incidents as well as analyze and review incident handling processes from managerial and technical perspectives. He or she must drive the IR team to encourage focused incident containment and recovery.

- **Security Analyst**

  Security analysts support the IM by working directly with the affected systems and networks. They research threats, attack vectors, and attack methodologies to suggest best responses.

- **Incident Coordinator**

  Incident coordinators connect different stakeholders affected by incidents, such as the incident handling team, the legal team, the human resources team, clients, and vendors. They play a vital role in coordinating between security teams and networking groups, facilitate communication, and keep everyone updated on the status of the incident. The incident coordinator should possess communication and technical skills and have a solid business sense of the organization's operations.

- **Forensic Investigator**

  Forensic investigators—experts in the forensic investigation of incidents—help organizations and law enforcement agencies to investigate and prosecute the perpetrators of cybercrimes. They are responsible for maintaining forensics readiness across an organization and implementing effective IH&R. They must also preserve and submit the evidence required to legally prosecute the attackers.

- **Threat Researcher**

  Threat researchers supplement security analysts by researching threat intelligence data. They gather all details about prevalent incident and security issues and help spread its awareness among users. They also use this information to build or maintain a database of internal intelligence.

- **System Administrator**

  System administrators look after the working and security of systems and can be very helpful in the IR process—they configure systems and provide and grant access. They can also help in gathering system information, separating the impacted systems from the network, and analyzing system data to detect and verify incidents. They can also facilitate containment and eradication by installing new patches and updates and by upgrading the systems across an organization. They are also responsible for backup, system recovery, and analyzing system logs.

- **Network Administrator**

  Network administrators are responsible for examining a computer network's traffic for signs of incidents or attacks, such as DoS, DDoS, firewall breaches, or other malicious forms of code. They install and use network sniffing and capturing tools as well as loggers to identify the network events involved in an attack. They must analyze network logs, gather logs of suspicious activity, and help in the detection of incidents at a primary level. They perform the actions necessary to block network traffic from a suspected intruder.

- **Internal Auditor**

  Internal auditors must ensure that an organization complies with the regulations, business standards, and laws of its regions of operation. They must regularly audit the policies and procedures followed by the organization to maintain information security. They must also ensure that the organization's systems, devices, and other network resources are up-to-date and compliant with industrial regulations. They must identify and report any security loopholes to management.

- **Financial Auditor**

  Financial auditors are responsible for calculating the costs involved in an incident, such as damages or losses caused by the incident and costs incurred by IH&R. Along these lines, they must notably estimate the cost of cyber insurance and claim it when required.

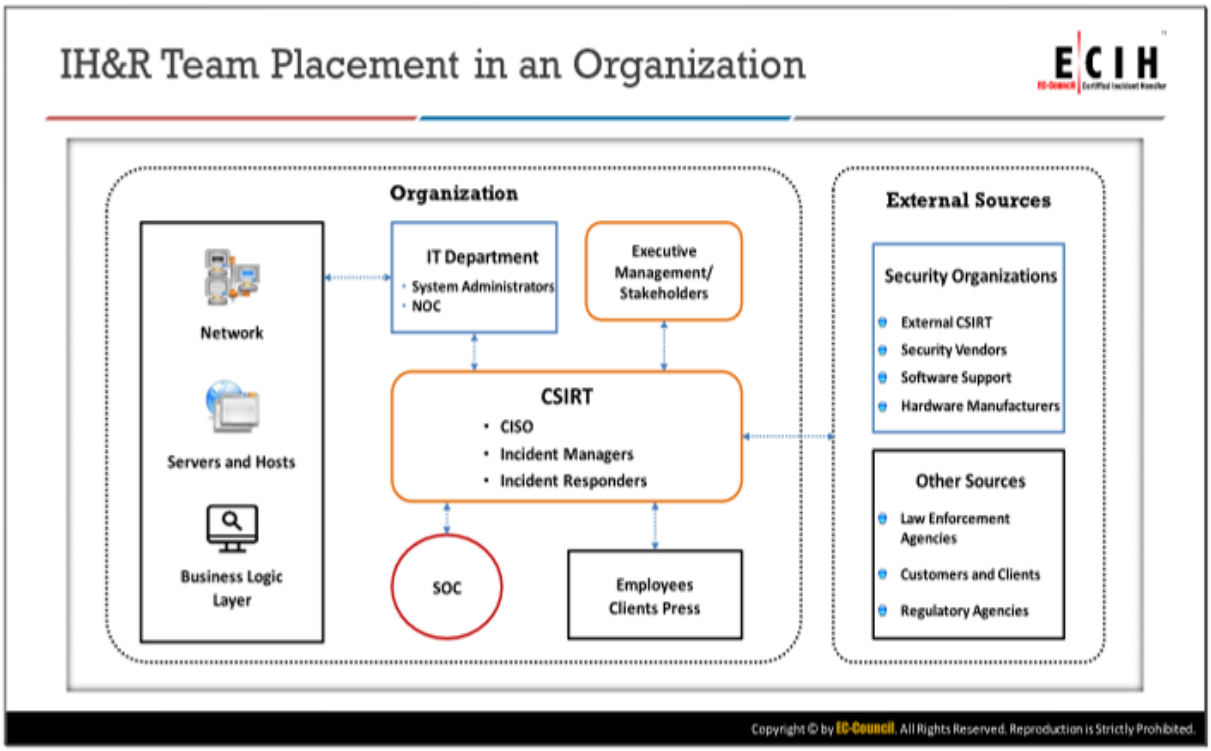
- **Human Resource**

  The human resources department is responsible for analyzing the human aspects of the disaster and conducting post-event counseling. Notably, it is responsible for tracking, recording, reporting, and compensating the organization's human resources for all the billable hours related to performing duties throughout the event. It also ensures the submission of records as well as other information related to payroll and keeps track of the records of all injuries along with the investigation results relating to events. Moreover, it is responsible for counseling people after the event and notifying various people, as per organization policy.

- **Public Relations**

  This department serves as a primary media contact and thus informs media about an event. It updates the organization's website information and monitors media coverage. Along these lines, it is responsible for stakeholder communication, including communications with:

  - The board
  - Foundation personnel
  - Donors
  - Grantees suppliers/vendors
  - Media



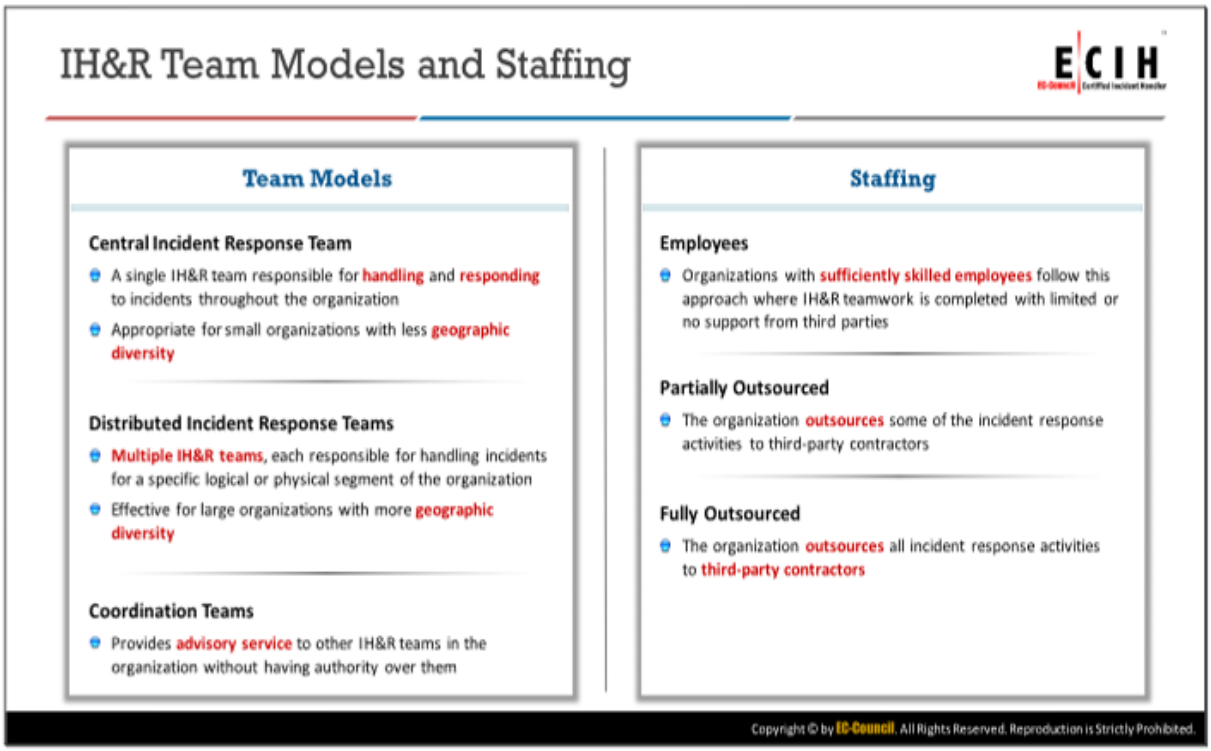
IH&R Team Placement in an Organization

The IR team, also called the computer security IR team (CSIRT), plays very important role in an organization. However, separately maintaining such a team can expend huge financial and other resources. Therefore, organizations often comprise their CSIRT teams with a few dedicated members and several other current employees who are experts in their fields.

Notably, a CSIRT can include network and system administrators, managers, stakeholders, employees, security operations center analysts, and so on. These members will have access to various resources and will coordinate with incident managers and incident responders to detect, contain, and eradicate incidents by providing their expertise.

To be sure, members of a CSIRT are granted access to work with employees, security operations centers, IT department teams, and so on. They act as first responders to gather information that plays a crucial role in the IH&R process. Notably, a CSIRT coordinates with the IT department to improve security across the organizational network, servers, and hosts.

Team members will coordinate with security organizations, peers working in other organizations, security vendors, software support, hardware manufacturers, and external CSIRT communities to gather information about various prevalent threats and to prepare themselves to respond to such threats. External sources share knowledge on new emerging attacks and different strategies for handling and responding to these attacks. The team can also coordinate with law enforcement agencies, customers, clients, and regulatory agencies to keep track of changes in standards, laws, regulations, and policies to make the organization compliant and secure.



IH&R Team Models and Staffing

An organization should have an appropriate IH&R team model and staff; this helps it successfully achieve its goals.

IH&R Team Models

An organization must plan and structure its IH&R team model based on risks involved, criticality of resources, type of services, availability of IR resources, number of members in a team, security evaluation report, vision, mission, and its goals for risk analysis and containment. Some of the most commonly implemented IH&R team models are:

- **Centralized IR Team**

  In this structure, a single team handles all the IR functions of a small organization. A centralized IR team is most effective for quickly responding to incidents. It is important to note that this structure is best suited for organizations operating from a single location.

- **Distributed IR Teams**

  Organizations with operations at multiple locations must implement a distributed IR team structure, wherein each location has a separate IH&R team to handle incidents. The organization must make these teams answerable to a single authority and maintain coordination between them. This model is effective for large organizations with more geographic diversity.

- **Coordination Teams**

  Coordination teams generally play an advisory role and are not directly responsible for IR. More specifically, coordination teams provide other IH&R teams in an organization with information and logistic support for IR.

IH&R Team Staffing

The selection of a skilled team is crucial for an effective IR. Organizations can use one of the following three IR team staffing methods:

- **Employees**

  Organizations with sufficient skilled employees follow this approach. The employees approach involves an IH&R team comprised of available human resources and in-house staff working with no or limited support from third parties.

- **Partially Outsourced**

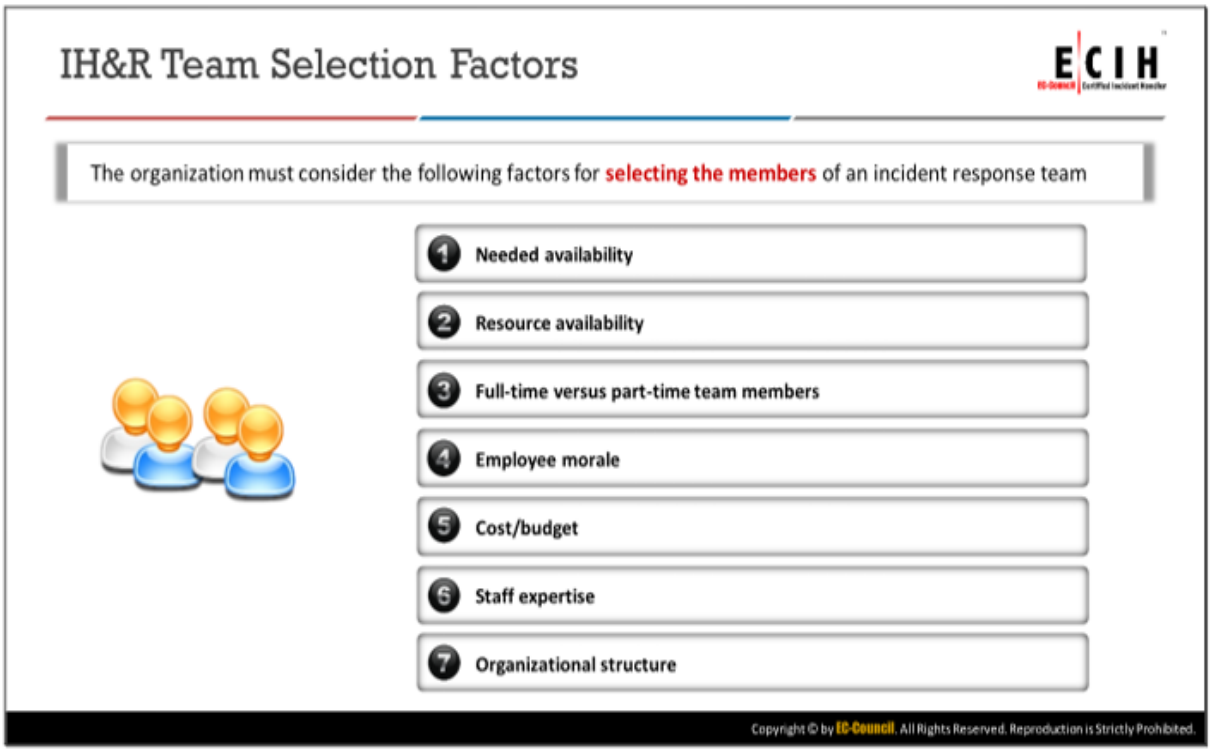
  In this model, the organization outsources some of its IR activities to third-party contractors. The type of IR activity that is outsourced depends on the following:

  - Availability of skilled people in the organization
  - The cost/benefit ratio of outsourcing the services
  - Criticality of perceived risks and incidents
  - Period of business continuity disruption

  Organizations can outsource incident handling activities that involve a long-term investment of financial and human resources and processes that do not involve highly confidential or sensitive information. They can also outsource activities that require additional technical expertise and support that is not available internally.

- **Fully Outsourced**

  In this staffing model, organizations completely outsource their IR activities to third-party contractors. Organizations generally prefer onsite contractors as they can quickly respond to an incident.



IH&R Team Selection Factors

An organization will choose an IH&R team structure and staffing model based on different factors specific its constitution such as:

- **Needed Availability**

  For organizations supporting critical infrastructures, damage from incidents increases with time; therefore, the IH&R team must be available to connect with other organization members over the phone or by other means around the clock.

- **Resource Availability**

  Any IH&R plan will fail if the organization does not have the technical expertise and equipment required to execute the plan. Organizations generally outsource their incident handling activities due to unavailability of in-house experts and their inability to invest in or maintain the required equipment.

- **Full-Time vs. Part-Time Team Members**

  Small organizations with limited funding and staff may not be able to afford permanent IH&R team members but may still require IR services. Accordingly, such firms tend to hire part-time IH&R team members to serve as a virtual IH&R team on which it can call during incidents. Usually, the IT help desk acts as a first POC when the incident takes place, as its members are very well trained in handling preliminary investigations, data gathering, and reporting incidents to the IH&R team. To be sure, organizations should ensure that any part-time members have the necessary expertise and awareness.

- **Employee Morale**

  The IR is very demanding and team members need to provide 24/7 support to fulfill their responsibilities. Because this kind of job is immensely stressful, there are many organizations that struggle to even find enthusiastic, accessible, proficient, and properly skilled people to fulfill such roles.

- **Cost/Budget**

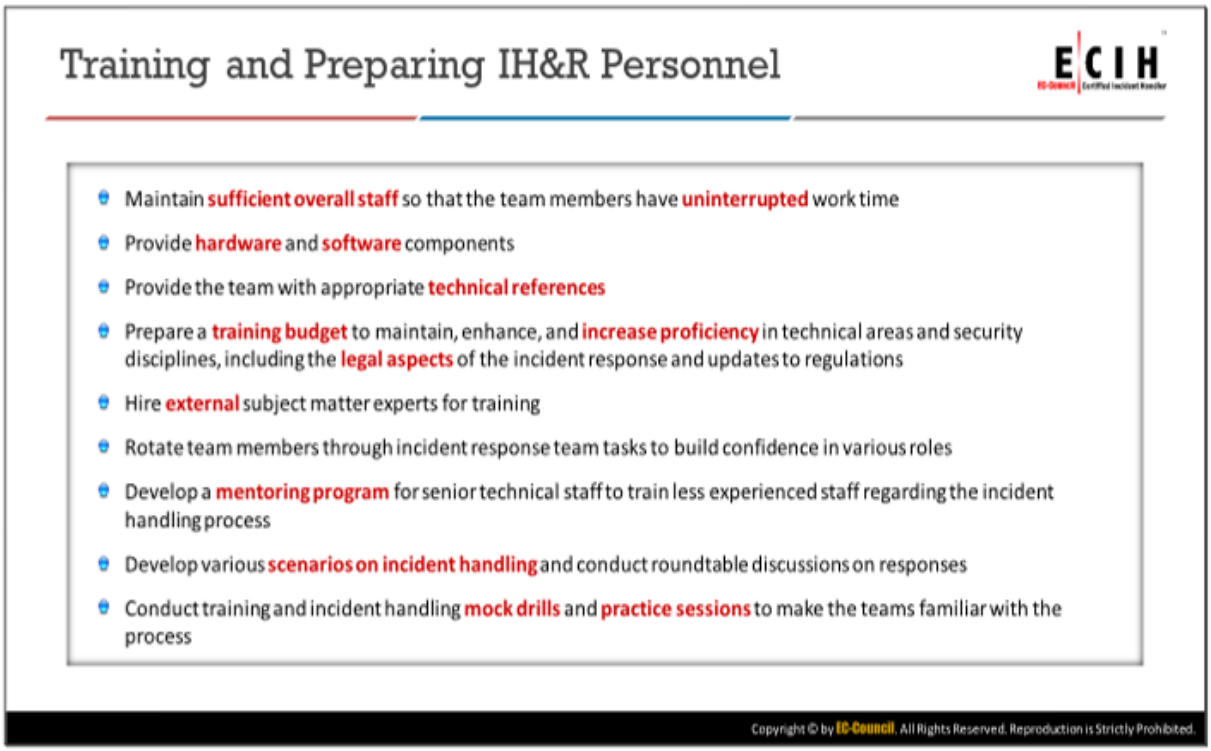
  As the IH&R team must be available for round-the-clock shifts, the costs involved in hiring personnel play a major factor in limiting team creation. Organizations must also calculate the expenses involved in training, conducting mock drills, providing and upgrading equipment, and meeting software and hardware requirements.

- **Staff Expertise**

  Experience and expert knowledge are important factors that organization must assess when selecting incident responders. These factors vary with the experience and number of risks an incident responder has handled in the organization. Compared to employees, outsourcers may have deeper knowledge of certain areas of IR; however, employees will nevertheless have a more capacious understanding of the organization, its resources, security solutions, and so on.

- **Organizational Structure**

  Large-scale or small-scale industries have various departments that function independently. If each department wishes to have its own IH&R team, the work will be more effective. An organization can also host a centralized IR entity that facilitates communication and implements standard practices among teams.



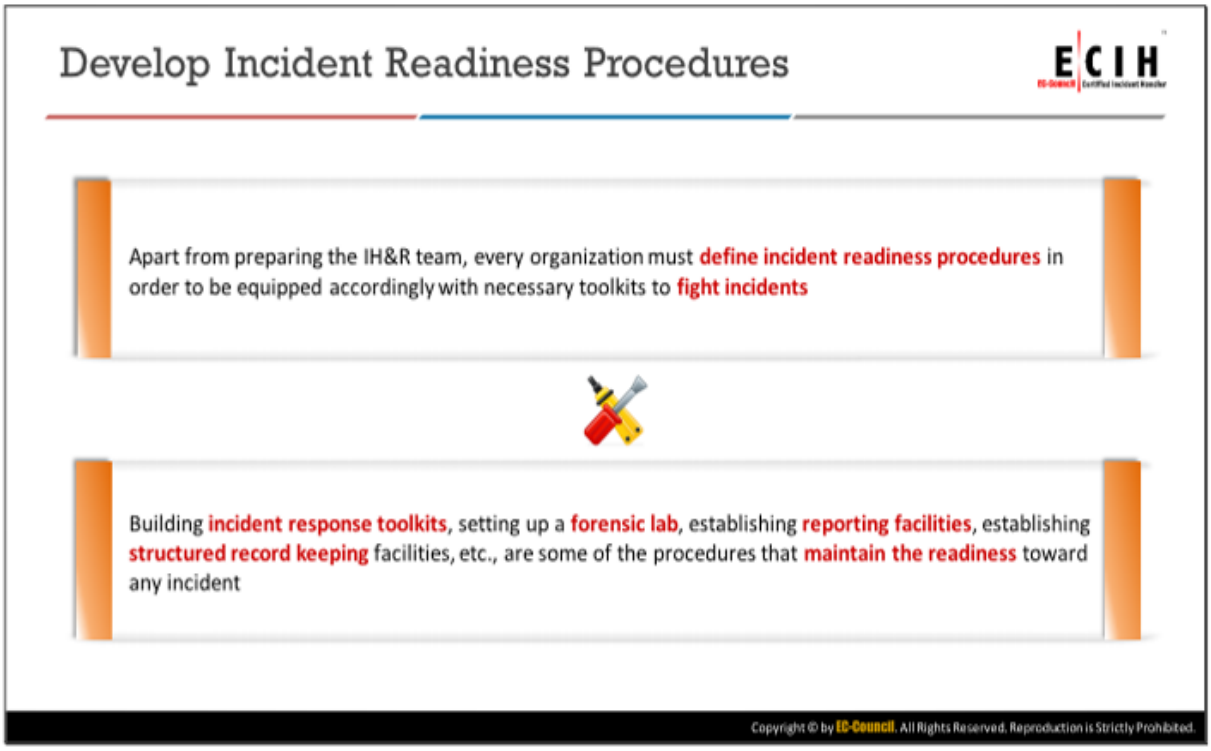
Training and Preparing IH&R Personnel

An IR team must always be completely trained and fully ready to implement an effective IR plan to protect an organization's assets and data from all types of incidents.

An organization can help the IH&R team be ready by ensuring the following:

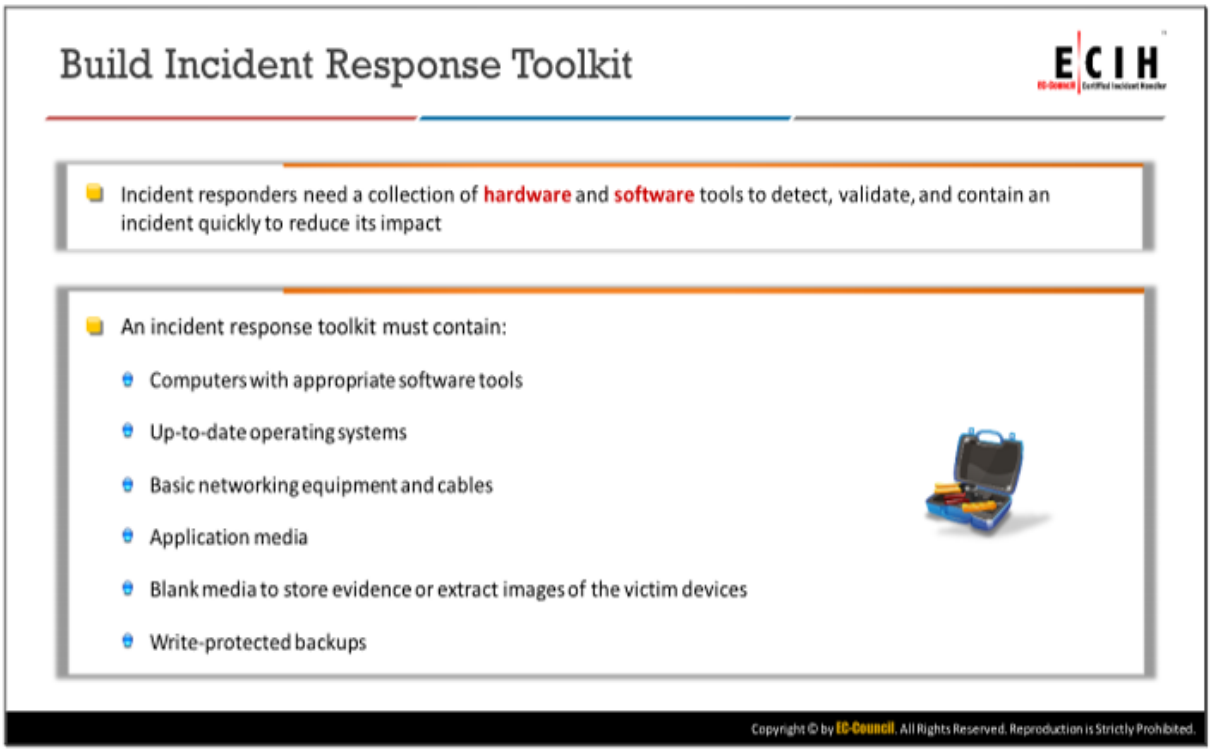
- Availability of appropriate books, articles, magazines, whitepapers, and other technical references to improve the team's technical knowledge of the subject
- Assignment of a part of the budget to send IH&R team members to conferences and training sessions to maintain, enhance, and increase proficiency in technical areas and security disciplines, including the legal aspects of the IR by the legal experts
- Provision of opportunities to team members to perform other tasks associated with IR, such as preparing educational materials, conducting security awareness workshops, and conducting research
- Consideration of the rotation of IH&R team members with other staff to achieve full coverage and to help them learn new skills
- Maintenance of required staffing so team members can take time off
- Creation of a mentoring program so that senior technical staff members can train less experienced staff
- Hiring of outside experts with good technical knowledge to train IH&R team members
- Development of various scenarios about incident handling and the institution of group discussions on various ways of handling them

- Rigorous IH&R training for all IH&R team members, including incident responders and management
- Incident handling mock drills to improve the performance of incident handlers, identify issues with policies and procedures, and improve communication
- Teaching of additional skills to the team such as teamwork, communication, aptitude, effective speaking, and effective writing to help team members explain scenarios to other non-technical authorities and work groups



Develop Incident Readiness Procedures

Apart from preparing an IH&R team, every organization must define its incident readiness procedures in order to be equipped with the toolkits necessary to fight incidents. Building IR toolkits, setting up a forensic lab, establishing reporting facilities, and establishing structured record-keeping facilities are some key procedures that must be performed to maintain readiness for any incident.

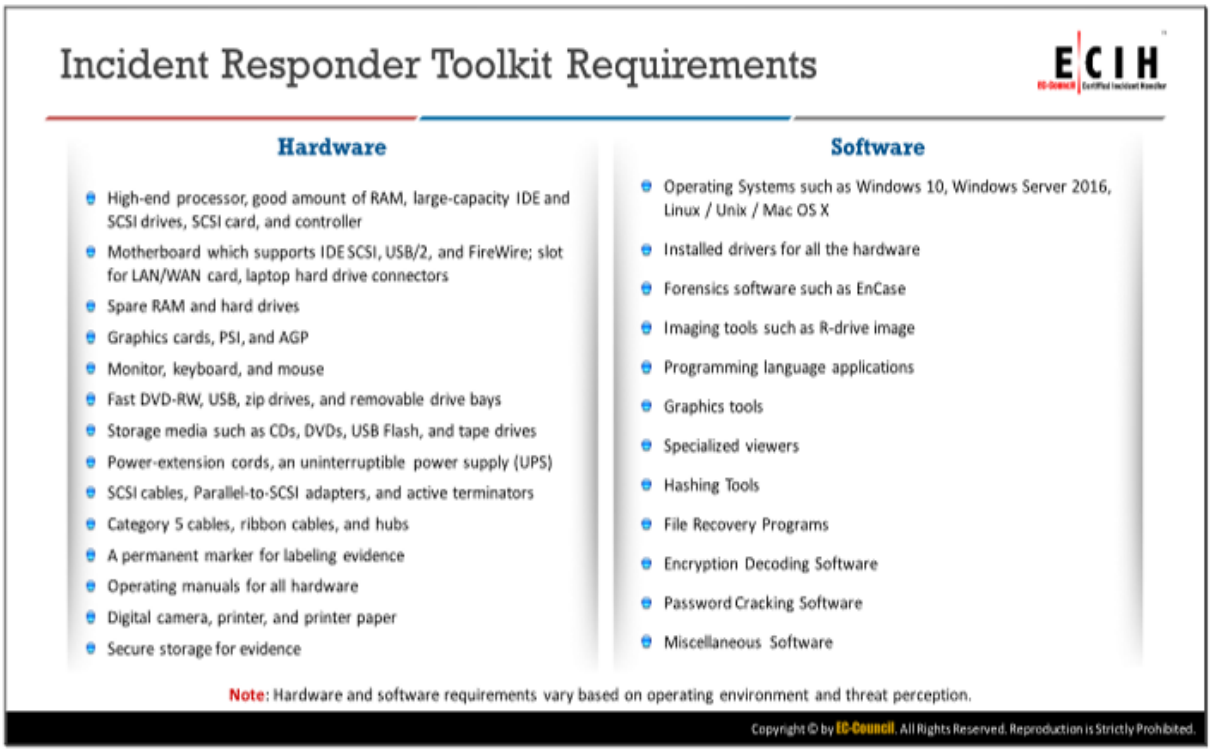


Build Incident Response Toolkit

Incident responders require a toolkit comprising hardware and software tools to detect, validate, contain, and eradicate an incident in time and reduce the impact of the incident. Accordingly, an organization must build an IR toolkit that contains:

- Computers with appropriate software tools
- Up-to-date operating systems and patches
- Basic networking equipment and cables
- Application media
- Blank media to store evidences or extract images from victim devices
- Write-protected backup devices

An organization should create its toolkit before commencing an IR process, as the response team needs to practice with the tools during mock drills to become familiar with them.



Incident Responder Toolkit Requirements

IH&R includes critical processes such as duplication of data, recovering data from deleted files, analyzing data over the network, and retrieving data from the slack. The IR includes various high-end and low-end processes; thus, the hardware configuration of IR workstations used for extreme processing will differ from that of a workstation used for routine tasks.

Hardware Requirements

The hardware requirements are as follows:

- High-end processor, good amount of RAM, large-capacity IDE and SCSI drives, and SCSI card and controller
- Graphic cards, PSI, and AGP
- Fast DVD-RW, USB, zip drives, and removable drive bays
- 8 GB of RAM for satisfying minimum processing requirements
- Storage media such as CDs, DVDs, USB Flash, and tape drives
- A motherboard capable of supporting IDE, SCSI, USB, a LAN/WAN card, and a fan attached for cooling the processor
- Power-extension cords and an uninterruptible power supply (UPS)
- Monitor, keyboard, and mouse, according to the comfort of the investigator
- A minimum of two hard drives for loading two different operating systems
  - The two operating systems should preferably be Windows and Linux
- Extra RAM and hard drive just in case they are needed

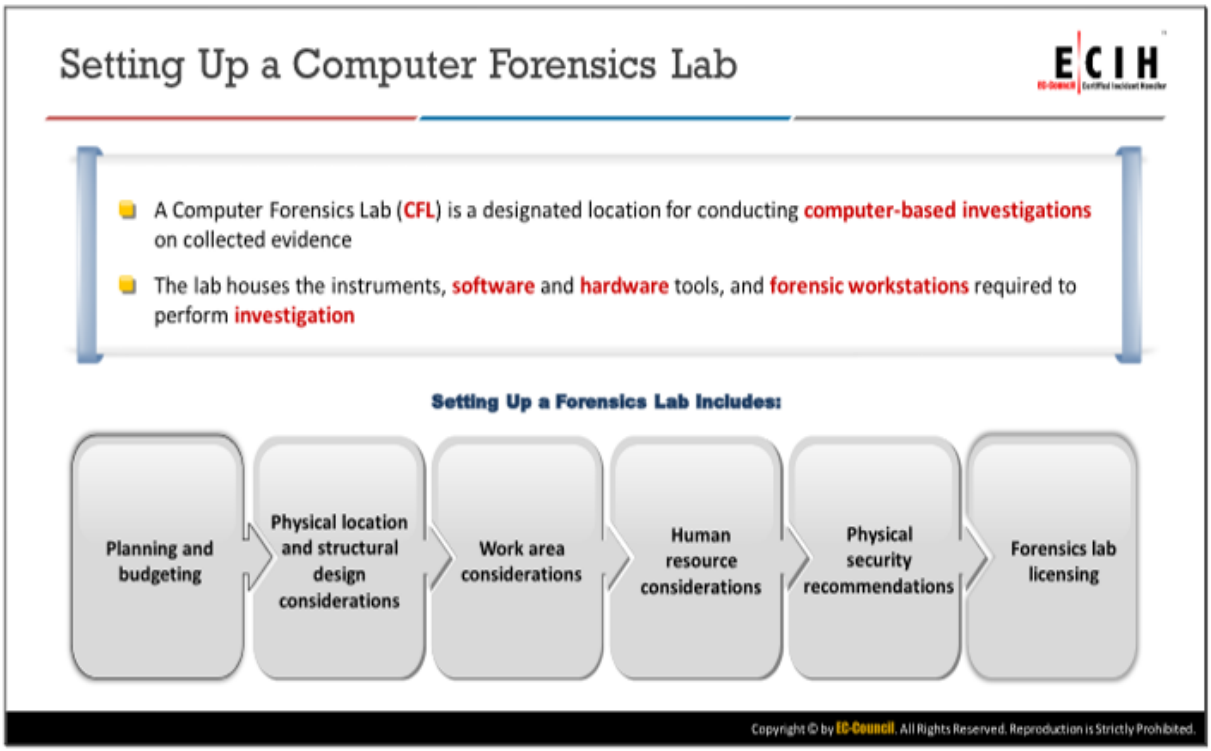
- SCSI cables, Parallel-to-SCSI adapters, and active terminators
- Category 5 cables, ribbon cables, and hubs
- A permanent marker for labeling evidence
- Operating manuals for all hardware
- Digital camera, printer, and printer paper
- Paper shredders and burn bags
- Paraben Forensics hardware, including Handheld First Responder Kit, and a Wireless StrongHold Bag

Software Requirements

The IR toolkit requires the following software:

- Operating systems (either Windows 10, Windows 8, Windows XP, Windows Server 2003, Windows 2007, Linux, Unix, or Mac OS X)
- Drivers for all hardware
- Forensics software packages (e.g., EnCase, FTK)
- Imaging tools (e.g., R-drive image, P2 eXplorer Pro)
- Programming language applications (e.g., Visual Studio Suite)
- Graphics tools (e.g., Adobe Photoshop, CorelDraw)
- Specialized viewers (e.g., File Viewer, QuickView Plus)
- Hashing tools (e.g., HashMyFiles, HashTab)
- File recovery programs (e.g., File Scavenger, PC Inspector File Recovery)
- Encryption decoding software (e.g., True Crypt, AxCrypt)
- Password cracking software (e.g., Aircrack, Cain and Abel, John the Ripper)
- Miscellaneous software (MS Office, WordPerfect/StarOffice/OpenOffice)

Note: Hardware and software requirements vary by operating environment and threat perception.



Setting Up a Computer Forensics Lab

A Computer Forensics Lab (CFL) is a designated location for conducting a computer-based investigation of the collected evidence in order to solve the case and find the culprit. The lab houses the instruments, software and hardware tools, suspect media, and the forensic workstations required to perform investigation of all types.

Setting up a forensics lab includes:

- **Planning and Budgeting**

  Before planning and evaluating the budget for the forensic investigation case, consider the following:

  - Break down costs into daily and annual expenditures
  - Refer to past investigation expenses
  - Be aware of updated technology
  - Using statistics, obtain an idea of the computer crimes most likely to occur

- **Physical Location and Structural Design Considerations**

  - Ensure the lab room is secured
  - Ensure heavy construction materials are used
  - Ensure lab exteriors have no windows
  - Ensure computer systems face away from windows
  - Consider room size, ventilation, and temperature

- Consider the number of workstations the room can occupy

- **Work Area Considerations**

  A lab's environment can affect its productivity. For our purposes, it is important to note that a lab must include a workspace for every examiner.

  Consider the following for examiner workspaces:

  - An examiner station requires an area of approximately 50–63 square feet.
  - A workplace requires a table large enough to examine a physical computer.
  - A forensic workstation requires a space large enough to accommodate additional equipment, such as notepads and printers.

- **Human Resources Considerations**

  All examiners, technicians, and administrators must be certified and experienced in their respective fields.

- **Physical Security Recommendations**

  - The room must be small with good floors and a good ceiling
  - The door must have a strong lock
  - The room must have a secure container, such as a safe or file cabinet
  - Visitor logs must be maintained

- **Forensics Lab Licensing**

  Forensics labs must be licensed by the concerned authorities to be trustworthy. Authorities provide such licenses after reviewing the lab and its investigative facilities. Some such licenses include:

  - ASCLD/LAB accreditation
  - ISO/IEC 17025 accreditation

Establish Reporting Facilities

- Develop and publish **detailed policies** for reporting security incidents
- Incident reporting policies should include:
  - Ways to report an incident
    - Email, phone, fax, etc.
  - Who receives the report
  - IH&R team, local law enforcement agencies, senior management, network administrators, etc. according to the type of incident
  - Details to be reported
    - Intensity of the incident, circumstances that revealed the incident, summary of hosts involved, description of the activity, type of confidential data involved, and other information the reporter believes to be relevant.
- **Educate users** to identify and report security incidents
- Make computer security **incidents reporting forms** and templates available to all users

Establish Reporting Facilities (Cont'd)

Example Incident Reporting Template

<Organization Name> Incident Reporting Template

Date: Name of individual completing the form:

Tracking number:

Incident Priority

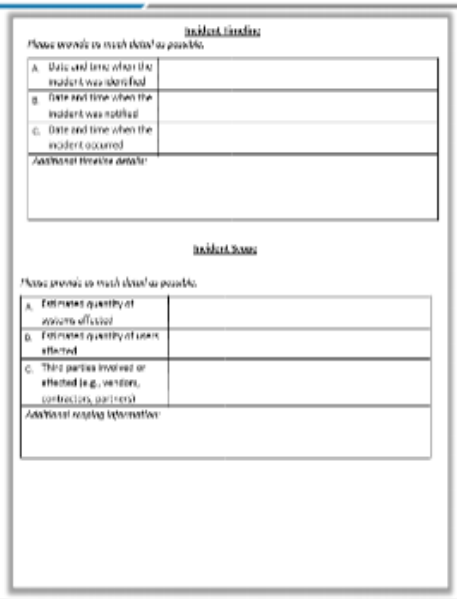
☐ HIGH	☐ MEDIUM	☐ LOW	☐ OTHER
Additional notes:			

Incident Type

Check all that apply

☐ Compromised System	☐ Lost Equipment/Theft
☐ Compromised User Credentials (e.g., lost password)	☐ Physical Breach
☐ Network Attack (e.g., DoS)	☐ Social Engineering (e.g., Phishing)
☐ Malware (e.g., virus, worm, Trojan)	☐ Law Enforcement Request
☐ Reconnaissance (e.g., scanning, sniffers)	☐ Policy Violation (e.g., acceptable use)
	☐ Unknown/Other (Please describe below.)

Incident observation notes:



Incident Timeline

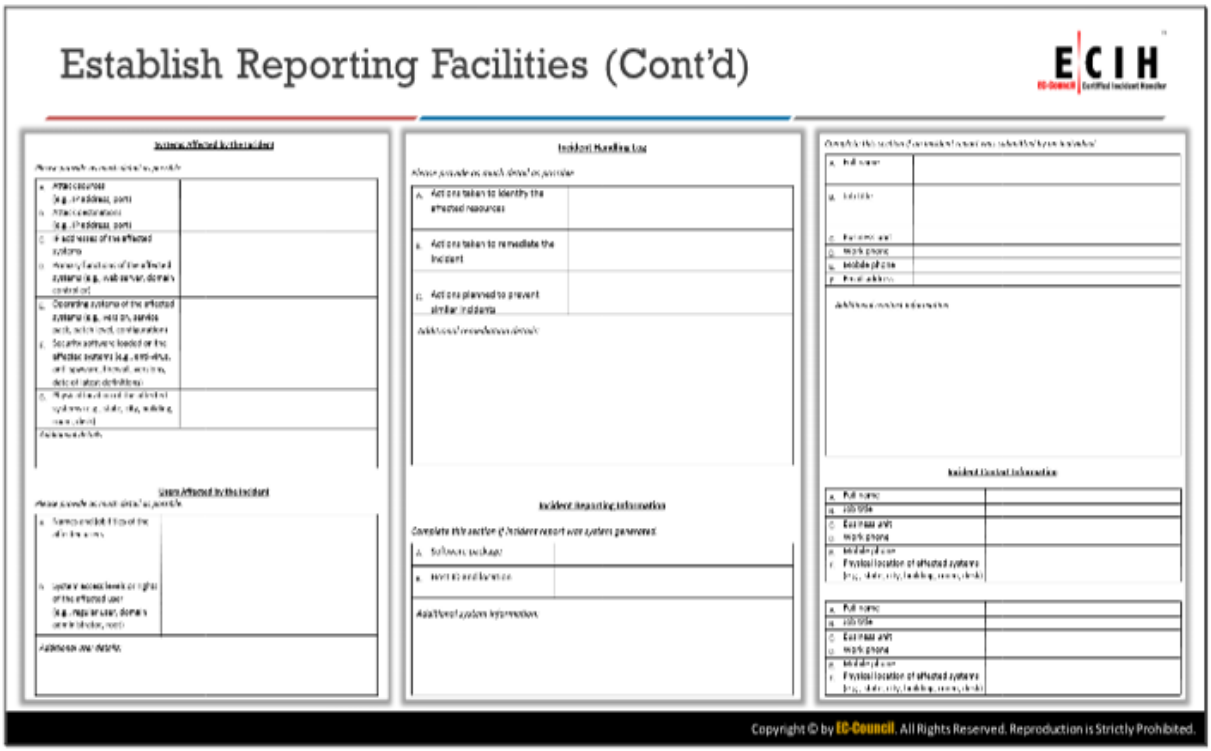
Please provide as much detail as possible.

A. Date and time when the incident was identified	
B. Date and time when the incident was notified	
C. Date and time when the incident occurred	
Additional timeline details:	

Incident Scope

Please provide as much detail as possible.

A. Estimated quantity of systems affected	
B. Estimated quantity of users affected	
C. Third parties involved or affected (e.g., vendors, contractors, partners)	
Additional scoping information:	



Establish Reporting Facilities

In an organization, incident responders should be able to report incidents as early as possible to obtain permissions for investigating the premises, stopping services, disconnecting web servers or systems, and performing any actions that may even momentarily disrupt service. IH&R team members should know the what, whom, how, and when of reporting incidents in order to obtain required approvals and efficiently handle an incident. Notably, an incident handler is responsible for creating, developing, publishing, and bringing into effect detailed policies for reporting security incidents.

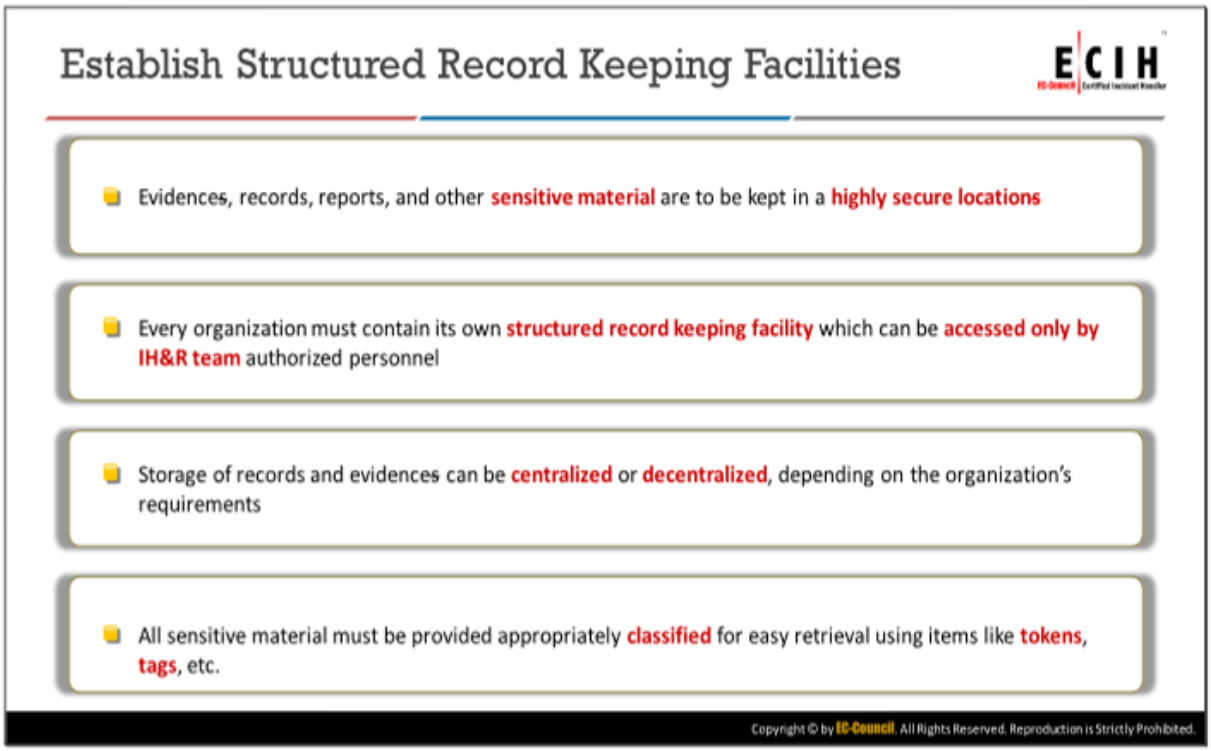
An incident reporting policy will guide an IH&R team in reporting incidents. The methods used for reporting incidents are crucial because these incidents may impact the organization's network; therefore, incident responders need to use different methods, such as email, mobile phone, landline, and fax.

The policy should also include the names, numbers, and designations of authorities to whom responders can report an incident. For example, responders can report an incident to the IH&R team, local law enforcement agencies, senior management, network administrators, and so on according to the type of incident. Policy designers may also consider adding a table listing the persons responsible for each type of incident.

The most crucial part of the report is the inclusion of the incident details. Responders should be trained to analyze an incident and choose what details to report based on the type of incident. Commonly reported incident details include the intensity of the incident, the circumstances that revealed the incident, a summary of the hosts involved, a description of the activity, and the type of confidential data involved.

Moreover, it is also important to train and educate users, IT support staff, network administrators, system administrators, and other staff to identify and report security incidents to members of the IH&R team. Along these lines, it can be helpful to develop computer security incident reporting forms and templates and make them easily available to all users.

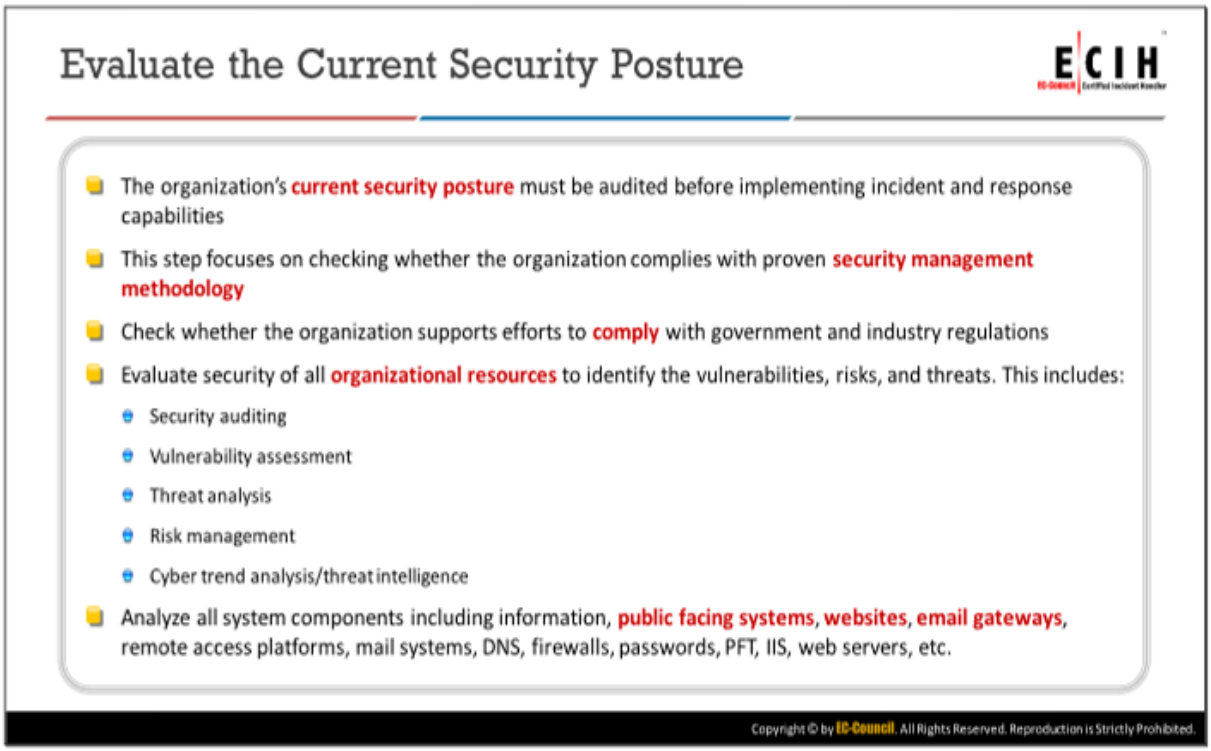
The screenshot shown on the above slides display an example of an incident reporting template.



Establish Structured Record Keeping Facilities

Evidence, records, reports, and other sensitive materials are to be kept in a highly secure location. Every organization must possess its own structured record-keeping facility accessible only by IH&R authorized personnel—internal users and employees must not be able to access such a storage facility where evidence is preserved. Accordingly, such a storage facility secures evidence and prevents evidence contamination or damage.

Notably, record and/or evidence storage can be centralized or decentralized, depending on the requirements of each organization; however, a storage facility should possess a structured record-keeping capability. All sensitive material must be organized with an appropriate classification system, such as one involving tokens and tags, to avoid mixing up different records, forms of evidence, or other sensitive materials. Helpful to note is that evidence storage bags are often employed to store sensitive material.



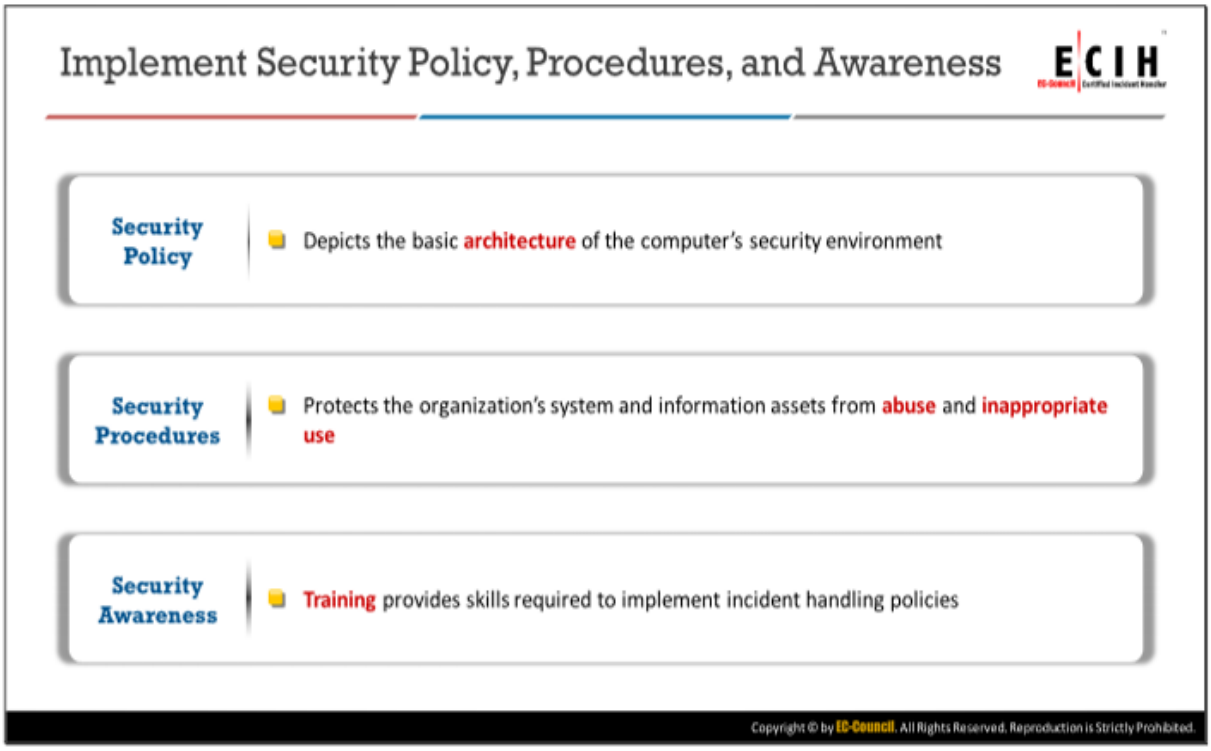
Evaluate the Current Security Posture

An organization must audit its current security posture before developing an IH&R plan. This will help the incident handler understand the security features employed and his or her role in protecting the organization from attacks. It will also enable the incident handler to check whether the organization leverages a proven security management methodology.

Under this step, the incident handler should check whether the organization supports efforts to comply with government and industry regulations as well as local and international information security laws. The IH&R team should assess the security of all organizational resources to identify the vulnerabilities, risks, and threats to all system components, including information, public-facing systems, websites, email gateways, remote access platforms, mail systems, DNS, firewalls, passwords, PFT, IIS, and web servers.

Steps involved in evaluating security include:

- Security auditing
- Risk management
  - Vulnerability assessment
  - Threat analysis
  - Cyber trend analysis/threat intelligence



Implement Security Policy, Procedures, and Awareness

One key task while evaluating the current security posture is to implement and check the security policies, procedures, and awareness of employees regarding incident handling.

- **Security Policy**

  Incident handlers are liable for analyzing an organization's assets and accordingly creating suitable security policies. Such policies should help the IH&R team efficiently execute the incident handling process.

  Security policies should address:

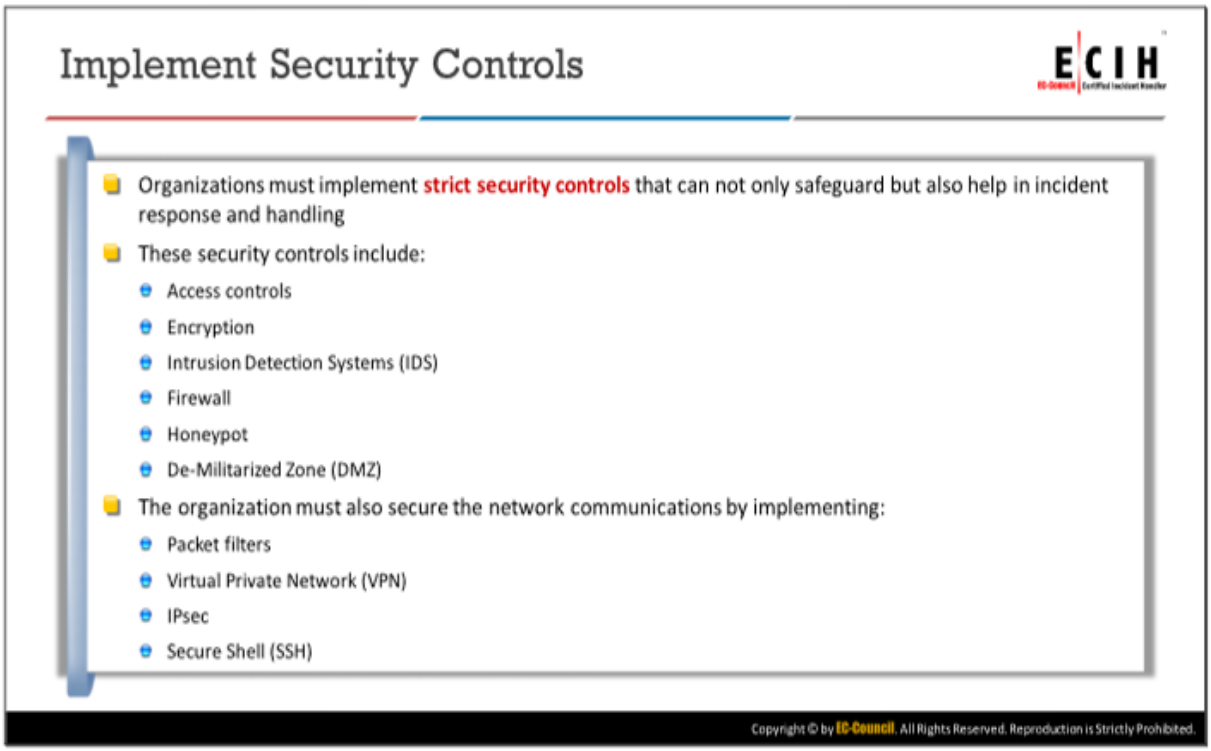
  - The securitization of sensitive information, systems, networks, devices, and accounts against internal and external attacks
  - The creation and assignment of secure user IDs, passwords, administrator accounts, privileges, access to web servers, databases, and other networking devices
  - The logging of network traffic and events in systems, servers, databases, and other networking equipment and the enabling of logs for security solutions including firewalls, antivirus programs, and IDS
  - Responses to potential security incidents, intrusion attempts, attacks, vulnerabilities, and threats
  - Proper usage policies for employees who use workstations, email, the Internet, and devices and who handle sensitive information
  - Ease of physical access to the building and different resources for the IH&R team
  - The creation of regular backups and their storage at an external location

- **Security Procedures**

  An IH&R team should have standard operational procedures (SOPs) for dealing with different types of attacks. The incident handlers will define SOPs and include the specific technical processes, techniques, checklists, and forms the IR team should use during the response process. SOPs should be elaborate and detailed to meet the requirements of the organization. These procedures should help to minimize errors, costs, and damages to assets. The procedures should be tested and validated for effectiveness being implemented in real time.

- **Security Awareness**

  Awareness should be created about incident handling processes among employees and their roles in the IH&R team should be discussed. Users should also be trained to implement secure practices across their systems, networks, accounts, and data as well as in how to cooperate with the IH&R team during and after IR procedures.



Implement Security Controls

The organization must configure and implement strict security controls in such a way that they not only safeguard network resources and information but also assist in IH&R procedures. As part of these security controls, the organization must limit access to its resources to the minimum required levels.

An organization must implement the following security controls:

- **Access Controls**

  Access controls ensure that only selected or eligible employees have access to sensitive data, critical devices, and other necessary resources required to accomplish the assigned tasks. The organization must develop and implement a policy regarding access to crucial data and resources as well as define different levels of privileges. Organizations should also deploy authentication and authorization methods to divide and maintain privileges.

- **Encryption**

  Encryption mechanisms should be implemented to ensure the confidentiality and integrity of the information stored and transmitted. The encryption process ensures that only the sender and the receiver of a message can read the message by preventing any unauthorized access. The mechanism also includes an encryption key that can be used to decrypt the message. Common encryption algorithms used to encrypt data include RSA, MD5, SHA, DES, and AES. An organization must ensure that data storage mechanisms implement strong encryption algorithms for its stored data as well as backups to prevent theft.

- **Intrusion Detection Systems (IDS)**

  An organization must implement hardware and software IDS across its network to filter network traffic for illegal activities, malware, policy violations, and data exfiltration.

- **Firewall**

  An organization must implement a secure firewall and configure it to filter both incoming and outgoing traffic to prevent all types of attacks. The firewall must be connected to an online database that automatically updates security policies and rules in accordance with current attack trends.

- **Honeypot**

  A honeypot is a computer system on the Internet intended to attract and trap people who attempt unauthorized or illicit use of a host system. Organizations must deploy multiple honeypot traps across their networks and configure them to alert their IH&R teams and other security personnel of any attempted security breaches.

- **De-Militarized Zone (DMZ)**

  A DMZ is a small network placed between an organization's private network and an outside public network that prevents an outsider from directly accessing the organization's server. Organizations must place multiple DMZs across their networks to trap intruders and block them from accessing the network.

Meanwhile, an organization must secure its network communications by implementing the following elements:

- **Packet Filters**

  An organization should implement packet filters that assess data transfers to and from networks to uncover any data theft attempts. Notably, implementing packet filters can be a little tricky: most communication is encrypted and filters fail to detect data theft across encrypted packets.

- **Internet Protocol Security (IPsec)**

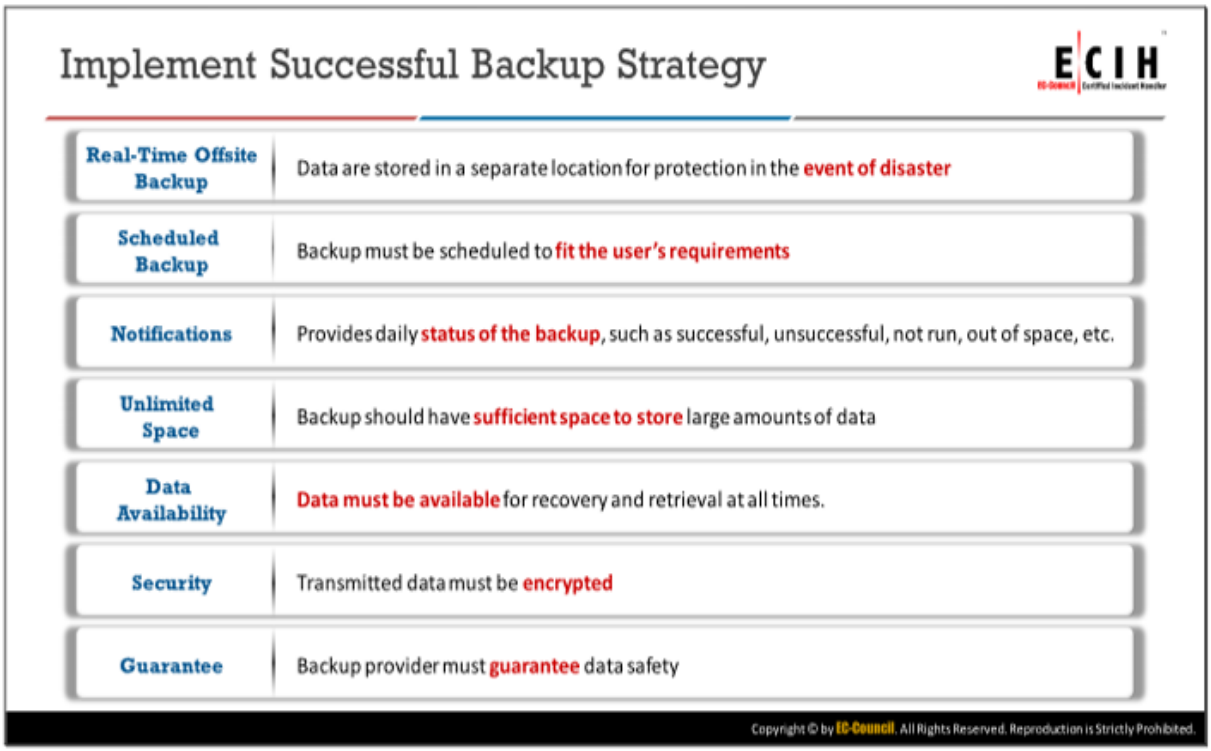
  Organizations implement IPsec to authenticate and validate packets during transmission.

- **Virtual Private Network (VPN)**

  A VPN allows an organization to use secure channels to transfer data in an encrypted medium. An organization must use a VPN with a secure encryption algorithm to transfer crucial data.

- **Secure Shell (SSH)**

  SSH is a protocol used to secure remote login and provide secure network services over an insecure network. SSH protects an organization against spoofing, sniffing, and eavesdropping. Implementing SSH protocols across web services and applications will secure data.



Implement Successful Backup Strategy

Creating a backup policy is one of the most important tasks of an incident management plan. In case of an incident, backup policies and procedures will save an organization time and money by making it easy for the organization to restore its compromised systems and services. It will also ensure a smooth recovery process in the event of a hard drive failure, virus attack, or natural disaster.

A successful backup strategy must have the following features:

- **Real-Time Offsite Backup**

  A real-time offsite backup indicates data stored in a place away from the original site for safekeeping in the event of disaster.

- **Scheduled Backup**

  Scheduled backups consistently save data based on a user's requirements.

- **Notifications**

  Notifications provide daily status updates on a backup situation such as whether the backup was successful, unsuccessful, or not run and whether the drive was out of space.

- **Unlimited Space**

  The strategy should ensure that unlimited space is available to backup large amounts of data.

- **Data Availability**

  The strategy must make data available at any time to ensure the retrieval and recovery of lost data.

- **Security**

  The strategy must ensure that transmitted data is encrypted.

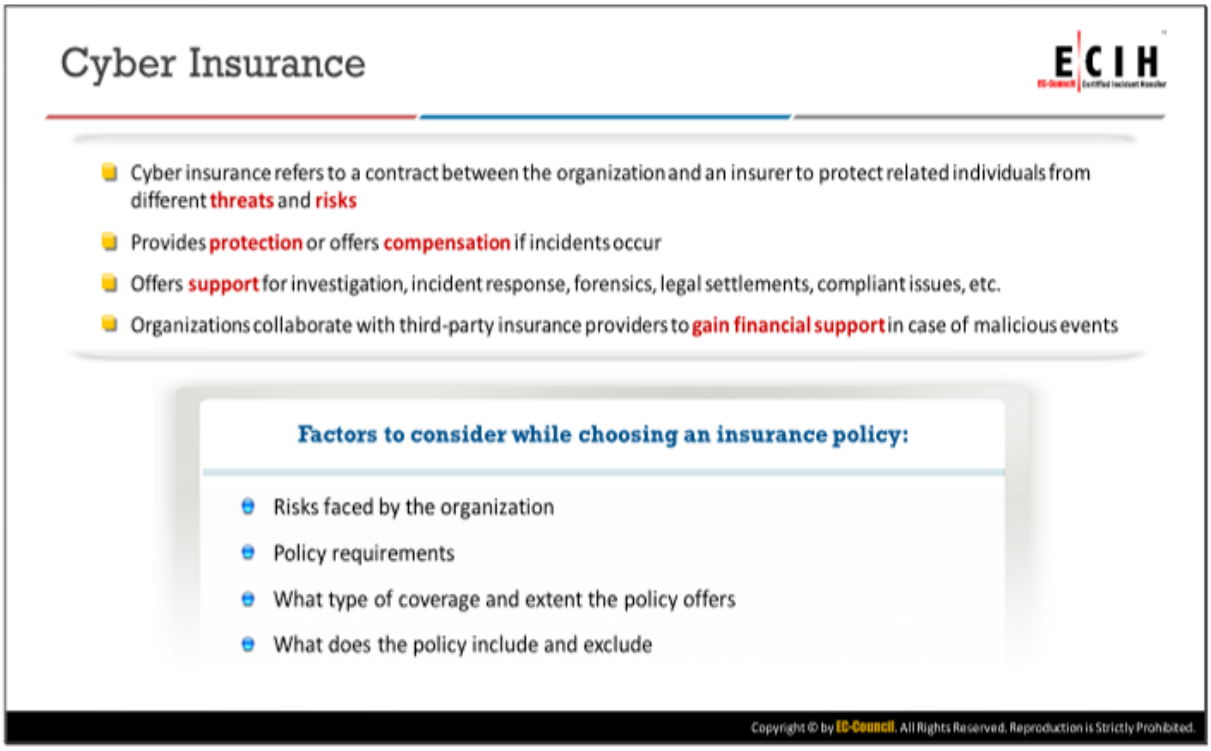
- **Guarantee**

  The strategy should mandate a backup provider that guarantees data safety.

Backup policies and procedures vary according to the needs of each organization and industry. An organization must select a backup process that supplements its requirements and ensure that it has multiple copies stored at different locations.

In sum, incident handlers should consider the following guidelines when selecting a backup strategy:

- The backup should be in real time and created at a far offsite location to secure data in the event of disaster.
- The backup schedule must fit the user's requirements.
- The backup system should provide alerts and daily status updates about the backup situation such as whether the backup was successful, unsuccessful, or not run and whether the drive was out of space.
- The backup system should have unlimited space for storing large amounts of data.
- The backup system must make data available at any time to ensure the retrieval and recovery of lost data.
- The backup system should encrypt transmitted data.
- The backup provider must guarantee data safety.



Cyber Insurance

Cyber insurance refers to a contract between an organization and an insurer to protect related individuals from different threats and risks. In other words, an insurer ensures that the business of an organization continues after an incident by providing cash to reduce the organization's related financial losses. An organization must therefore select an appropriate insurance policy to insure its assets, data, and other infrastructure to protect itself from any losses it may incur from an incident.

The contract between an organization and an insurer (also called an "insurance policy") determines the premium and contract period (that is, the period during which the insurer will provide protection or offer compensation if an incident occurs). Although such insurance does not cover whole losses, it will compensate an organization based on the damage and type of incident it suffers.

Why do organizations need cyber insurance?

Cybersecurity has become one of the most crucial elements of a business owing to organizations' high dependency on technology as well as the increase in cyber threats that can inflict huge financial and reputational losses. Sometimes, organizations will require financial support to cover any damages and may even fail to survive such incidents. Therefore, many organizations collaborate with third-party organizations that claim to offer protection from attacks, as well as provide financial support, in case of any malicious events.

Apart from financial assistance, insurance may offer support in investigation, IR, forensics, legal settlements, compliant issues, and so on. These features make cyber insurance a necessity for all organizations.

What to look for?

Cyber insurance comes in various forms and offers a wide range of coverage options that allow organizations to select policies that best suit their coverage and premium requirements. Ideally, a business cannot select a single coverage option due to the ever-changing nature of the technology landscape, attacks, and security requirements. Therefore, organizations should select the best of all available options and try to evaluate and renew such options according to changing requirements.

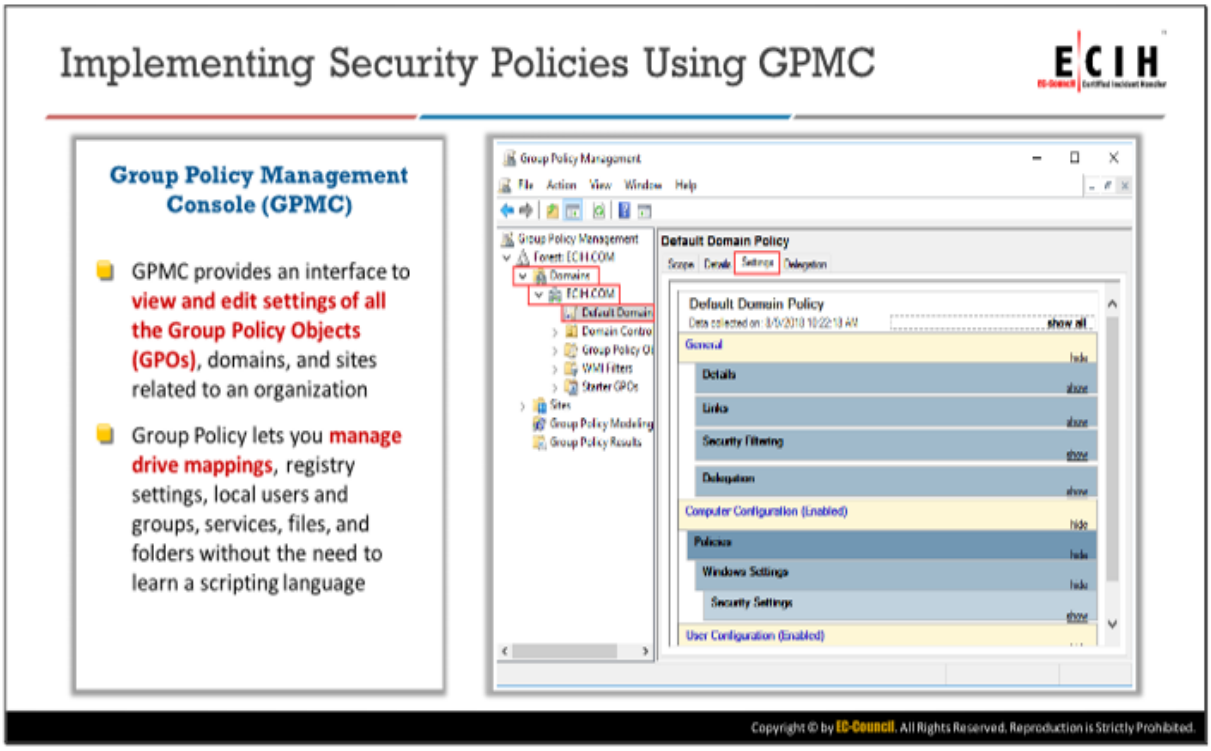
Factors for an organization to consider when choosing a cyber insurance policy include:

- Risks the organization faces or the requirements of the policy
- Types of incidents the policy covers
- Type and extent of the coverage the policy offers
- The policy's inclusions and exclusions
- Triggers for the activation of the policy
- Cost of an incident
- Covers first-party and third-party losses

Incident handlers and other security officials should assist management in selecting the best plans based on their requirement and the different forms of coverage offered. The organization should ensure that the insurance policy it selects covers all the different types of cybersecurity threats, losses, and investigation-related expenses it is liable to face.

The organization should also consider the processes of filing an insurance claim, notifying reporting authorities, and collecting any evidence and supporting documents required. During the selection of a cyber insurance policy, an organization should ensure that the claim covers:

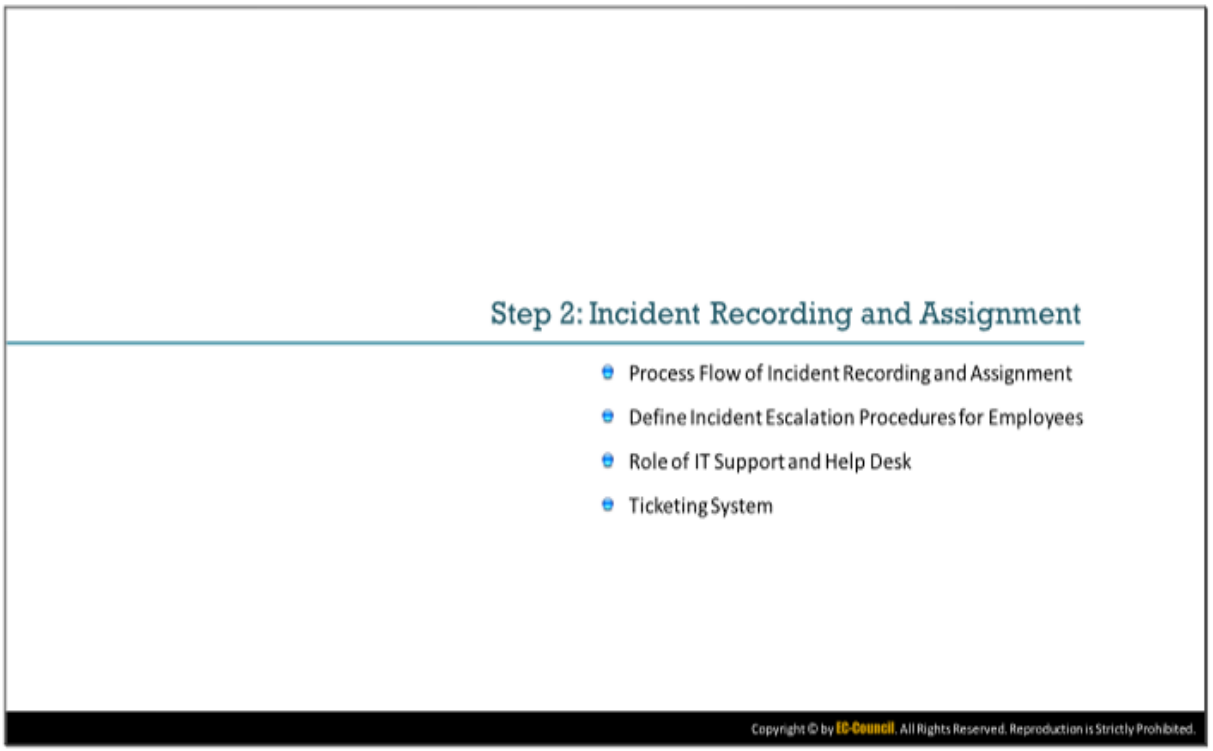
- Network and connected devices
- Hardware and software assets, including applications, operating systems, and security solutions
- Staff and other human resources
- Reasonable response time for data breach incidents, including recovery and response planning
- Digital assets, including stolen and lost data
- Losses occurring due to third-party systems
- Legal and compliant settlements, as well as includes governmental fines
- Protection from terrorism and cyber extortion
- Business disruptions
- Expenses for IR, recovery, and forensics



Implementing Security Policies using GPMC

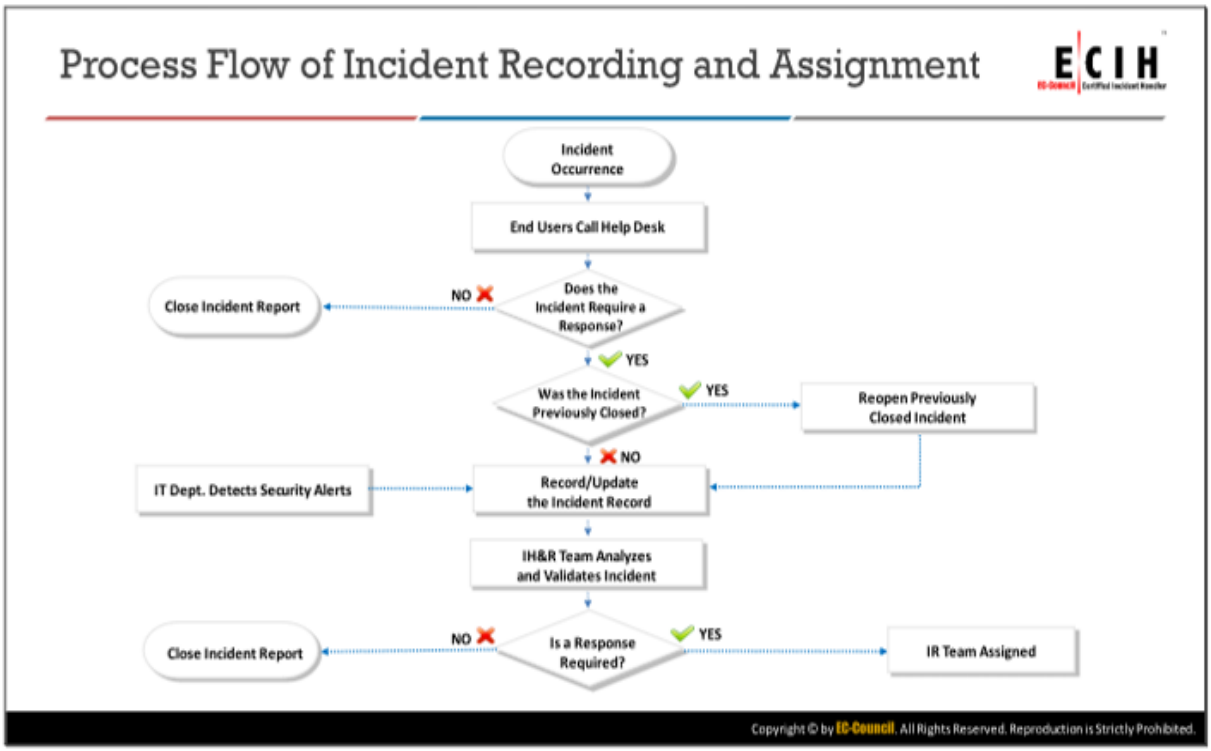
In Windows operating systems, the Group Policy Management Console (GPMC) is part of Windows Administrative Tools. GPMC is a scriptable interface for managing Group Policy. More specifically, GPMC provides an interface for viewing and editing the settings of all Group Policy Objects (GPOs), domains, and sites related to an organization.

Group Policy Preferences provide more than twenty Group Policy extensions that expand the range of configurable preference settings in a Group Policy Object (GPO). Group Policy lets users manage drive mappings, registry settings, local users and groups, services, files, and folders without the need to learn a scripting language.



Step 2: Incident Recording and Assignment

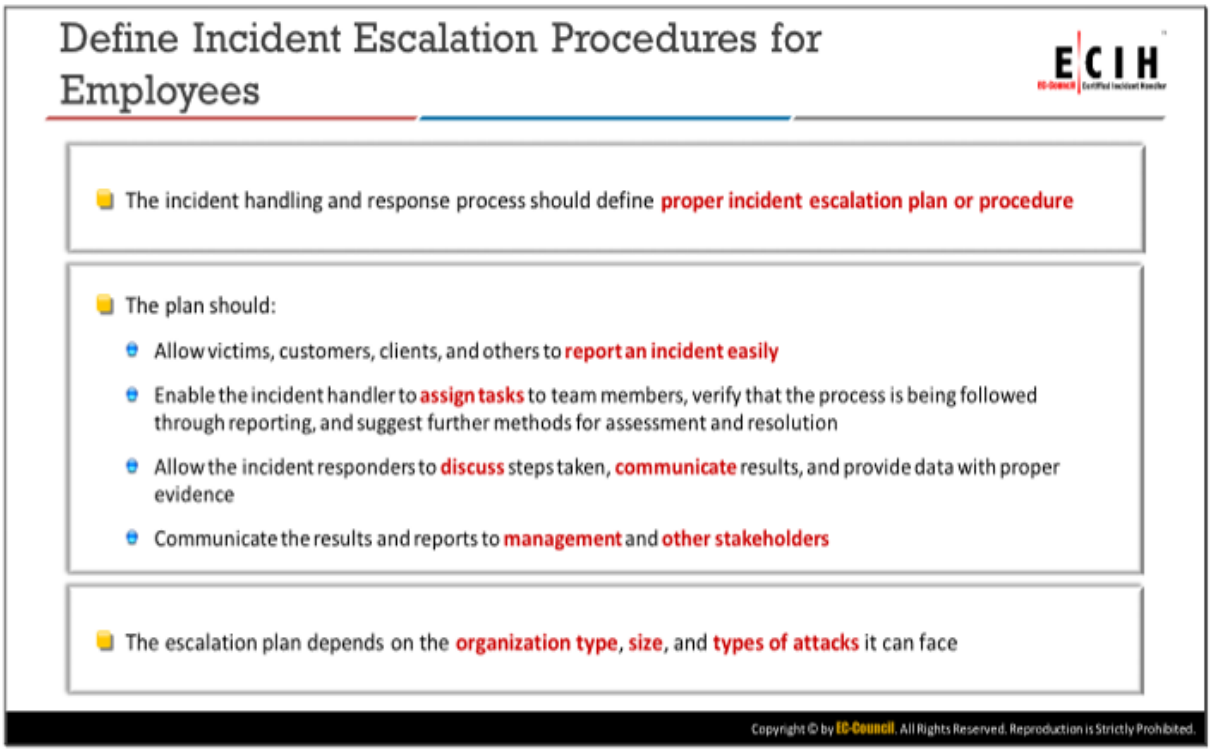
After preparation, the next step in the IH&R process is incident recording and assignment. This section discusses the process flow of incident recording and assignment, the incident escalation plan, the ticketing system, and role of IT support. Notably, incident recording and assignment is the phase in which the incident is noticed.



Process Flow of Incident Recording and Assignment

If an employee finds abnormal changes or indicators of an incident, then he or she should immediately cross-check his or her database to confirm the changes and inform help desk personnel, such as system or network administrators, about the situation. For our purposes, it is important to note here that a help desk consists of experienced incident handlers with years of experience. A help desk will accept such a request from an employee and conduct a preliminary examination to determine whether the employee is reporting a valid intrusion or breach from malicious sources. If the help desk finds that the incident did occur, then it will file a case for further enquiry. Next, it will try to determine whether the incident reflects any previous incidents and conduct further examinations. If the incident is found to mirror a previous incident, then the help desk will reopen the previously closed incident and update the incident record. Otherwise, it will record it by collecting information about the incident, such as security alerts and indicators from the IT department. This incident record is sent to the IR department for analysis and validation. If the IR department finds the incident to be valid, then it will immediately assign the IR team for further analysis.

The process flow of the incident recording and assignment phase is outlined in the figure shown on the above slide.

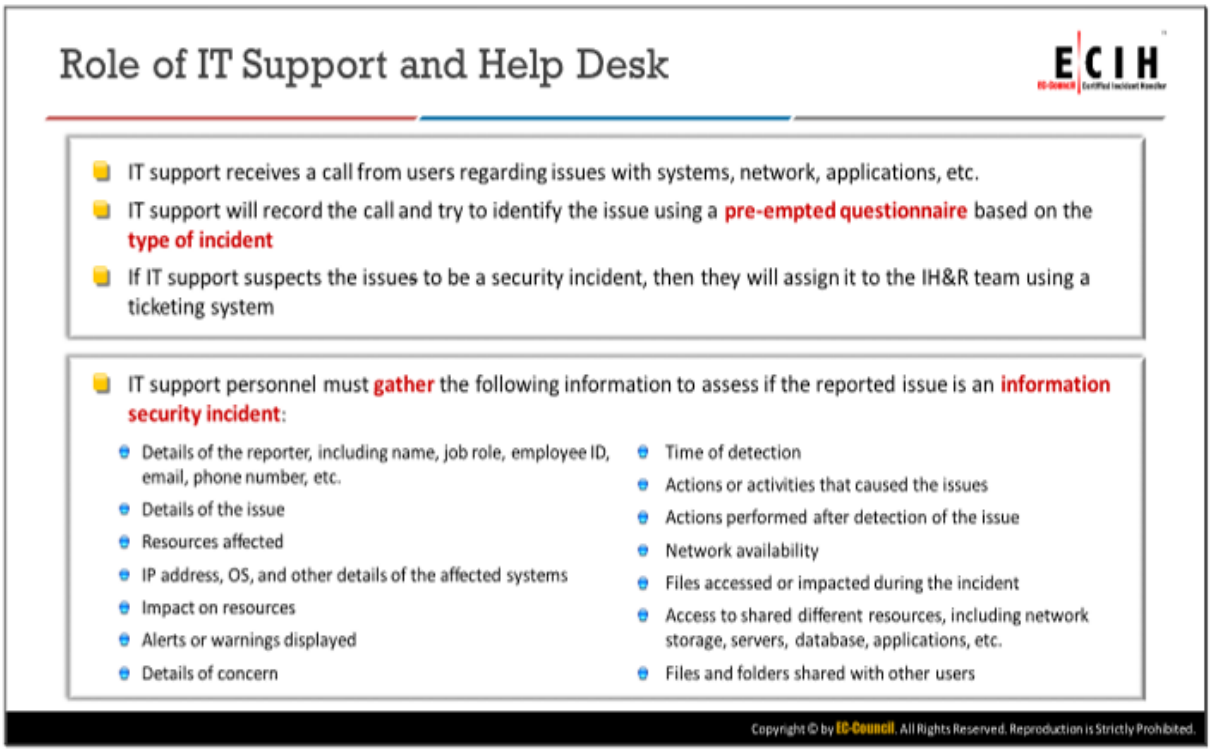


Define Incident Escalation Procedures for Employees

The IH&R process should define a proper incident escalation plan or procedure. The defined escalation procedure must satisfy the following objectives:

- Allow victims, customers, clients, and other people to easily report an incident
- Enable the incident handler to assign tasks to team members, verify process followed, obtain reports about progress, and suggest methods
- Allow the incident responders to discuss the steps, communicate the response results, and provide result data with proper evidence
- Communicate the result and report it to management and stakeholders

The escalation plan depends on each organization's type and size as well as the types of attacks it may face. Notably, the plan should be easy to implement and all employees should be able to easily follow it, even if they are not technically educated. If an incident does occur, the victims are the first to encounter any attack indicators; thus, employees should be trained about various indicators of compromise and the process of reporting them to a help desk or tech support.



Role of IT Support and Help Desk

When an employee finds abnormal issues with systems, networks, or applications, he or she should immediately call IT support to inform it of the issue. IT support will record the call and try to identify the issue using the prepared questionnaire designed for the specific type of incident. If IT support suspects the issue to be a security incident, then it will assign the issue to the IR team using a ticketing system.

Tech support or help desk personnel should analyze the event by interviewing the victim or reporting person for more details—this will help in assessing the incident type and in determining whether the victim accidentally accessed any triggers.

The help desk will send all report and interview details through a ticketing system to the incident handler, who will then assign a first responder from the IH&R team for analysis and validation. The first responder will analyze the compromised systems, network, databases, and other devices to validate the incident. Notably, this helps identify the compromised systems, networks, applications, services, and devices. The first responder will also list the compromised elements and convey all known incident details to the incident handler through the same ticketing system.

IT support personnel must gather the following information to assess whether a reported issue is an information security incident:

- Details of the complainant, name, job role, employee ID, email, phone number, and so on
- Details of the issue
- Resources affected

- IP address, OS, and other details of the affected systems
- Impact on resources
- Alerts or warnings displayed
- Details of concern
- Time of detection
- Actions or activities that caused the issues
- Actions performed after detection of the issue
- Network availability
- Files accessed or impacted during the incident
- Access to shared resources, including network storage, servers, databases, applications, files, and folders

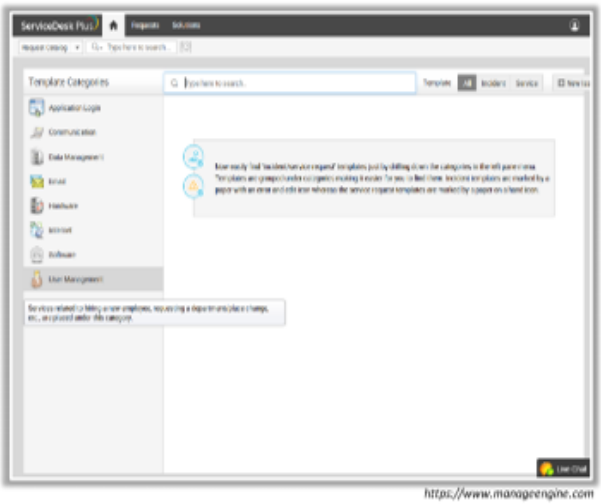
Ticketing System

- Issue tracking systems or ticketing systems simplify incident responses and handling processes by **tracking details of incidents**
- Organization must use the ticketing systems to keep track of all incident response activities
- Some commonly used ticketing systems include ManageEngine ServiceDesk Plus, osTicket, SolarWinds MSP, etc.

Advantages of using ticketing systems:

- Generates tickets automatically on discovering suspicious patterns from firewall, IDS, and SIEM
- **Systematically collects** details about the incident
- Helps in assigning priority to incidents based on the compromised system, type of incident, etc.
- Alerts the responsible persons and distributes tasks automatically
- Stores details of the incidents, solutions, and results

ManageEngine ServiceDesk Plus is a comprehensive ticketing system employed by various IT security teams across companies



https://www.manageengine.com

Ticketing System (Cont'd)

AlienVault OSSIM

This open source **security information and event management system** is integrated with a selection of tools designed to aid incident handlers in handling and responding to security incidents

https://www.alienvault.com

- **osTicket** https://github.com
- **SolarWinds MSP** https://www.solarwindsmsp.com
- **IR-Flow** https://www.syncurity.net
- **Request Tracker for Incident Response (RTIR)** https://bestpractical.com
- **IBM Resilient Incident Response Platform** https://www.ibm.com

Ticketing System

Organizations can use issue tracking systems or ticketing systems to simplify the IH&R process. "Tickets" are requests made by users regarding different issues. In an IR scenario, tickets represent suspicious events observed by users across networks, applications, systems, and devices.

A ticketing system also helps in tracking the event, victim, damage, time taken to solve the issue, members allocated, methods implemented in finding a solution, and so on. It also helps in maintaining communication between IH&R team members and simplifying the process of seeking permissions from relevant authorities by presenting the details saved on a ticker.

If a user raises a ticket upon observing an issue with the system, then the system will automatically send the ticket to the help desk and the system administrator. Help desk personnel will look after the issue, and if they qualify it as an incident, they will use the raised ticket to seek permission from the administrator to initiate a validation process. If the issue turns out to be an incident and thus requires the response of the IH&R team, then the help desk will forward the ticket to the IR team along with concerned authorities, such as the IH&R team, victim, and other pre-defined members. This process will go on until the assigned member closes the ticket after solving the issue.

Notably, the assigned IH&R team will examine the system, collect evidence and artifacts for forensics analysis, scan other systems to locate other victim devices, and follow an appropriate containment plan. The team will enter the results of each stage of the investigation into the ticketing system, which will communicate results to concerned members of management and stakeholders along with the incident handler. The team will use various eradication methods to prevent the occurrence of similar attacks in the future.

The IR team will also be responsible for recovering any damaged devices, systems, and data to maintain business continuity. It is the responsibility of the IH&R team to update the details of the IR process followed in the ticketing platform. Meanwhile, the incident handler is responsible for analyzing the reports and suggesting upgrades, replacements, and any updates required for various devices across the organization to prevent the re-occurrence of such incidents.

Details saved in a ticket include:

- Issues, errors, and vulnerabilities observed
- Systems or devices showing suspicious signs
- Time of observation and reporting
- Email IDs used for reporting
- Names of the reporting person and the assigned members in charge of solving the issue
- Methods applied to solve the issue and their respective results
- Statistical analysis of tickets

Advantages of using a ticketing system:

- Automatically generates tickets upon discovering suspicious patterns from a firewall, IDS, and/or SIEM
- Systematically collects details about an incident
- Helps in assigning priority to incidents based on the compromised system, type of incident, and so on

- Alerts the responsible persons and automatically distributes tasks
- Stores details of the incidents, solutions, and results
- Helps to create a chain of custody and documents for reports
- Ensures proper and timely IR
- Stores details of costs incurred in the IR process

Organizations should install and implement ticketing systems to keep track of the progress of IH&R processes. The following ticketing tools may help organizations perform ticketing in incident management: ManageEngine ServiceDesk Plus and AlienVault OSSIM.

- **ManageEngine ServiceDesk Plus**

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

  A comprehensive ticketing system employed by various IT security teams across global companies. It is effectively used in incident management, problem management, change management, and IT project management applications. ManageEngine ServiceDesk Plus is very well-known for employing recent technologies, such as automation and artificial intelligence, in its ticketing systems.

- **AlienVault OSSIM**

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

  OSSIM (Open Source Security Information Management) is an open source security information and event management system integrated with a selection of tools designed to aid incident handlers in handling and responding to security incidents. In OSSIM, a ticket serves as a tracking tool that contains information about detected alarms or any other issues that need to be managed in a workflow. These tickets help incident handlers to track the progress of an issue and guide their investigations of the issue. This tool also provides an audit trail to track the events, actions, and progress of the issue.

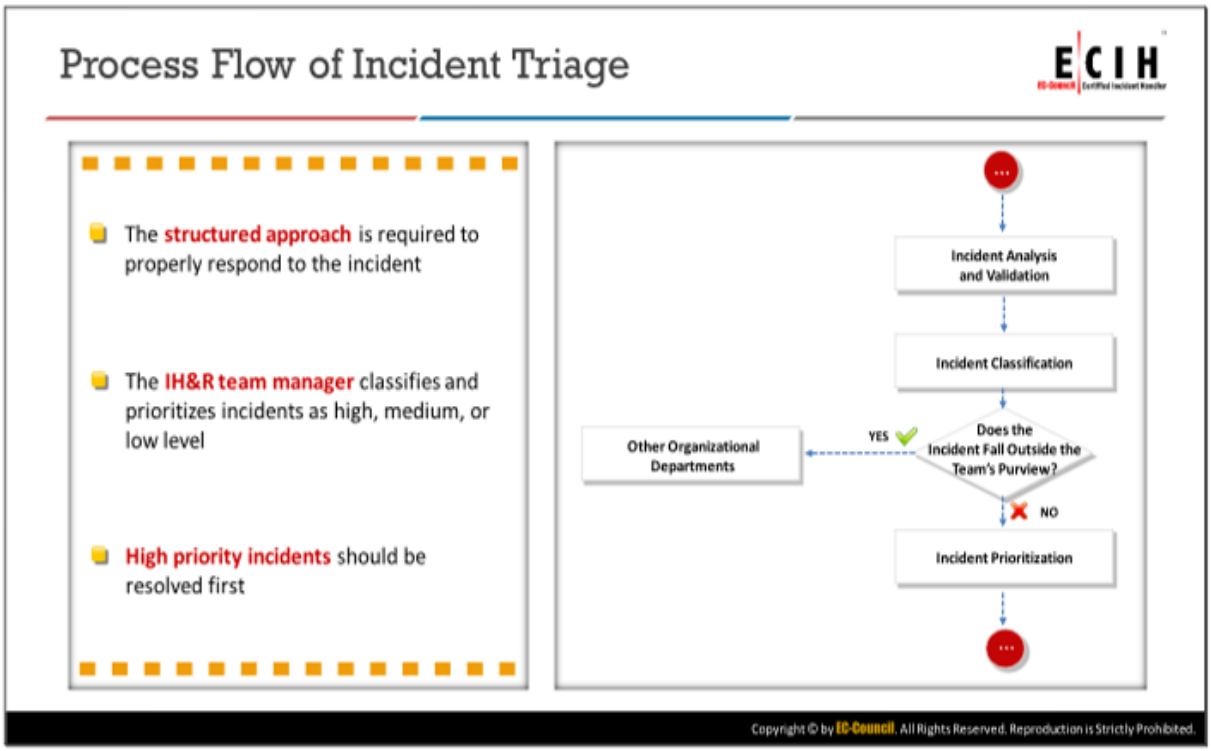
A few more good examples of IT ticketing software are listed below:

- osTicket (*https://github.com*)
- SolarWinds MSP (*https://www.solarwindsmsp.com*)
- IR-Flow (*https://www.syncurity.net*)
- Request Tracker for IR (RTIR) (*https://bestpractical.com*)
- IBM Resilient IR Platform (*https://www.ibm.com*)
- Freshdesk (*https://freshdesk.com*)

Step 3: Incident Triage

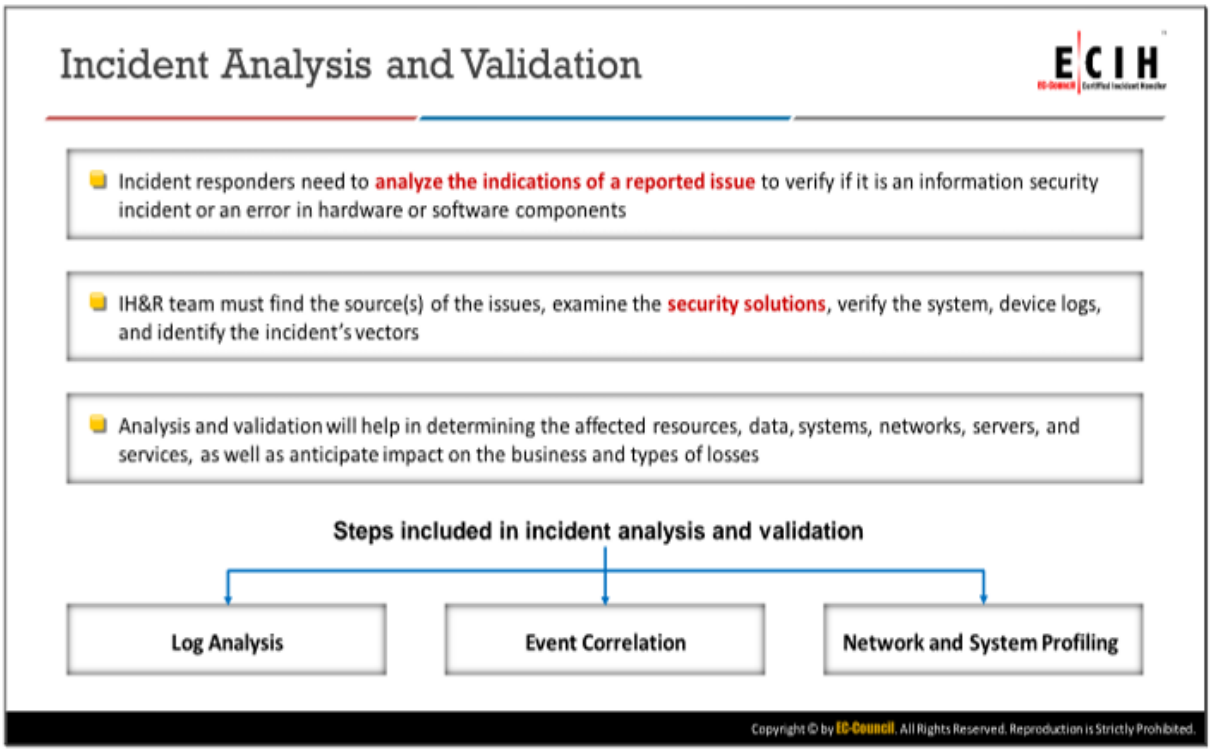
After incident recording and IH&R team assignment, an IH&R team is responsible for taking over and analyzing the incident with critical reasoning and good judgment. As noted above, an IH&R team should have a structured approach for efficiently responding to an incident. Along these lines, an IH&R team manager should classify and prioritize incidents based on their risk level (high, medium, or low). The team should classify incidents and first attend to high-priority incidents, then medium-priority incidents, and finally low-priority incidents.

This section discusses the process flow of incident triage, incident analysis and validation, incident classification, and incident prioritization.



Process Flow of Incident Triage

An IR team will first assess the incident's details and correlate indicators with logs and other system files to validate the incident and determine any impacted systems, networks, devices, and applications. The team will then classify the incident by its type. A notable classification method involves the comparison of standard criteria, such as networks performance, system behavior, logs, event correlation, data packets, network traffic, files, and applications, before and after the incident. Depending on the impacted resources or source of compromise or tools used in the attack, the IH&R team will also classify the incident as either an endpoint, network, malware, application, or browser incident. Next, the IH&R team manager will prioritize the incidents based on their risk level (high, medium, or low) as described above. The prioritization depends on the severity of the impact and its effect on the business. Other factors that impact classification include the nature of the incident, the criticality of the systems impacted, the number of systems impacted, and the legal and regulatory requirements with which the IH&R process must align. If the incident falls outside the IH&R team's purview, then the team must contact other organizational departments. The complete process flow of incident triage is displayed in the figure shown on the above slide.



Incident Analysis and Validation

Incident responders need to analyze the indicators of a reported issue to verify whether it is an information security incident or a hardware or software error. The team should ideally evaluate each indication to determine its legitimacy. They must find the different sources of all indicators, examine available security solutions, verify the system and device logs, and identify the incident and its vectors. Even if an indication is accurate, this does not necessarily mean that an incident has occurred—not every incident is a security incident; some incidents, such as a web server crash or the modification of sensitive files, may be due to human error. Incident analysis helps in determining if an incident needs to be handled or registered by the IR team, if no further action is required, or if it should be passed off to other teams for processing.

The IH&R team must then perform various validation activities to determine the attack details such as type, vectors, duration, source, and evidence. Analysis and validation also help in determining the affected resources, data, systems, networks, servers, and services; impact on the business; and different types of losses. The IH&R team can use this data to classify and prioritize the incidents.

Some of the steps involved in incident analysis and validation to verify data modification are listed below:

- **Log Analysis**

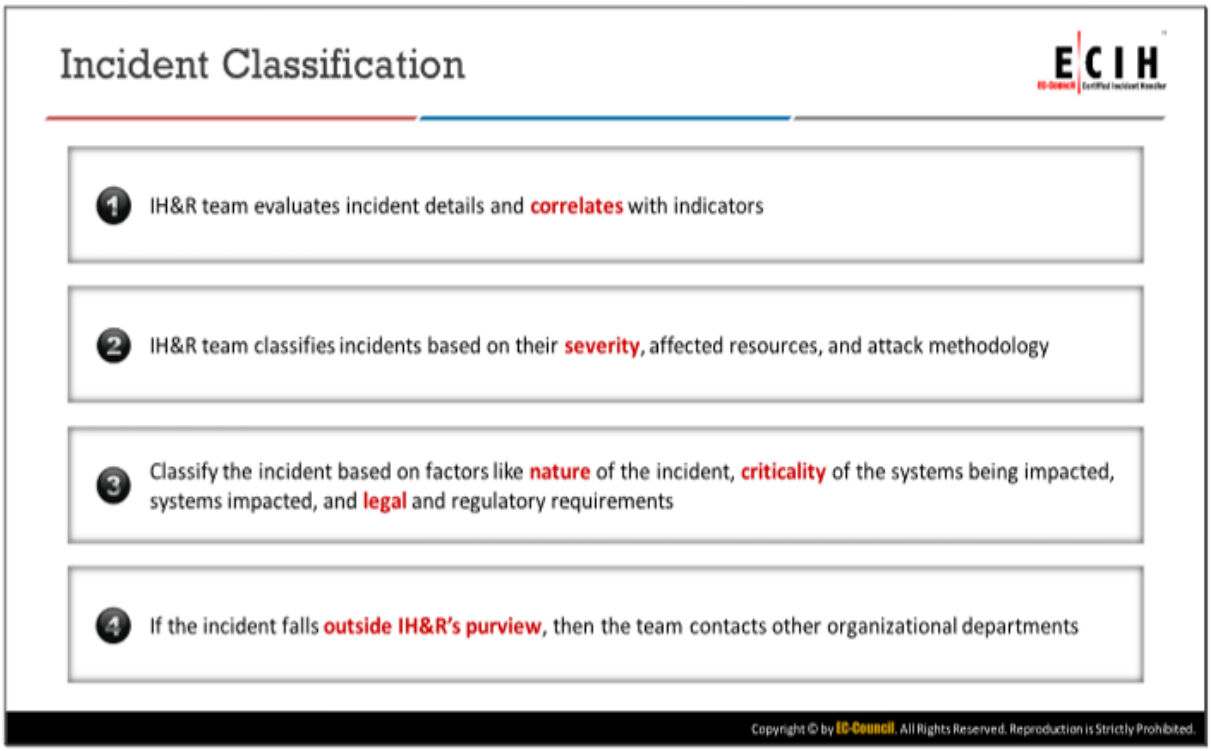
  Information related to the incident might be available in several places such as IDPS, firewall, application, and router logs. Accordingly, logs should be deployed from centralized logging servers and logging devices to gain duplicates.

- **Event Correlation**

  Event correlation is a technique used to assign new meanings to relate a set of events that occur in a fixed amount of time. Several logs may evidence an incident—for example, a firewall log may reveal an IP address while an application log may reveal a username. Using event correlation, the IR team can identify the relation between all available information.

- **Network and System Profiling**

  Profiling is the process of identifying the changes made to the various characteristics of expected activity. Monitoring network traffic and bandwidth, checksums of critical files, and file integrity are some of examples of profiling.

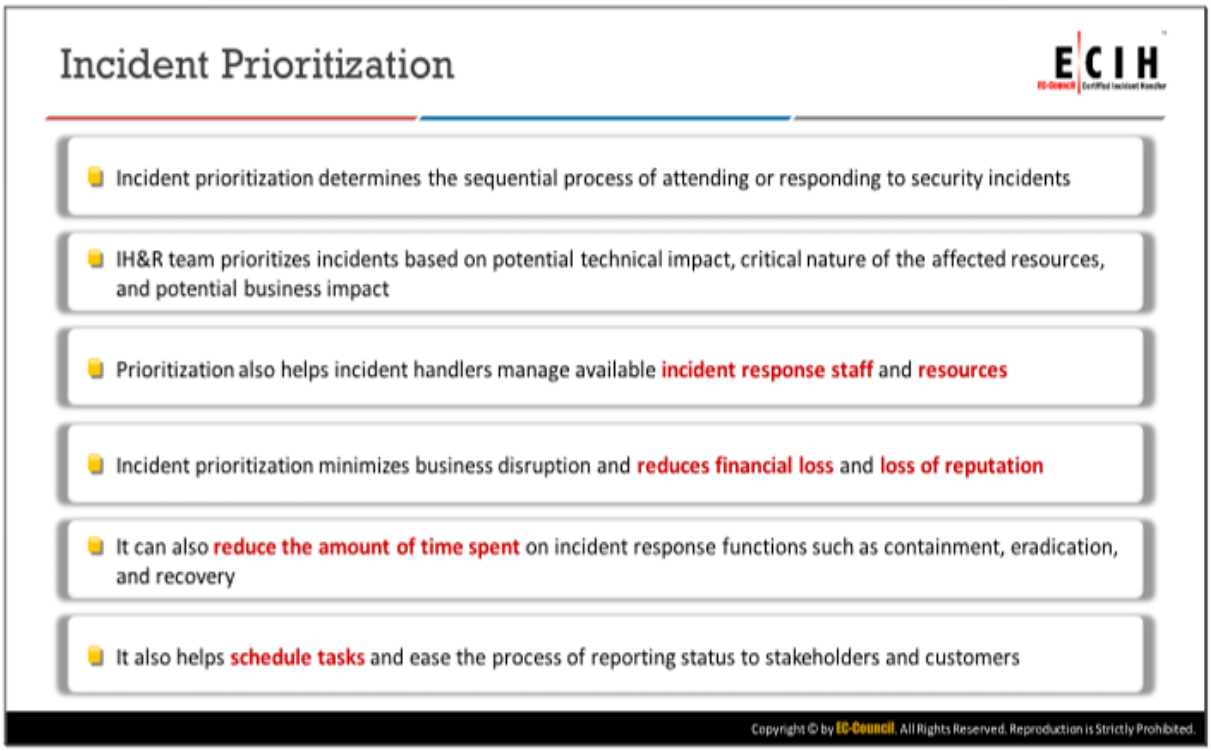


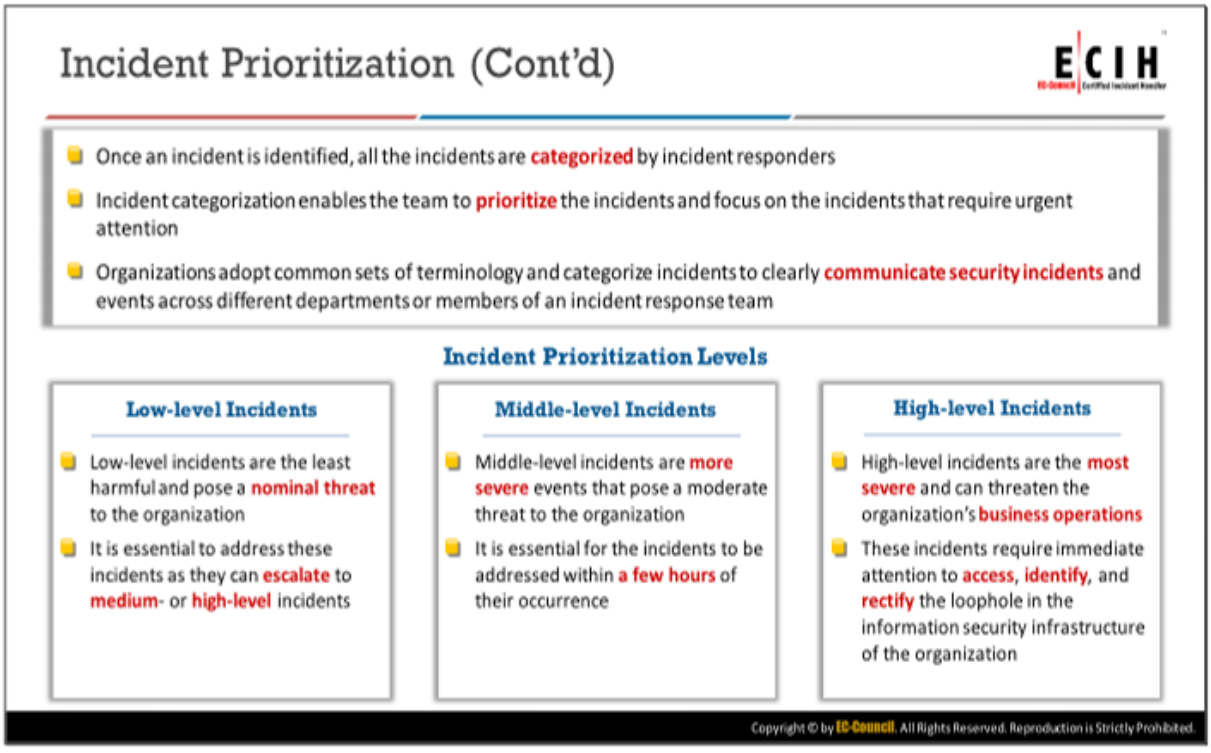
Incident Classification

The classification of an incident depends on its potential targets and the severity of its impact. The purpose of incident classification is to gather all information required to determine its category and the time required for its resolution, to name but only a few of the criteria necessary to collect for effectively responding to an incident.

In this stage, an IH&R team must:

- Evaluate incident details and correlate them with indicators
- Classify incidents based on:
  - Nature of the incident
  - Criticality of the systems impacted
  - Number of systems impacted
  - Legal and regulatory requirements
  - Severity
  - Affected resources
  - Attack methodology
- Contact other organizational departments if the incident falls outside the IH&R team's purview





Incident Prioritization

Incident prioritization is the most critical decision in the IH&R process: to. Be sure, incidents must not be handled on a first-come, first-served basis. Instead, incident prioritization determines the sequential process by which a team attends to security incidents. More specifically, an IH&R team prioritizes incidents by prioritizing incidents with the highest business impact to enable the organization to continue to offer business services and reduce financial losses during or in the wake of an incident.

This prioritization must depend on the severity of the impact, the importance of the compromised resources, the operations disrupted, and the losses incurred due to the incident. It is the responsibility of the incident handler to prioritize the compromised elements and sort them according to the most important devices or applications required for business continuity. Next, the incident handler assigns a team to respond to the incident and suggests methods for detection and containment based on the impact of the incident.

Prioritization will also help incident handlers to manage the available IR staff and resources. The incident handler assigns the level of priority, predefined criteria, requirements, and urgency related to restoring the compromised resource. As already suggested, working on the most severe incidents first enables the organization to minimize business disruption and financial and reputational losses. Moreover, this style of prioritization can also reduce the amount of money and time spent on IR functions, such as containment, eradication, and recovery. On another note, prioritization also helps in scheduling tasks and easing the process of reporting the status of the incident response to stakeholders and customers.

With the emerging number of diverse cybersecurity incidents, assigning a priority category to an incident has become an essential step in the incident management process—as soon as an incident is identified in an organization, an incident responder will categorize it. Helpful to note here is that organizations have adopted a common set of terminology and tend to categorize incidents in ways that enable them to clearly communicate security incidents and events across different departments. While, as noted above, incidents are generally categorized according to their severity or origin, organizations may also develop their own set of categories to distinguish between different security incidents.

Incident priorities are mainly categorized into the three following levels:

- **Low-level Incidents**

  Low-level incidents are the least harmful incidents that pose a nominal threat to an organization. At times, a reported low-level incident may not be severe but still have the potential to act as a predecessor for other major security incidents. Accordingly, it is essential to address low-level incidents to prevent them from escalating to medium- or high-level incidents. Thus, although such incidents have a negligible impact on a business, they should always be resolved by incident responders within one working day. During low-level incidents, services to users and customers continue at their regular pace, but the organization loses efficiency.

  Low-level incidents are identified by the following symptoms:

  - Loss of personal password
  - Unsuccessful scans and probes in the network
  - Request to review security logs
  - Presence of computer virus or worm
  - Failure to download antivirus signatures
  - Suspected sharing of an organization's accounts

- Minor breaches of an organization's acceptable usage policy
- Compromised system password
- Unknown sharing of an organization's account
- Misuse of computer peripherals

- **Middle-level Incidents**

  Middle-level incidents are more severe events that pose a moderate threat to an organization. Such incidents require further investigation by incident handlers to analyze their impact and severity. These incidents can result in a false positive and may interrupt organizational operations to some extent. It is essential for incident handlers to handle such incidents within few hours of their detection. During middle-level incidents, organizations may be unable to provide essential services to a group of system users for a certain period of time; this may be slightly inconvenient for customers.

  Middle-level incidents are identified by the following symptoms:

  - Inactive external/internal unauthorized access to systems
  - Unfriendly employee termination
  - Access violation during an attempt to access the computer or network equipment as a super user
  - Unauthorized data storing and processing
  - Destruction of property related to a computer incident
  - Localized virus/worm outbreak
  - Personal theft of data related to a computer incident
  - Computer virus or worm of comparatively large intensity
  - Illegal access to buildings
  - Breach of an organization's acceptable usage policy

- **High-level Incidents**

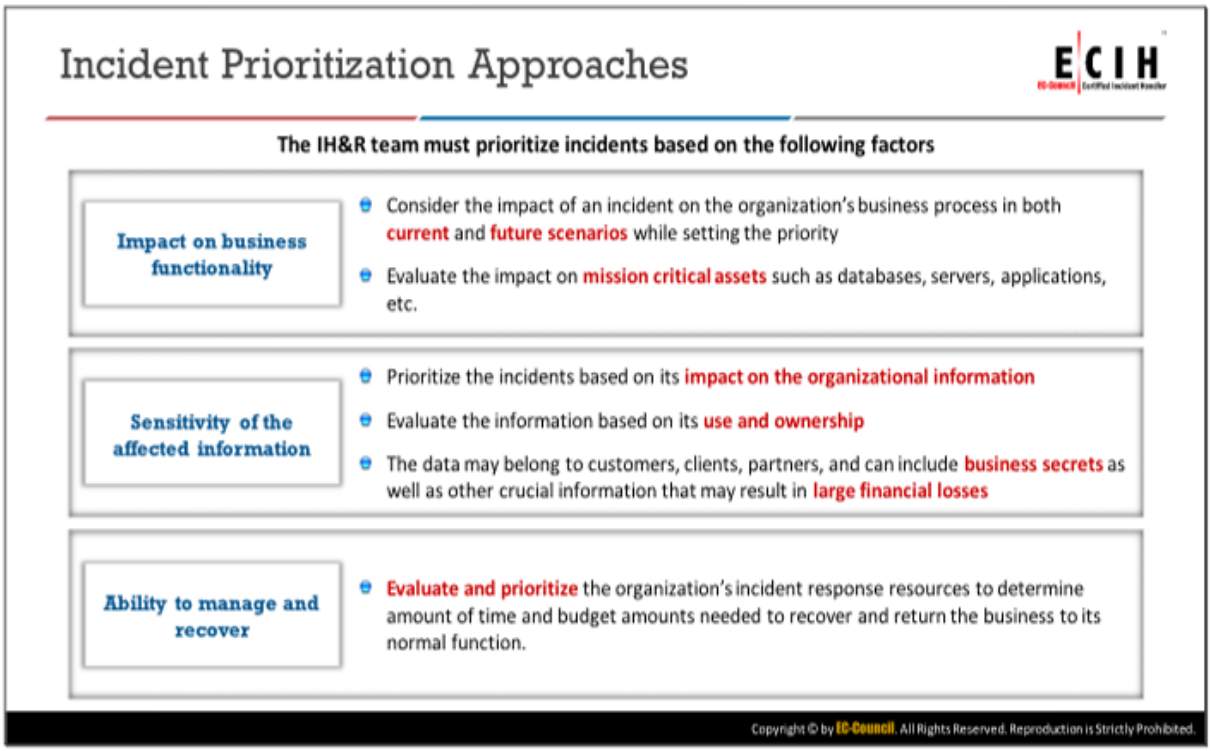
  High-level incidents are the most severe kind of incident that can threaten an organization's business operations. Such incidents are reported to the computer security officer for comprehensive cybersecurity planning and are handled by IR teams on an urgent basis. These incidents require due attention to access, identify, and rectify the loophole in the information security infrastructure of the organization. High-level incidents can have a huge impact on the services an organization provides to a large number of customers; moreover, such incidents often interrupt business and may greatly impact an organization's finances.

  The following are generally identified as high-level incidents:

  - Denial-of-service attacks

- Suspected break-in in any company computer
- The presence of harmful viruses, worms, and trojan horses capable of causing serious data corruption or loss
- Unauthenticated modifications to system hardware, firmware, and software
- Destruction of property exceeding $100,000
- Personal theft exceeding $100,000, including illegal electronic fund transfers or downloads/sales
- Any kind of pornography (child pornography is a severe crime), gambling, or violation of any law
- Abnormal changes in hardware, software, and firmware systems
- Illegal file downloads by the suspected user or unknown users
- Illegal downloads of music, videos, software, and any other copyrighted materials
- Violations of cyber law (this a cybercrime that can lead to legal action)
- Cyber terrorism

Apart from these elements, other incidents may fall into the category of high-level incidents if judged as such by a cybersecurity officer; these include: the illegal use of computers and related equipment, unintended actions, and scans and probes into the network.



Incident Prioritization Approaches

The IH&R team must prioritize incidents based on the following factors:

- **Impact on Business Functionality**

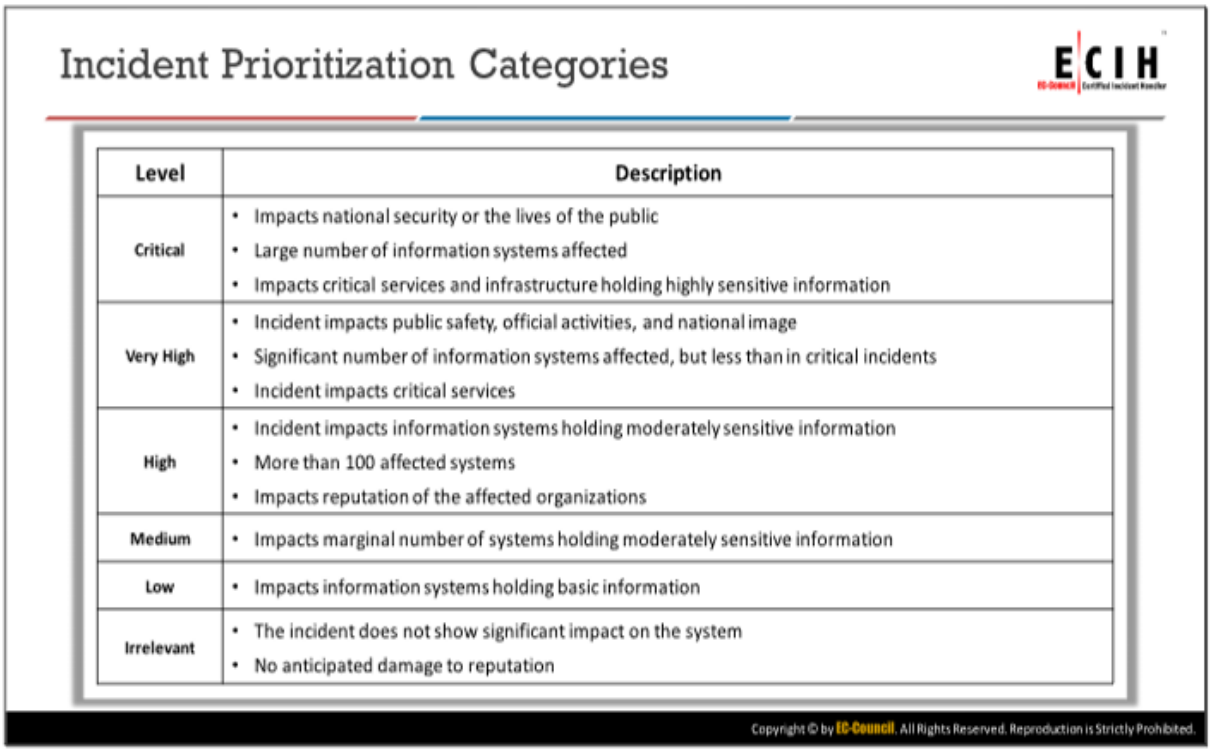
  IT system incidents generally impact the functionality of the business and therefore negatively impact the users of affected systems. IH&R teams should consider how an incident affects business continuity and the functionality of compromised systems. Notably, when assigning incident priority, they must consider the incident's impact on an organization's business process from both current and future perspectives while carefully evaluating the incident's impact on business-critical assets such as databases, servers, and applications.

- **Sensitivity of the Affected Information**

  Incidents, such as those involving sensitive data exfiltration by a malicious agent, affect the confidentiality, integrity, and availability of organizational information. IH&R teams must prioritize incidents based on their impact on organizational information and evaluate this information based on its use and ownership—such data may belong, for example, to customers, clients, or partners and can include business secrets and other crucial information that may result in huge financial losses.

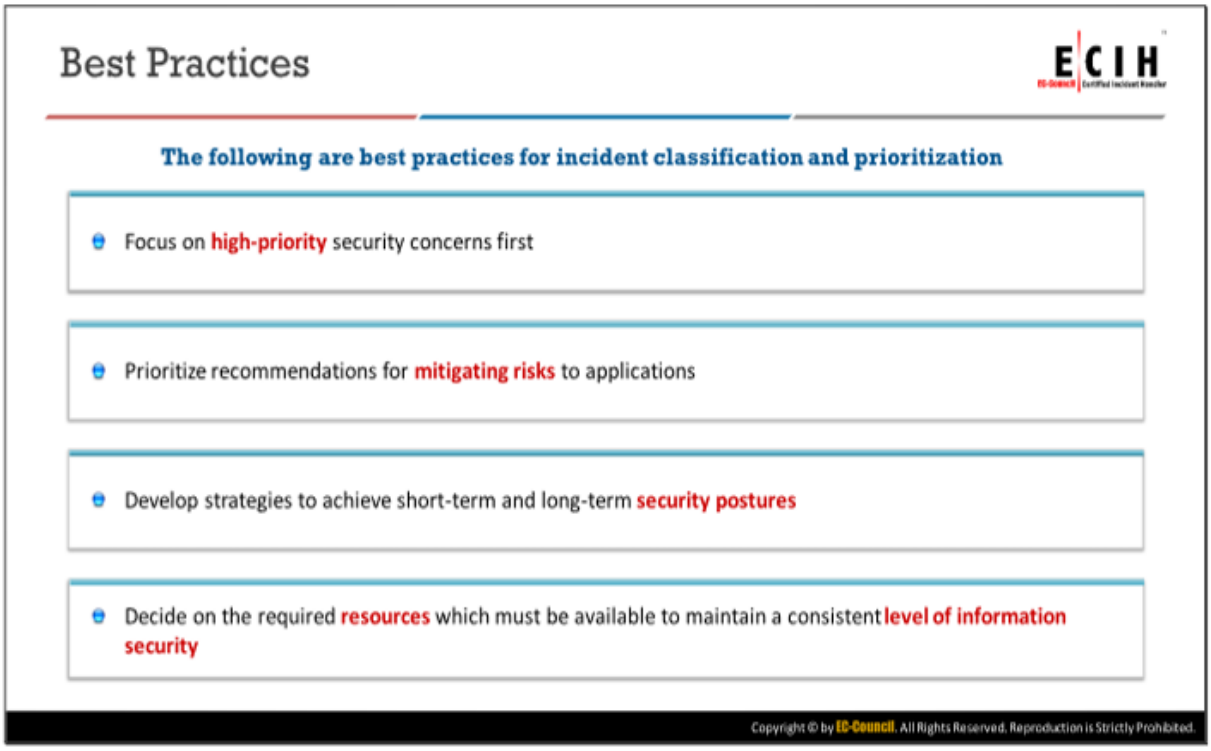
- **Ability to Manage and Recover**

  The size and amount of data and resources affected by the incident determines the amounts of time and other resources required to recover from the incident. IH&R teams must prioritize the incident based on the resources required to return the business to its normal functionality.



Incident Prioritization Categories

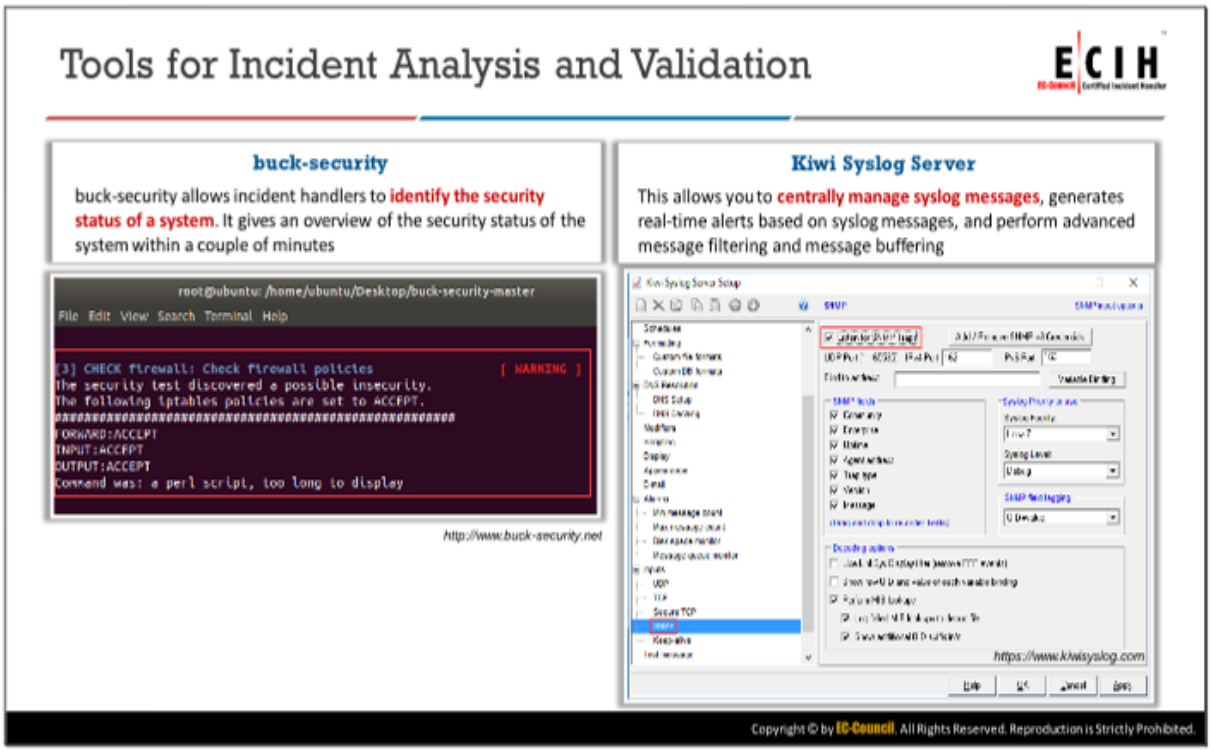
The table shown on the above slide outlines incident categories/levels of severity.

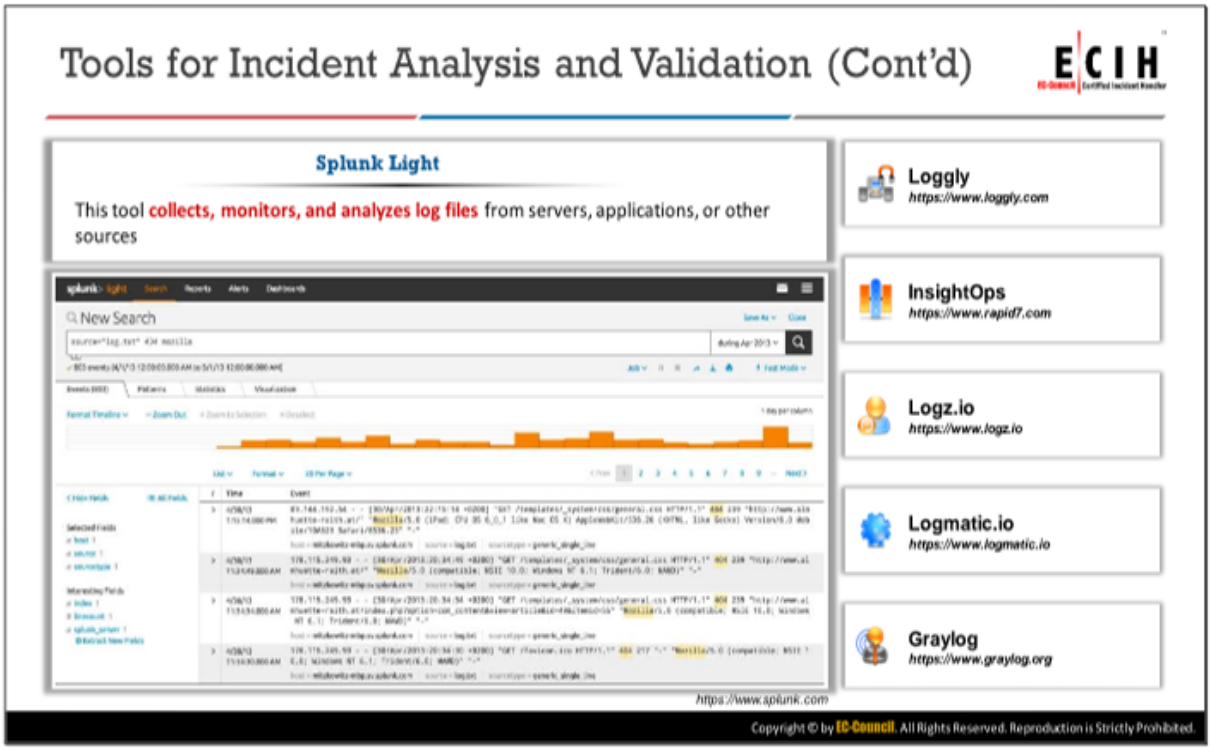


Best Practices

The best practices for incident classification and prioritization that IH&R teams should follow are listed below:

- Focus on high-priority security concerns first
- Prioritize recommendations for mitigating risks to applications
- Develop strategies to achieve short-term and long-term security postures
- Decide on required and available resources to maintain a consistent level of information security





Tools for Incident Analysis and Validation

Incident analysis and validation tools help incident handlers perform security scans to capture logs from various network systems and devices to analyze and detect malicious activities related to security incidents.

Some important tools used for incident analysis and validation are listed below:

- **buck-security**

  Source: *http://www.buck-security.net*

  buck-security is a collection of security checks for Linux. It was designed for Debian and Ubuntu servers but remains useful for any Linux system. It allows incident handlers to identify the security status of a system; notably, it provides an overview of the security status of a system within a couple of minutes.

- **Kiwi Syslog Server**

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

  The Kiwi Syslog Server is a centralized and simplified log message management tool that can be used across various network devices and servers. It is used to centrally manage syslog messages, generate real-time alerts based on syslog messages, and perform advanced message filtering and message buffering. It collects syslog messages, SNMP traps, and Windows event log data from IT infrastructure. Moreover, it monitors logs in real time through a secure and intuitive web interface.

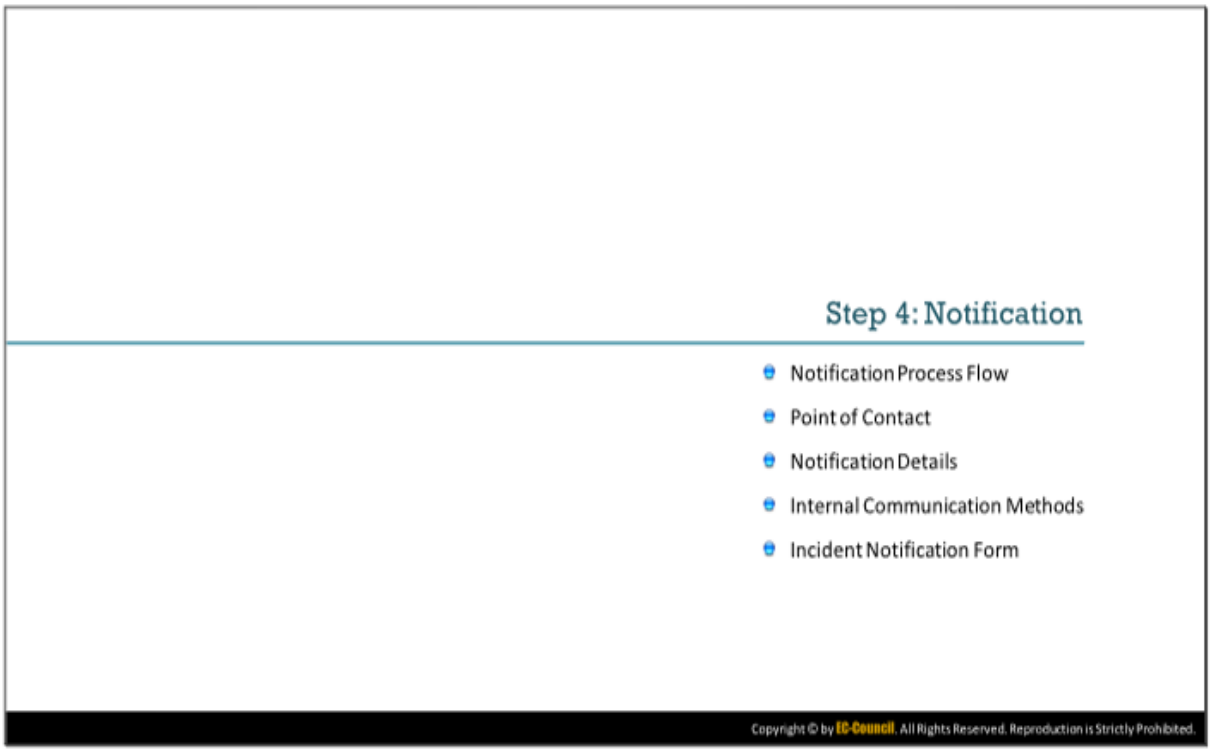
- **Splunk Light**

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

  Splunk Light is a tool for collecting, monitoring, and analyzing log files from servers, applications, or other sources. The tool collects data from multiple sources and performs indexing, monitoring, reporting, and notification services. Alerts from Splunk Light can automatically trigger actions, such as sending automated emails, executing remediation scripts, or posting RSS feeds. Moreover, Splunk Forwarders collect data that is not available over the network or visible to the server on which Splunk software is installed to deliver reliable, secure, and real-time universal data collection for tens of thousands of sources.

Some additional tools used for incident analysis and validation are listed below:

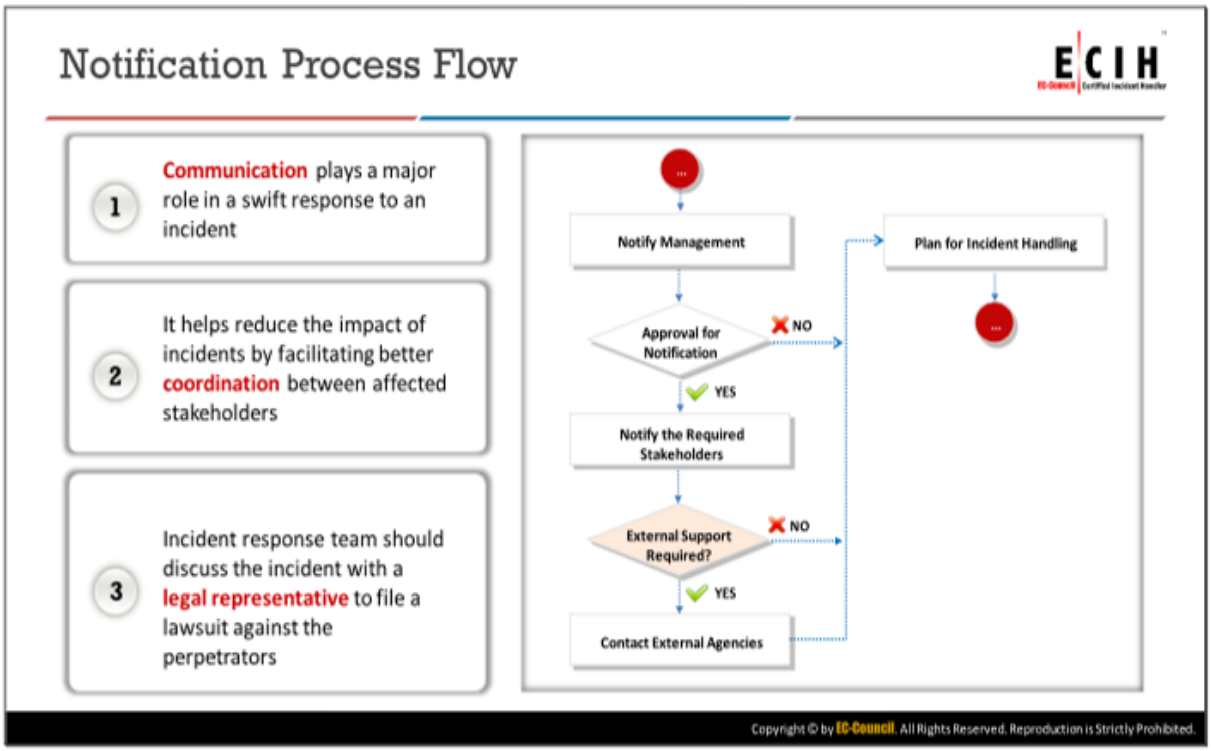
- Loggly (*https://www.loggly.com*)
- InsightOps (*https://www.rapid7.com*)
- Logz.io (*https://www.logz.io*)
- Logmatic.io (*https://www.logmatic.io*)
- Graylog (*https://www.graylog.org*)



Step 4: Notification

After completing the incident triage phase, the IH&R team will be aware of the possible incident. An organization hit by a security incident needs to notify the appropriate internal and external personnel to minimize the repercussions of the security event. This notification can save valuable assets from becoming vulnerable and help individuals within the organization to play their corresponding roles. In such a time, cooperation can reduce the complexity and magnitude of resolving the security threat or incident.

This section discusses the process flow of notification, point-of-contact, details about which to notify stakeholders, and internal communication methods. It also offers a sample notification form.



Notification Process Flow

Communication plays a major role in enabling an organization to swiftly respond to an incident. It also helps reduce the impact of an incident by facilitating better coordination between different stakeholders affected by the incident. Communicating the initial response process and results to IH&R team members crucially helps them understand the type of response required and their responsibilities in handling the incident. The detailed process flow of notification is displayed in the figure shown on the above slide.

Incident handlers or responders must communicate the severity of the incident to management or authorized persons to gather relevant approvals for performing IR procedures. Such communications would include details of the first report, initial processes performed to assess the situation, detection methods applied, impacted resources, and management strategy. The IH&R team should also discuss the incident with a legal representative and the organization should file a lawsuit against the perpetrators.

After obtaining the approval, the IH&R team should communicate any matters related to the incident to necessary stakeholders. Meanwhile, as noted above, all employees and other stakeholders must communicate with their IH&R team whenever they suspect a security breach. The IH&R team lead should discuss any breaches with core team members and other members of the organization to effectively handle the incident. Incident handlers can also communicate part of the situation to an external party after approvals from management if they require external support to handle the incident.

After controlling and mitigating the incident, the IR team can disseminate the details of the incident and lessons learned from it across the organization and to media to create awareness. Although it depends on the circumstances of an incident, the typical goal of a response strategy is to examine the most appropriate response procedure. The response plan should consider the

political, technical, legal, and business factors caught up in the incident; to be sure, a response strategy generally depends on the circumstances of the incident.

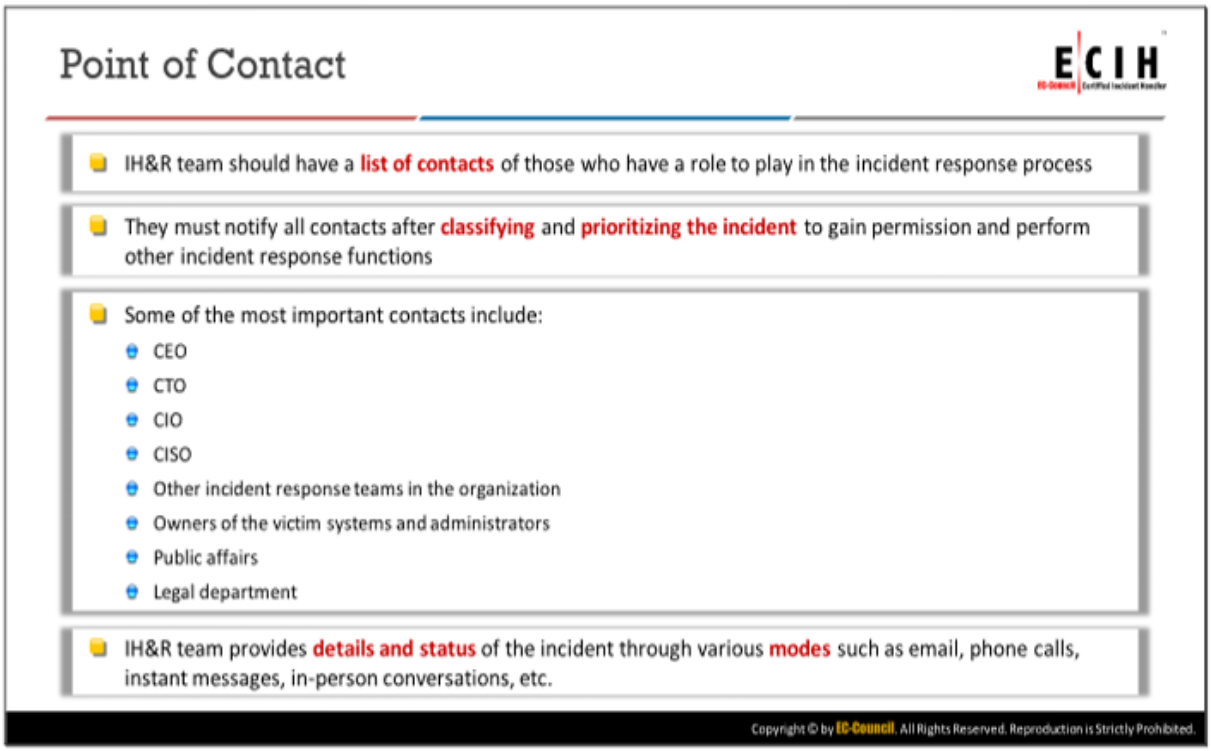
The factors that affect the resources required to investigate an incident include:

- Forensic duplication of related computer systems
- Criminal referral
- Civil litigation

Relatedly, key questions to ask in unpacking an incident include:

- What is the range of impact of the incident on systems?
- How sensitive is the compromised or stolen information?
- Who are the attackers?
- Is the public aware of the incident?
- What unauthorized level(s) of access have the attackers gained?
- What are the attackers' skills?
- What was the total downtime for the system and the user?
- What was the total loss in dollars?

The information gathered during the initial response is important for selecting a response strategy; however, before selecting a response strategy, IH&R teams should reinvestigate the details of the incident.



Point of Contact

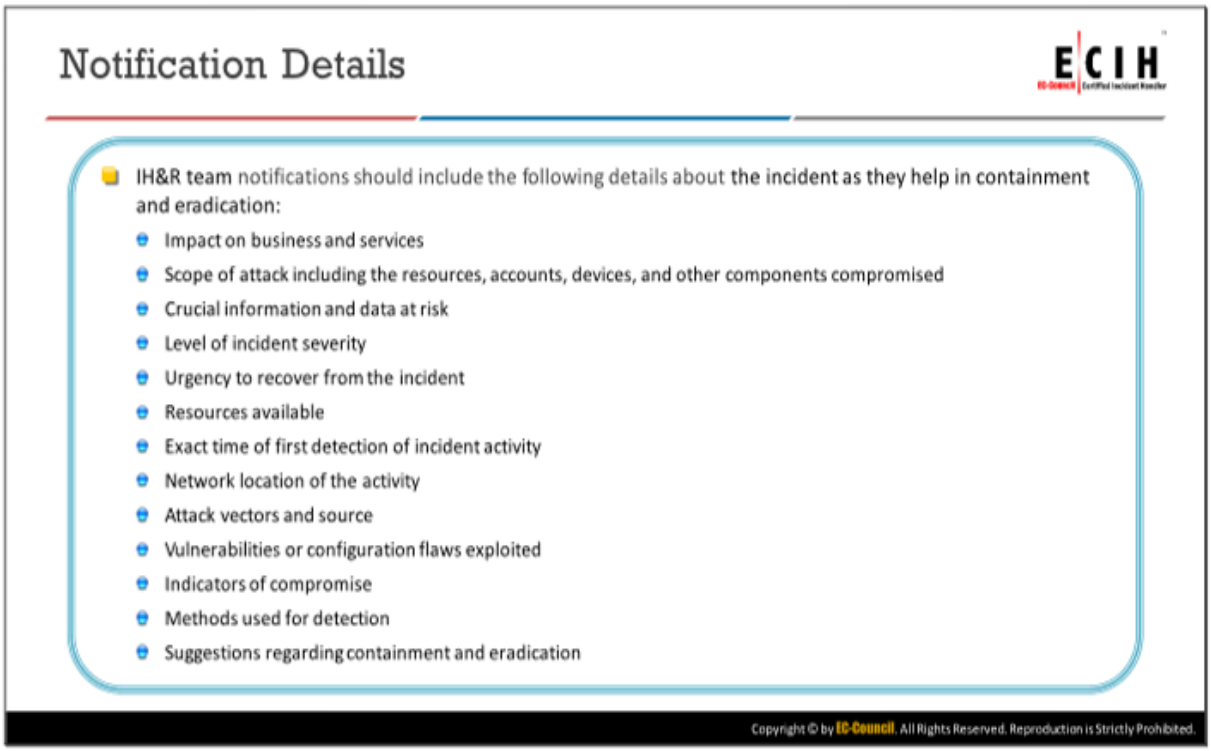
"Point of contact" refers to the personnel the IH&R team must contact to report an incident and obtain necessary permissions. The organization must assign a certain senior level employee with decision-making power as the point of contact for details such as incident severity and priority.

Organizations must ensure that their IH&R teams have a list of contacts who play a role in the IR process. They must notify all such contacts after classifying and prioritizing an incident to gain permission and perform other IR functions.

Some of the most important contacts include:

- CEO
- CTO
- CIO
- CISO
- Other IR teams in the organization
- Owners of the victim systems and administrators
- Public affairs
- Legal department

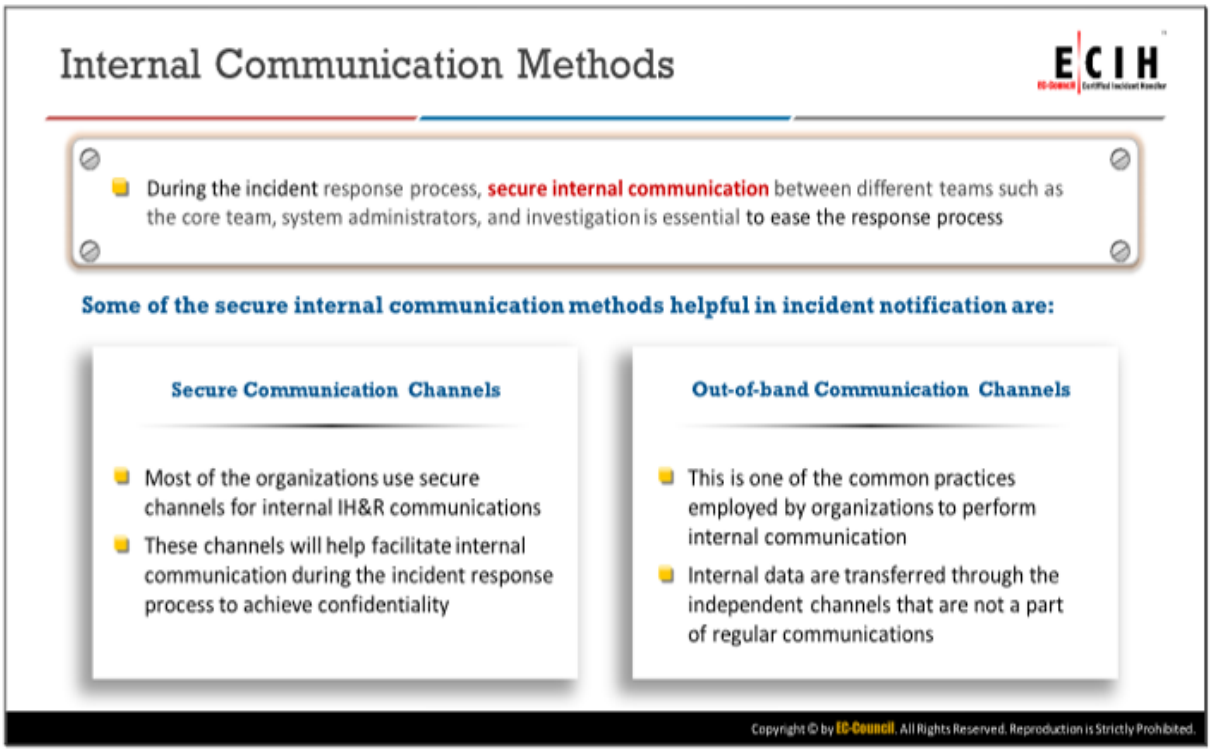
An IR team can provide details about and the status of the incident through various modes of communication such as email, phone calls, instant messages, and in person; therefore, the list must include the aforementioned details of the personnel required to facilitate such communication. Although responders can relate preliminary information with informal means, they must use a written document or report to obtain permissions from the assigned authorities.



Notification Details

An IH&R team should notify stakeholders about the following incident details to facilitate containment, eradication, and the granting of required permissions:

- Impact on business and services
- Scope of attack, including the resources, accounts, devices, and other components compromised
- Crucial information and data at risk
- Level of incident severity
- Urgency with which the organization must recover from the incident
- Resources available
- Exact time of detecting the first incident activity
- Network location of the activity
- Attack vectors and source
- Vulnerabilities or configuration flaws exploited
- Indicators of compromise
- Methods used for detection
- Suggestions regarding containment and eradication



Internal Communication Methods

Internal communication is a key requirement not only in the notification phase but also in every phase of IR process—planning, investigation, detection, and recovery. During the response process, different teams within the organization, such as the IH&R core team, system administrator team, investigation team, and management team, work simultaneously. Internal secure communication between these teams is essential for easing the response process. Organizations must make sure that the right information is communicated to the desired person or team at the right time.

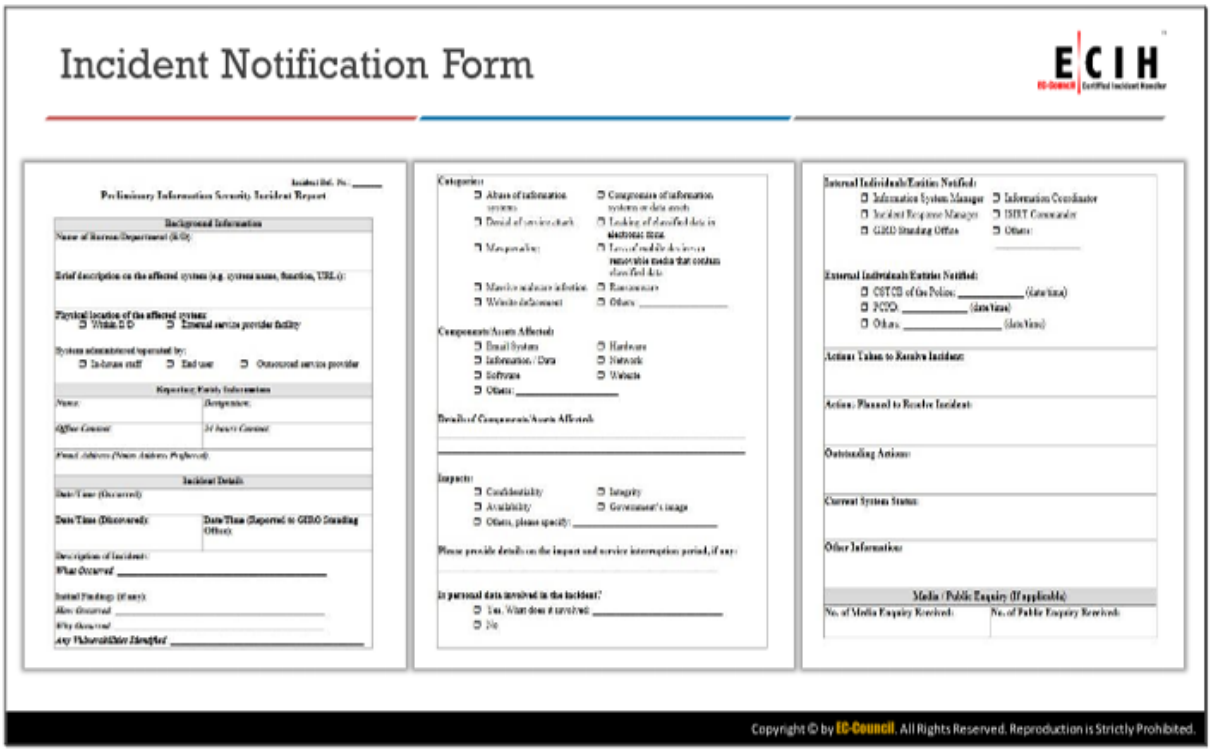
Helpful secure internal communication methods for incident notification include:

- **Secure Communication Channels**

  Most of organizations use secure channels for internal IH&R communications. These channels facilitate confidential internal communication during the IR process.

- **Out-of-Band Communication Channels**

  Out-of-band communication channels are a common internal communication practice employed by organizations. In this practice, Internal data is transferred through independent channels that are not used in regular communications.



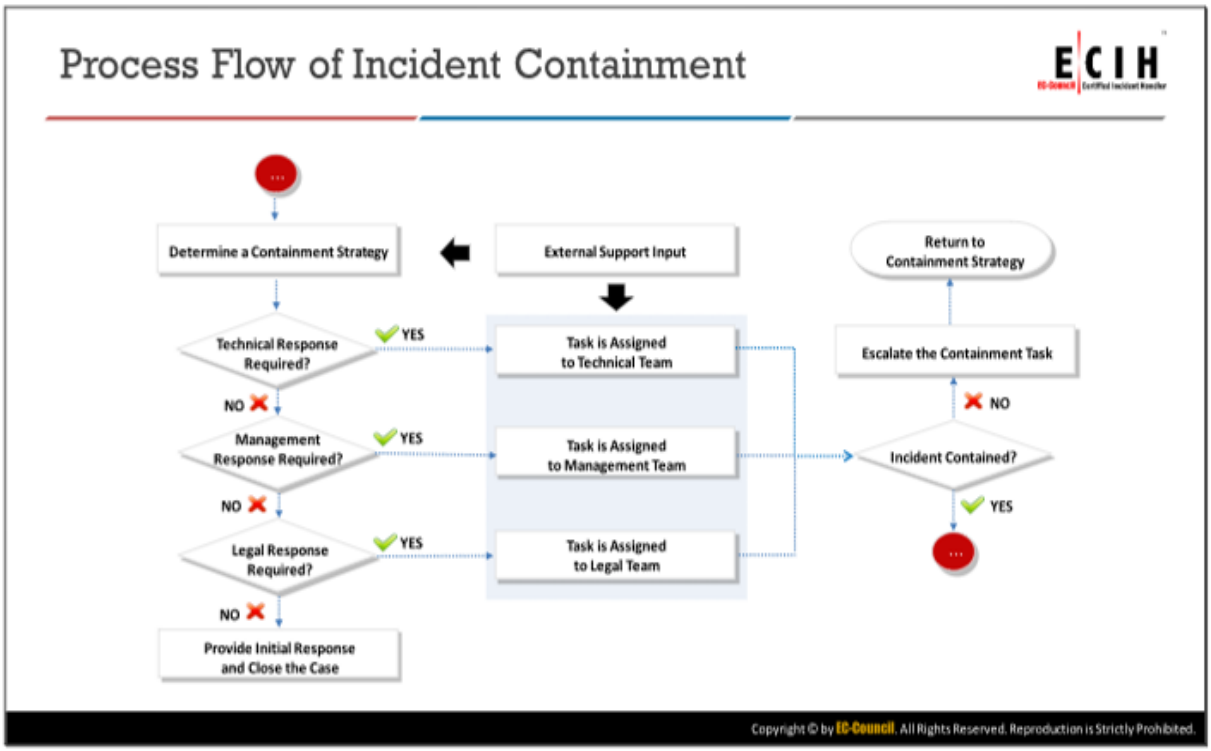
Incident Notification Form

The screenshots shown on the above slide display a sample incident notification form.

Step 5: Containment

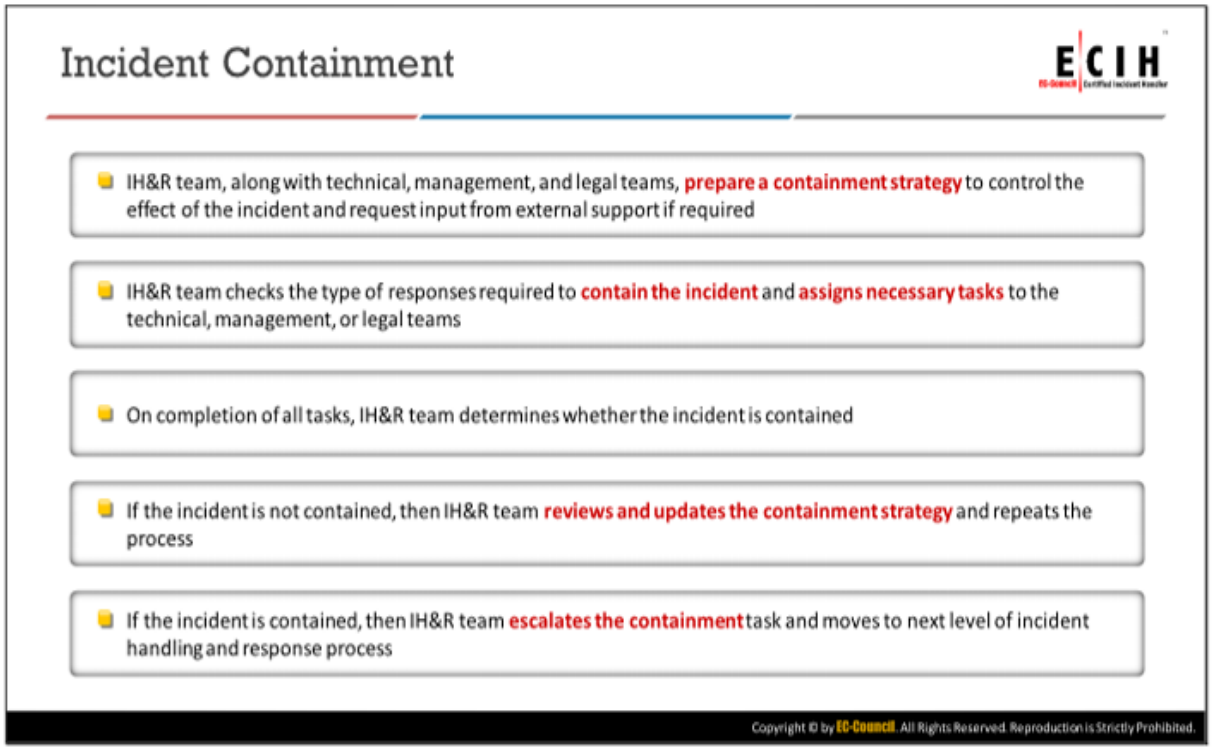
Containment focuses on limiting the scope and extent of an incident. It deals with information and computing services. The aim of the containment stage is to stop the attack from spreading to similar resources across the organization and to reduce losses and damages.

This section discusses the process flow of containment, common techniques used in the containment process, and guidelines for incident containment.



Process Flow of Incident Containment

The process flow of containment starts with deciding the appropriate containment strategy for the particular type of incident. Then, depending on the requirements of the technical response, management response, or legal response to the incident, the task will be assigned to the technical team, management team, or legal team respectively in order to contain the incident. Depending on the containment status, the containment task can be escalated back to the containment strategy stage to facilitate any modifications to strategy.



Incident Containment

If the security incident compromised systems, networks, or workstations, then the IH&R team must determine whether to shut down the system, disconnect the network, or continue the operations to contain the attack.

The response to all these situations depends on the type and magnitude of the incident. Shutting down the systems and disconnecting them from the network is the best option when the incident has compromised critical files and sensitive information. However, incident responders should also ensure that such actions do not disrupt business or, at the very least, ensure they restore the functions at the earliest.

The IH&R team plays a significant role in this stage by reducing a threat or incident's magnitude or complexity to prevent further damage to the organization.

Some of the key activities of an IH&R team in containing a security incident include:

- The IH&R team, along with technical and managerial personnel, must prepare a containment strategy to control the effects of the incident(s).
- The strategy must include feedback from external support, if required.
- The IH&R team must check the type of response required to contain the incident and assign the tasks to the technical, managerial, or legal teams to contain the incident.
- Once the relevant team has completed the assigned task, the IH&R team must ensure that the containment was successful.
- If incident containment failed, then the IH&R team must escalate the process to an advanced stage, review and update the containment strategy, and restart the process.

- If the incident was contained, then the IH&R team must close the containment task and move to next level of the IH&R process.

Common techniques used in the containment phase include:

- **Disabling of Specific System Services**

  To reduce the impact of the incident and to continue system operations, the team should temporarily disable the compromised system services. If the incident has occurred through an unknown vulnerability, then the IH&R team should disconnect the system from the network until they resolve the issue.

- **Changing of Passwords and Disabling of Accounts**

  If the attacker has compromised the accounts or systems used to access accounts, then the IH&R team should disable these accounts and change the passwords on all affected systems to minimize any further loss of data in the network and systems. Moreover, it is also necessary to change the passwords of all systems that interact with the affected system to contain the attack.

- **Complete Backups of the Infected System**

  Create backups of the data on affected systems and use it to restore the services offered by that system if it is damaged during IR. System backups can also help in the further investigation of the incident.

- **Temporary Shutdown of the Compromised System**

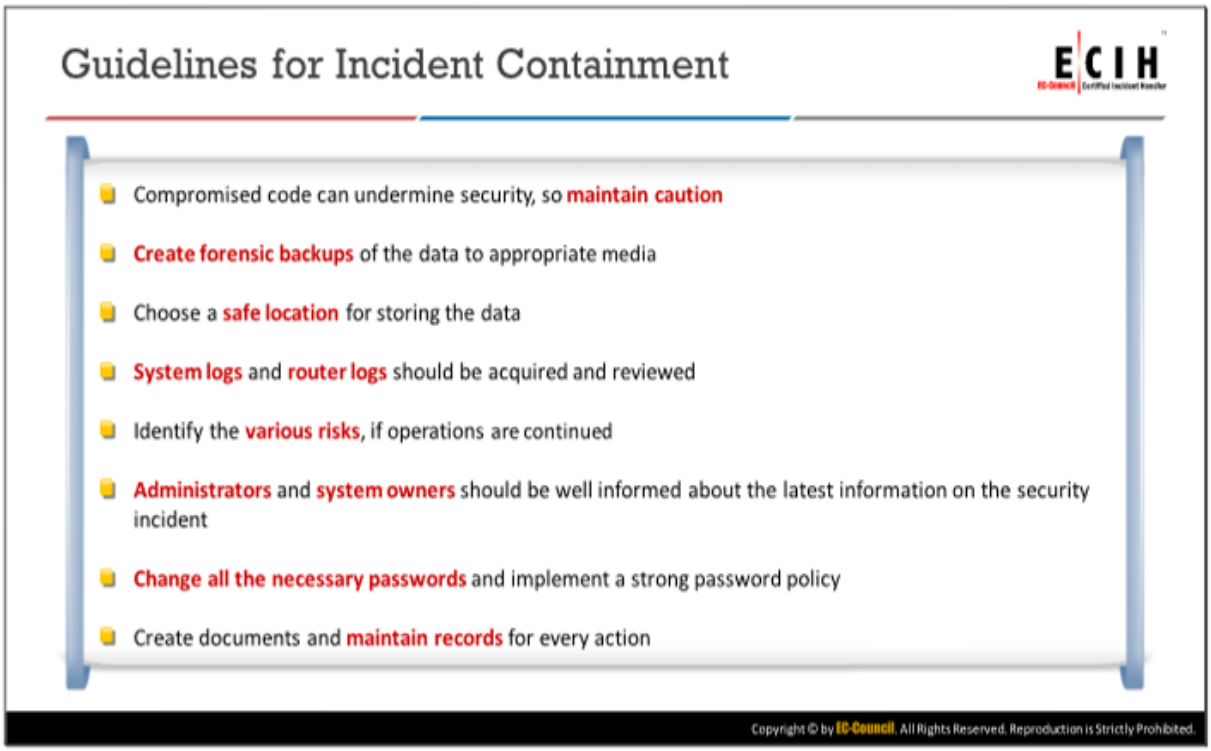
  If compromised computer systems must be shut down to contain the situation, then shut them down temporarily. This shutdown limits the damage caused by the incident and gives the IH&R team extra time to analyze the problem.

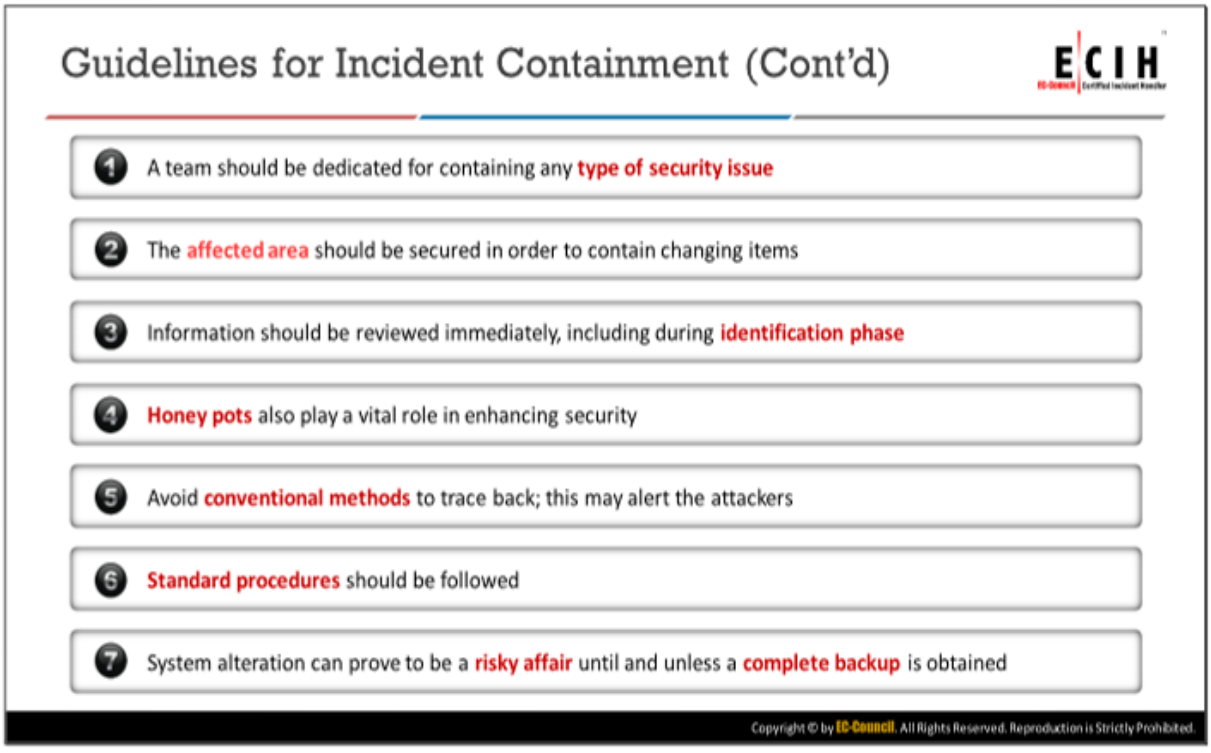
- **System Restoration**

  The IH&R team can repair or replace the systems compromised and recovered from the incident with a trusted backup copy using hardware resources. Before restoring the system, identify the incident sources such as vulnerabilities, threats, and access paths and patch the system.

- **Maintaining a Low Profile**

  If the attack is network-based, then concerned individuals should be careful not to tip off the intruder, who may be hoping to do more harm to other systems in the network by erasing every chance of tracing his or her work. Maintain standard procedures, including the use of intrusion detection systems and the latest antivirus and antispam software.



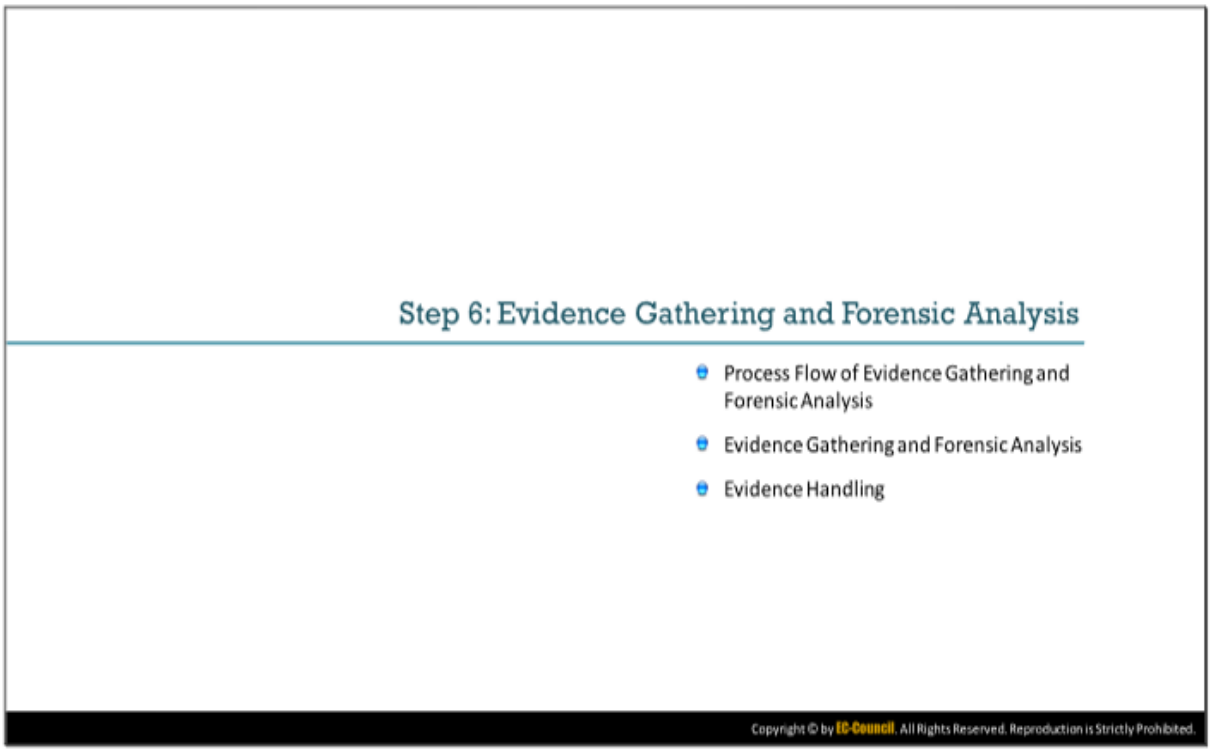


Guidelines for Incident Containment

The main purpose of the containment strategy is to control the effects of the attack as soon as possible and to maintain business continuity. Incident responders must adhere to the following guidelines to properly contain an incident in the organization:

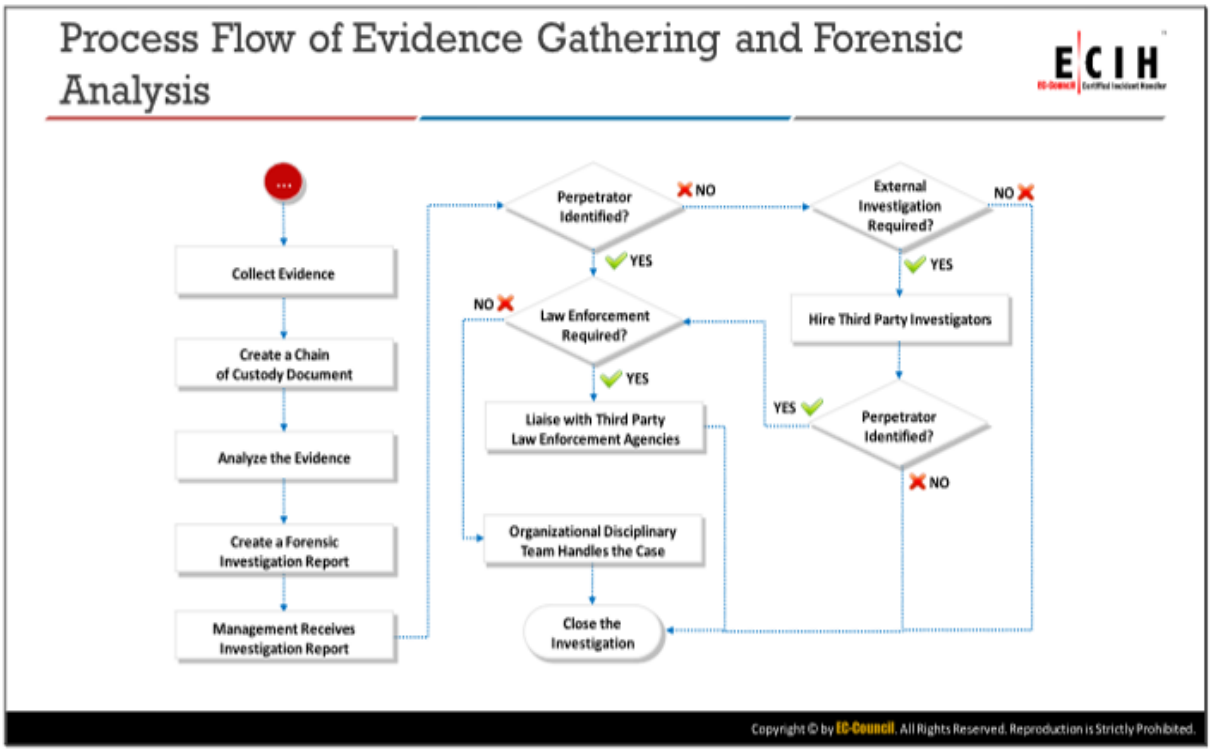
- Compromised code can undermine security; therefore, it is important to maintain caution

- Create forensic backups of the data with proper media
- Choose a safe location for data storage
- System logs and router logs should be acquired and reviewed
- Identify all risks if operations continue after the incident
- Administrators and system owners should stay well-informed about the latest information regarding the security incident
- Change all necessary passwords and implement a strong password policy
- Create documents and maintain records for every action
- Dedicate a team to containing any type of security issue
- Secure the affected area to contain changes
- Review information right from the identification phase
- Remember that honeypots significantly enhance security
- Avoid conventional methods for tracing back incidents; they may alert attackers
- Frame and encourage IH&R team members and other employees to follow standard procedures and policies during the containment process
- Remember that system alterations are risky until the IH&R team obtains a complete backup



Step 6: Evidence Gathering and Forensic Analysis

After containing an incident, an IH&R team must concentrate on digging deep into the incident by gathering more information about it, identifying its root cause, uncovering threat actors behind it, and specifying its threat vectors. These objectives can be achieved in the evidence gathering and forensic analysis phase of the IH&R process. This section discusses the process flow of evidence gathering and forensics analysis, the concepts of evidence gathering and forensics analysis, and evidence handling.

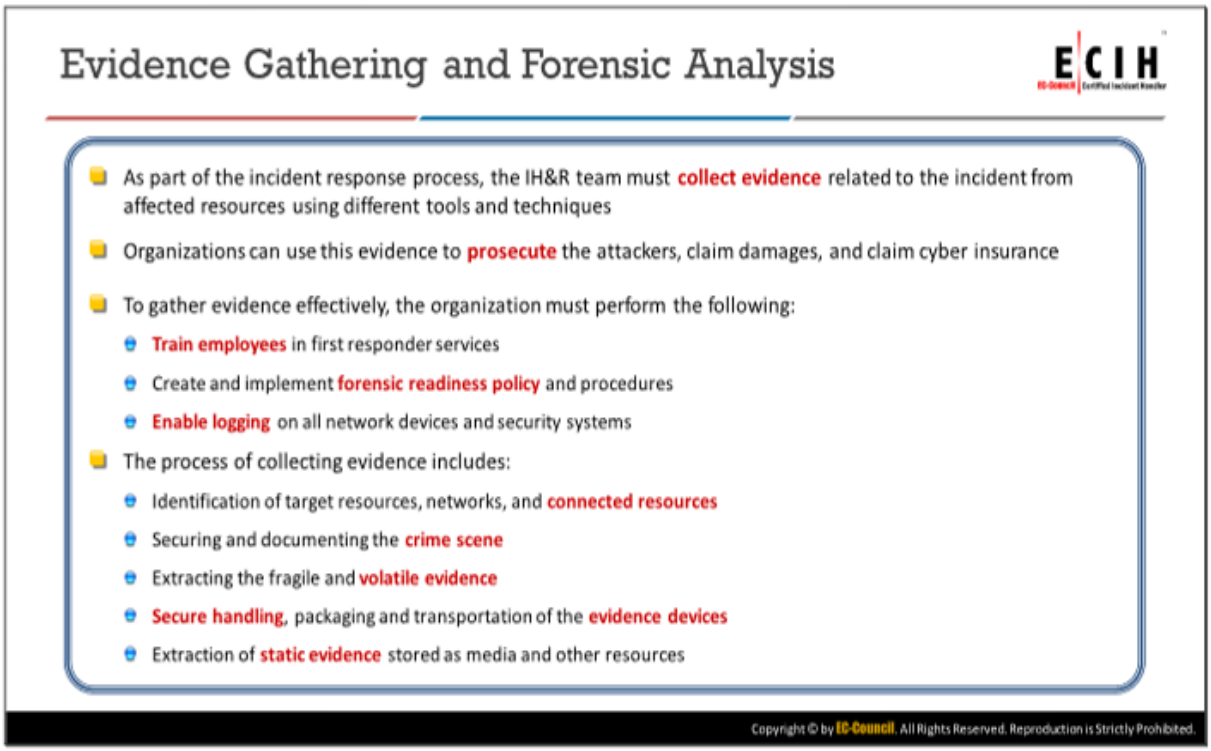


Process Flow of Evidence Gathering and Forensics Analysis

An IH&R team will collect crucial evidence about the incident and simultaneously create a chain of custody document. After collection and protection, investigators must analyze existing evidence to identify the cause and nature of the incident and trace the perpetrators of the crime. Moreover, they must also document the results of forensic analysis and submit them to management for further processing. If the analysis can identify the perpetrator, then the management will decide whether they will legally prosecute the perpetrator or let the organization's disciplinary team handle the case. If there is need for law enforcement, then management or a designated authority will contact a third-party law enforcement agency.

If the investigation fails to identify the perpetrator, then management must decide whether to close the investigation or to pass it to an external investigation agency for further investigation. If third-party investigators can investigate the incident and identify the perpetrator, then they will report such findings to management and management will make further decisions. Meanwhile, if third-party investigators also fail to identify the perpetrator, then the IH&R team or management can recommend an update to the IH&R processes that will enable them to carry out more successful investigations in the future.

The process flow of evidence gathering and forensics is displayed in the figure shown on the above slide.

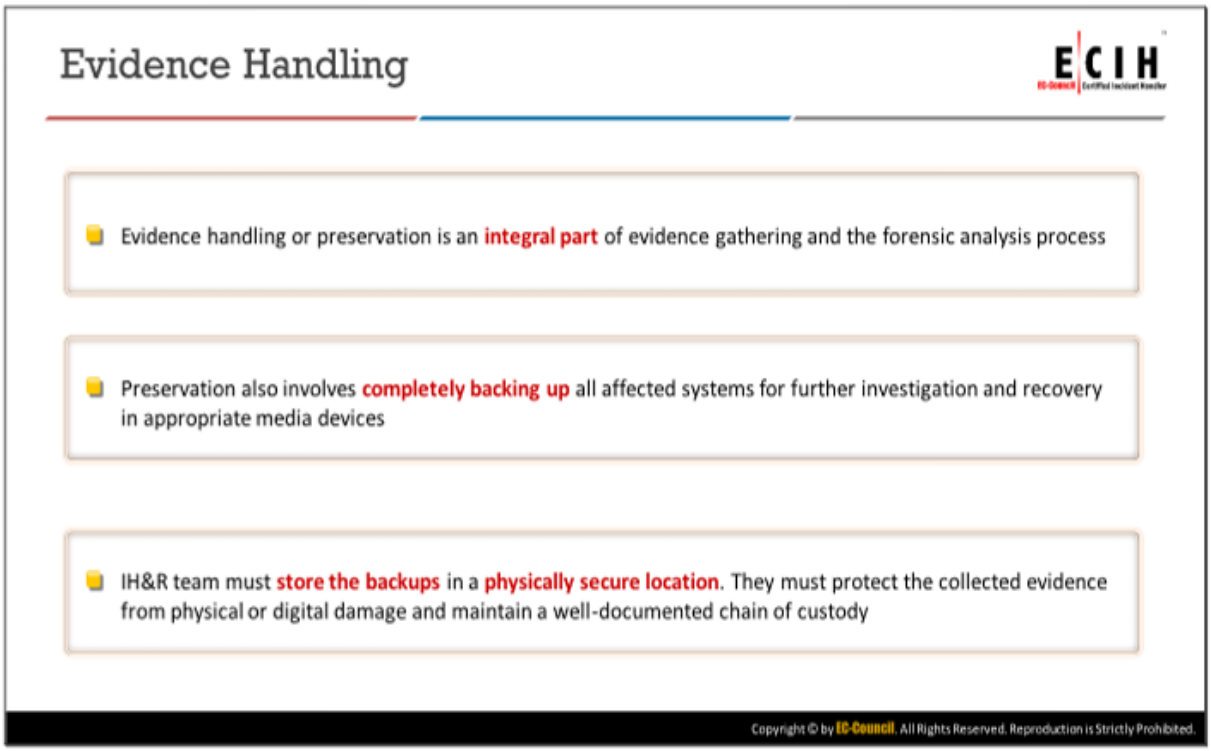


Evidence Gathering and Forensics Analysis

Evidence gathering and forensics analysis is one of the most important phases in the IH&R process. As noted above, after containment, the IH&R team is responsible for finding further details about the incident, such as any remaining information about the incident, the incident's root cause, the threat actors behind the incident, and the incident's threat vectors.

More specifically, the IR team must gather evidence from victim resources using different tools and techniques and use it to eradicate the incident, create reports about the attack, and close the exploited vulnerabilities. The organization can then use this information to prosecute the attacker(s) and claim damages and cyber insurance. To be sure, evidence helps the organization find and patch any vulnerabilities exploited and other attack vectors.

- To gather evidence effectively, the organization must:
  - Train employees in first responder services
  - Create and implement forensic readiness policies and procedures
  - Enable logins on all network devices and security systems
- The process of collecting evidence includes:
  - Identification of target resources, networks, and connected resources
  - Securing and documenting the crime scene
  - Extracting fragile and volatile evidence
  - Secure handling, packaging, and transportation of the evidence devices
  - Extracting static evidence stored as media and other resources

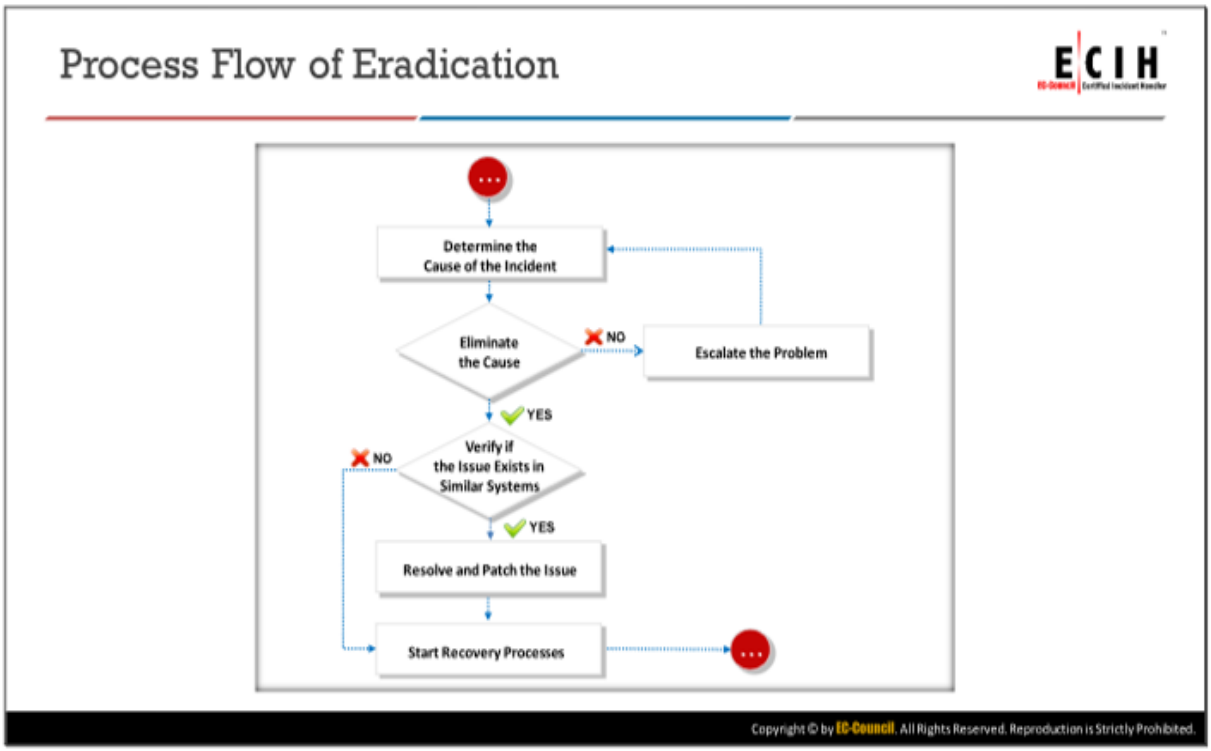


Evidence Handling

Evidence handling or preservation is an integral part of the evidence gathering process. Preservation also involves completely backing up all affected systems for further investigation and recovery in appropriate media devices. As noted above, the IH&R team must store all backups in a physically secure location, protect the collected evidence from physical or logical damage, and maintain a well-documented chain of custody. Only individuals authorized for legal or data recovery purposes should have access to the backup.

Step 7: Eradication

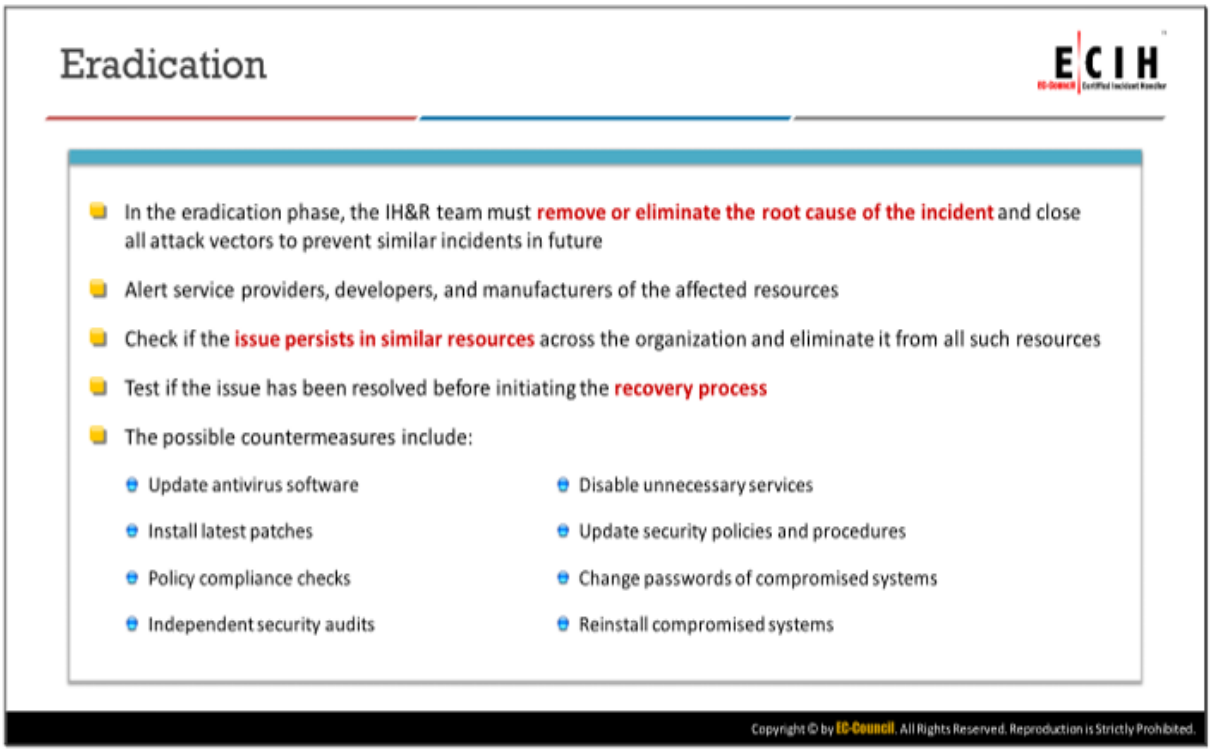
After evidence gathering and forensic analysis, the IH&R team is responsible for completely eradicating the incident and its related causes, identified vulnerabilities, and so on. This section discusses the process flow of eradication, the concepts involved in the eradication phase, and the tools used to detect missing security patches.



Process Flow of Eradication

After evidence gathering and forensic analysis, the IH&R team will have specific information about the incident. At this point, the team is responsible for acting in response to this information to eradicate the root causes of the incident(s). The process flow of eradication is displayed on the above slide.

In order to eradicate the issue, it is necessary to first perform a vulnerability analysis to determine if the network is still vulnerable to such attacks and, in response, to harden network security. If the cause is still present, then try to eliminate it; otherwise, escalate the problem to the relevant department(s). If the main cause is eliminated, then verify whether the issue exists in similar systems. After identifying and eliminating all threats, the team must resolve the security posture. This next step involves implementing protection tools and techniques, such as firewalls, routers, and router filters; configuring network security devices and applications to block the identified attack paths; and patching all identified vulnerabilities to stop further exploitation. In extreme cases, this step also requires changing the different externally visible network component addresses to remove established attack paths. In all cases, the team should perform internal audit of all resources before initiating the recovery process.

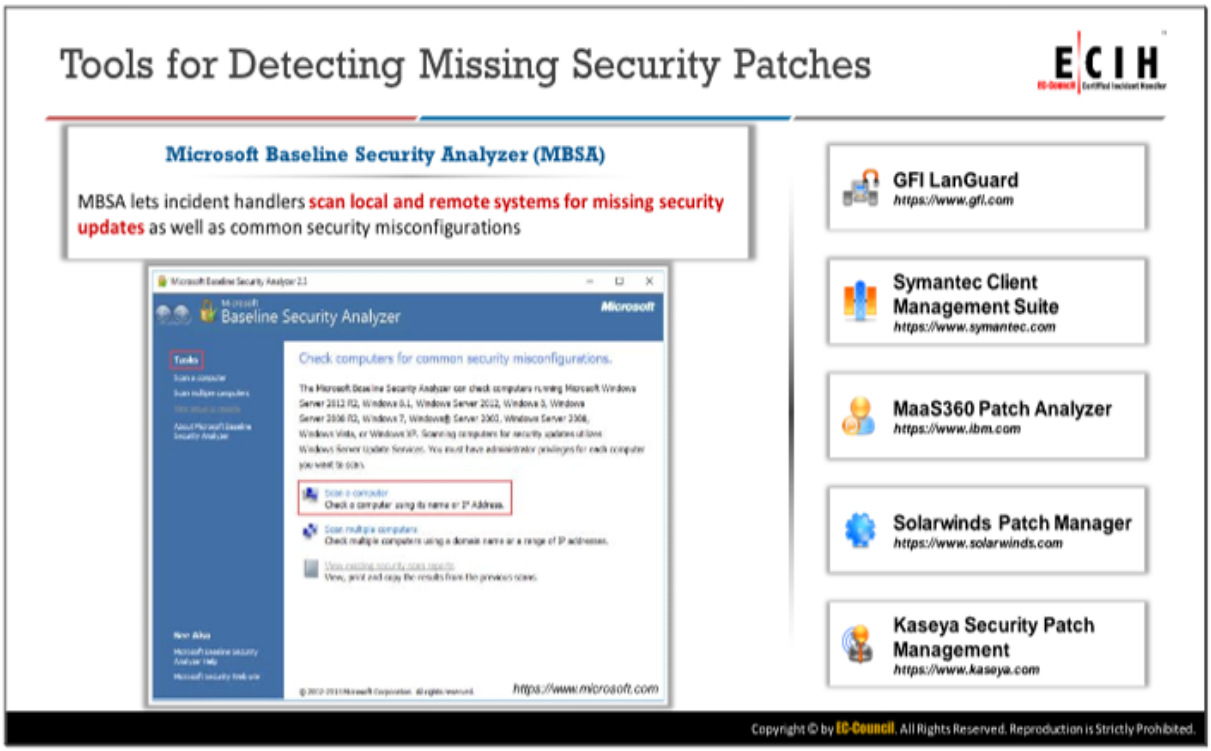


Eradication

In the eradication phase, the IH&R team must remove or eliminate the root cause of the incident and close all attack vectors to prevent similar incidents from occurring in the future. The IH&R team must alert all service providers, developers, and manufacturers about the affected resource; check if the issue persists in similar resources across the organization; eliminate the issue from any such resources; and test whether the issue has been resolved before initiating the recovery process.

Accordingly, the IH&R team must perform the following countermeasures as part of the eradication phase:

- Update antivirus software with new malware signatures and patterns
- Install the latest patches on systems and network devices
- Conduct independent security audits
- Check for policy compliance and update obsolete policies and procedures
- Disable any unnecessary services
- Change passwords for all compromised systems, accounts, and network devices
- Eliminate access paths and exploits
- Install an updated operating system, software, and services in compromised systems only after removing all traces of the attack
- Rebuild the affected or compromised systems, servers, databases, and networks
- Validate the effectiveness of all corrective steps or countermeasures



Tools for Detecting Missing Security Patches

Tools for detecting missing security patches help incident handlers to install the latest patches on their systems and networks. Patching any identified vulnerabilities helps an IH&R team prevent its system from being further exploited and eradicate the root causes of the exploitation.

The following is an important tool for detecting missing security patches in a Microsoft system:

- **Microsoft Baseline Security Analyzer (MBSA)**

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

  Microsoft Baseline Security Analyzer (MBSA) is a tool designed for IT professionals to help small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations. MBSA lets incident handlers scan local and remote systems for missing security updates as well as common security misconfigurations. MBSA includes a graphical and command line interface that can perform local or remote scans of Microsoft Windows systems. It is important to note that, in assessing missing security updates, MBSA only scans for missing security updates, update rollups, and service packs available from Microsoft Update.

Some additional tools for detecting missing security patched are listed below:

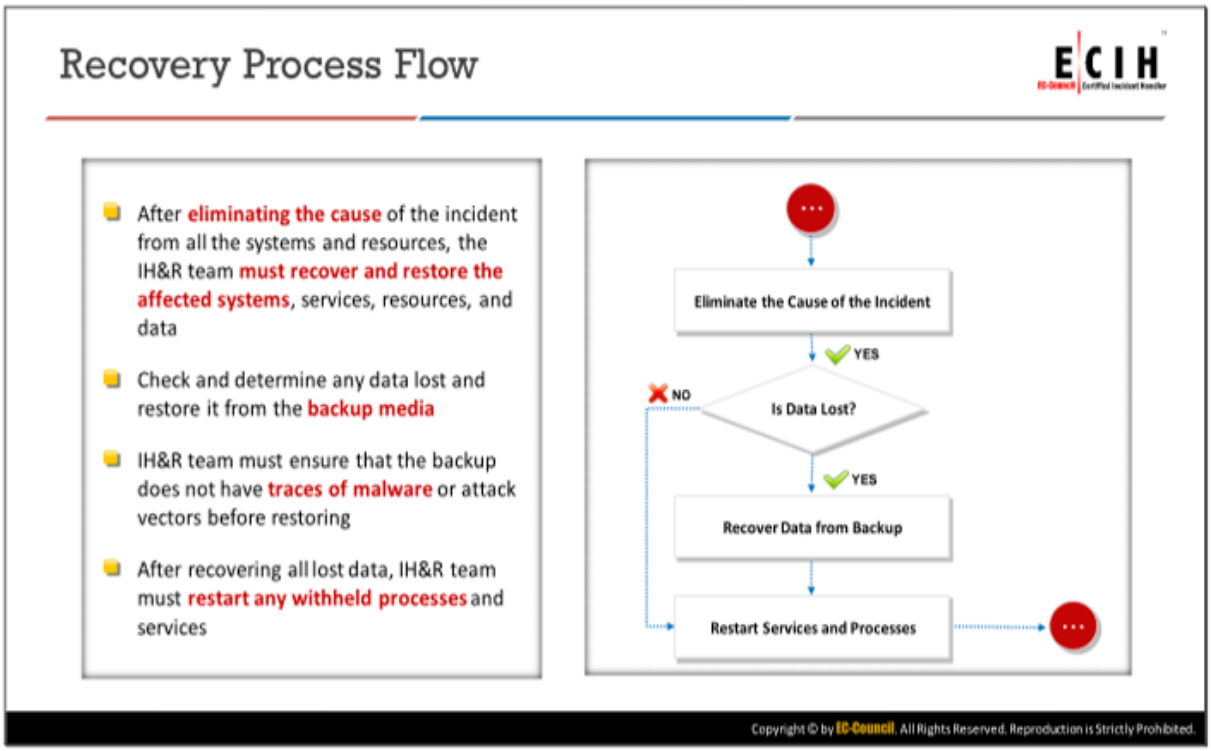
- GFI LanGuard (*https://www.gfi.com*)
- Symantec Client Management Suite (*https://www.symantec.com*)
- MaaS360 Patch Analyzer (*https://www.ibm.com*)
- Solarwinds Patch Manager (*https://www.solarwinds.com*)

- Kaseya Security Patch Management (*https://www.kaseya.com*)
- Software Vulnerability Manager (*https://www.flexera.com*)
- Ivanti Endpoint Security (*https://www.ivanti.com*)
- Patch Connect Plus (*https://www.manageengine.com*)
- Automox (*https://www.automox.com*)
- Prism Suite (*https://www.newboundary.com*)

Step 8: Recovery

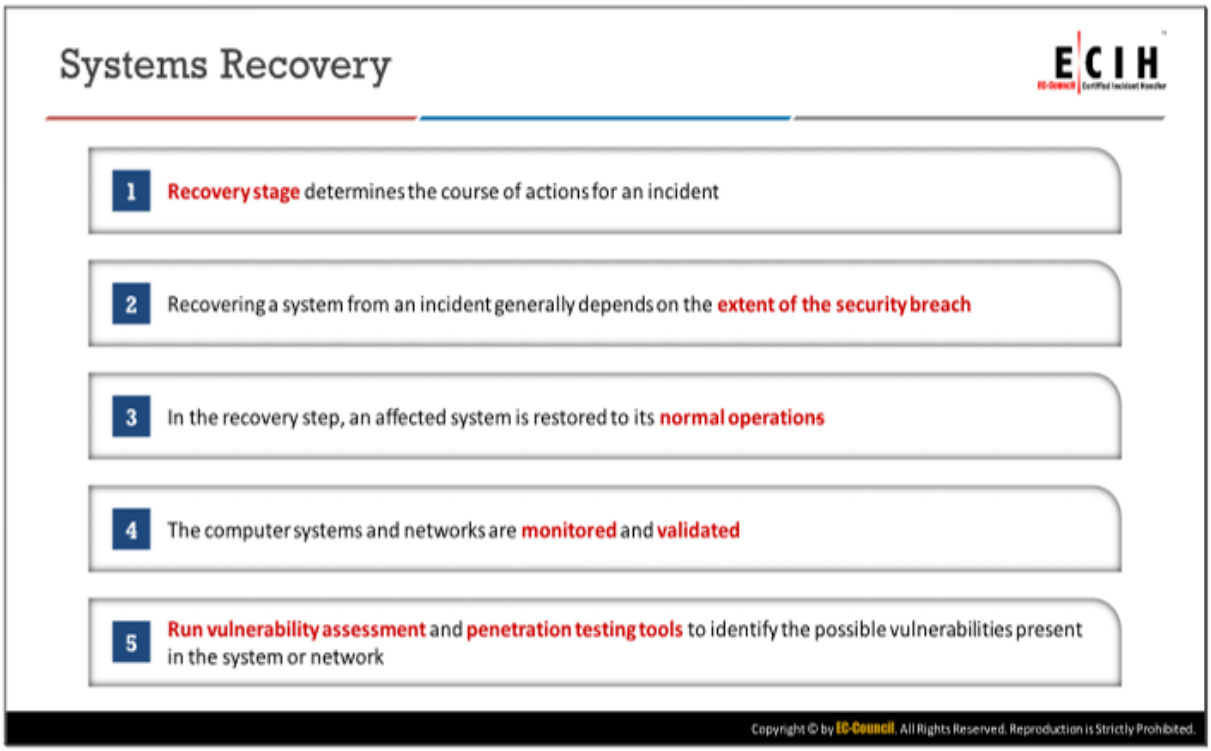
After the eradication phase, during which all root causes of the incident are eliminated, the IH&R team must restore all affected systems, services, resources, and data through a recovery process. This phase of the IH&R process is essential to the maintenance of normal business operations after the incident.

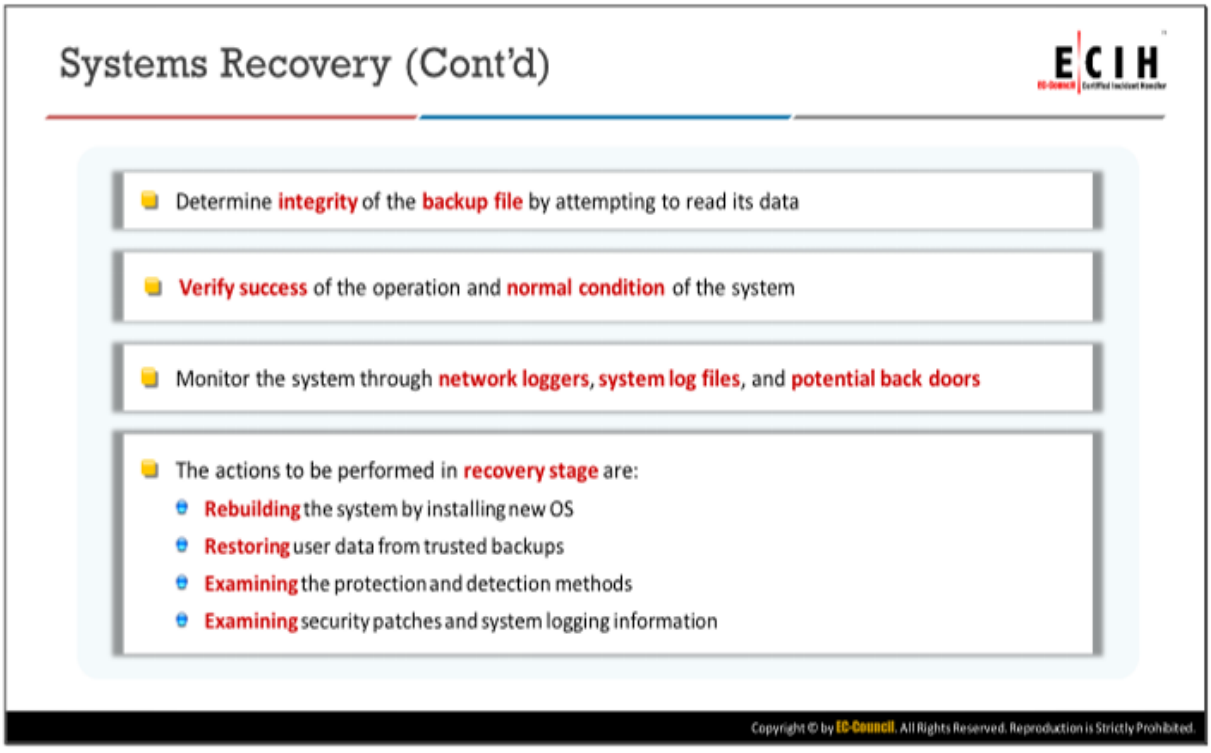
This section discusses the process flow of recovery and the concepts of systems recovery and remediation planning.



Recovery Process Flow

After eliminating the cause of the incident from all systems and resources, an IH&R team has to identify whether the data is lost. If the data is lost, then the IH&R team has to recover the data from backups and restart the affected services and processes in order to maintain business continuity.





Systems Recovery

Recovery is the process of restoring lost data from backup media. During this process, an IH&R team has to make sure the backup does not have traces of malware or attack vectors before performing the restore. The time it takes to recover a system generally depends on the extent of the security breach. Recovery involves various techniques such as network perimeter security, strengthening user ID credentials, effective patch management, renewing files and

software, and rebuilding systems. After recovering all lost data, the IH&R team must restart all the withheld processes and services.

Recovering a system after an incident generally depends on the extent of the security breach. An IH&R team should decide whether to restore the existing system or completely rebuild the system—notably, the team can use the system backup for either process.

Therefore, the two steps in systems recovery are:

- **Determine the Course of Action**

  Devise various strategies for system recovery according to the impact of the incident and select an appropriate plan after considering the availability of resources, the criticality of affected systems, and the results of a cost-benefit analysis.

- **Monitor and Validate the Systems**

  By monitoring and validating affected systems, the IH&R team can ensure that recovered systems do not have any traces of incident causes and are operating within normal conditions. Helpful to note here for our purposes is that validation also involves checking the integrity of restored information from a backup. Teams should also be sure to conduct regular vulnerability assessments and penetration testing to monitor system behavior and possible vulnerabilities in the system or network. To be sure, it is important to monitor the system for potential back doors, which can result in the loss of data.

Notable actions the response team must perform during the recovery stage include:

- Rebuilding the system by installing a new OS
- Restoring user data from trusted backups
- Examining protection and detection methods
- Examining security patches before installation and enabling system logging

The IR team must also determine the integrity of the backup file by reading its data and verifying its integrity before restoring it on the systems. It is also important for the team to verify success of the operation and the normal condition of the system after installing the backup. The team must monitor the system using network loggers, system log files, and potential back doors after installation and during usage.

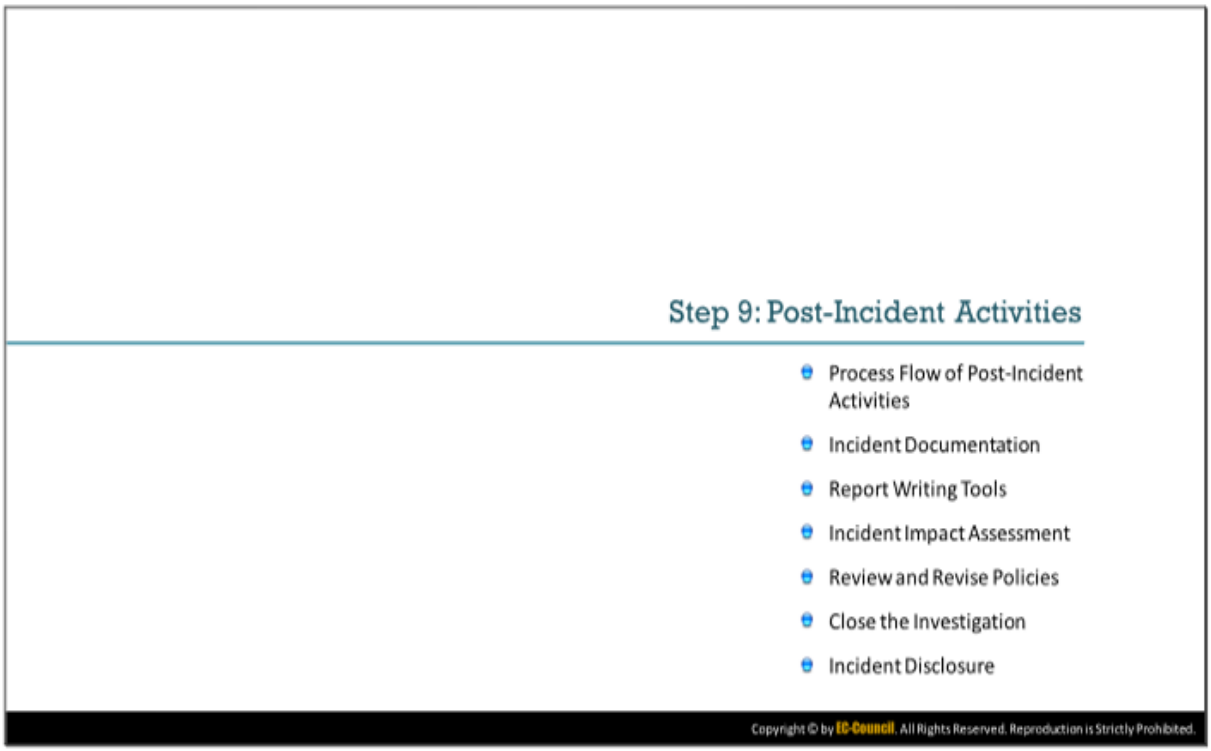
Recovery and Remediation Plan

Recovery plans are developed for specific departments within an organization to allow them to recover from incidents. The purpose of recovery planning is to prepare such departments to not only survive an incident but also continue their normal business operations. To facilitate this, an organization must be confident in the critical operations it believes will help it sustain or resume business during and/or after an incident.

More specifically, organizations require recovery planning for the following reasons:

- It helps in continuing critical business operations during and after an incident

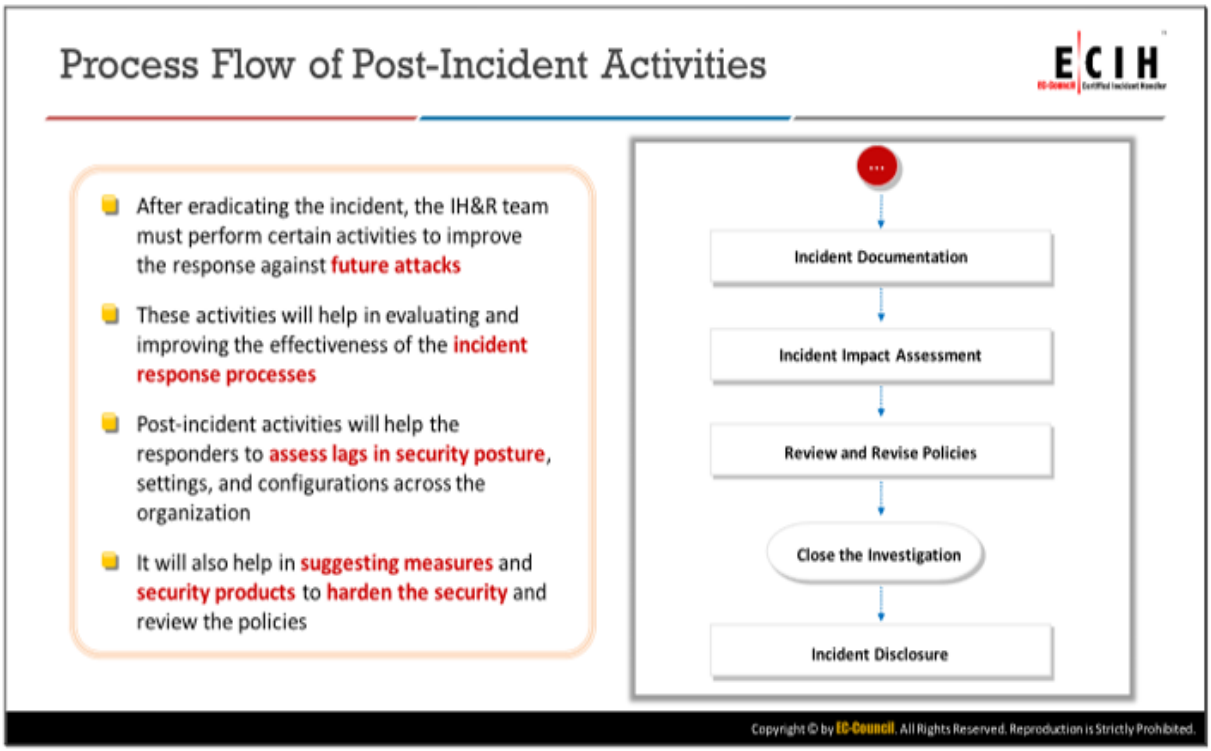
- It helps prevent organizations from shutting down after an incident
- It facilitates quick and effective decisions during an incident
- It identifies and prioritizes important business and support functions
- It provides effective supervision of recovery tasks
- It protects an organization's confidential information



Step 9: Post-Incident Activities

After eradicating the incident, an IH&R team must perform certain activities to improve its response to future attacks. Accordingly, "post-incident activities" refer to the actions and precautions that an organization and response team must perform to be better prepared to handle and respond to future incidents. In this stage, the team will discuss all the drawbacks it faced during the response functions and try to eliminate them.

This section discusses various post-incident activities and elements, such as incident documentation, report writing tools, incident impact assessment, policy review and revision, and incident disclosure.



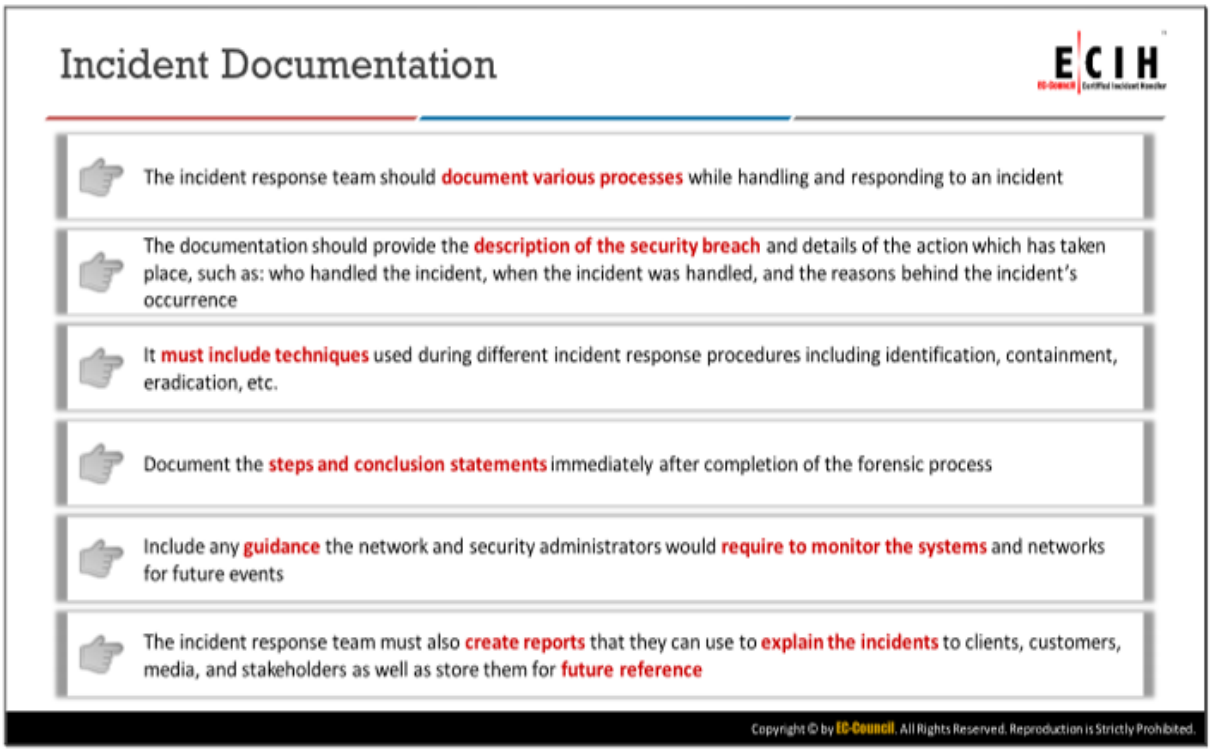
Process Flow of Post-Incident Activities

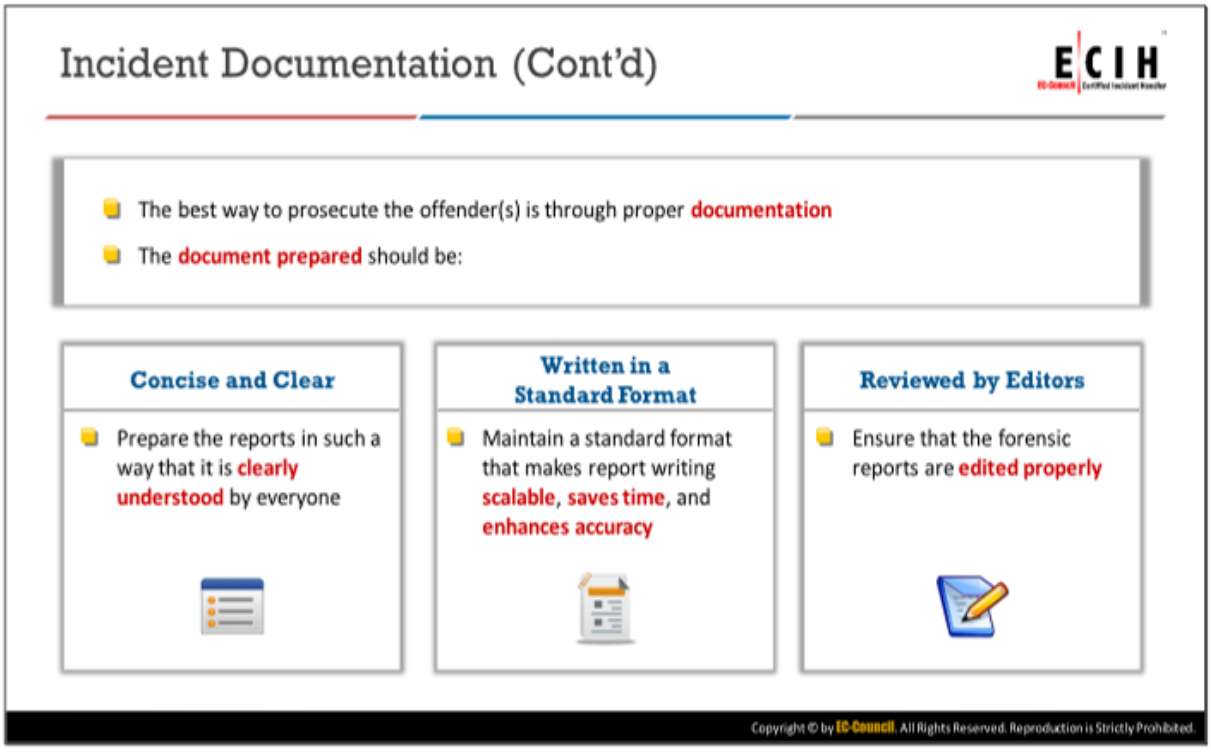
Post-incident activities help in evaluating and improving the effectiveness of IR processes by helping responders assess lags in security postures, settings, and configurations across their organization. They also help in suggesting measures and security products an organization can use to harden its security and optimize its policies.

To be sure, organizations should conduct meetings with staff and other involved parties to understand all lessons learned from the incident and improve in any areas in which it currently falls behind. These activities will help in evaluating and improving the effectiveness of IR processes by offering insight into how to best update policies, procedures, security postures, settings, and configurations across the organization to build a robust network.

Moreover, to learn from the experience, the IH&R team must have a document about the incident that reveals any details about the incident, vulnerabilities exploited, response measures implemented, results, pitfalls in the response process, and drawbacks in communication and management. Accordingly, as noted throughout this module, the IH&R team should document every step of the IR as well as the lessons implemented. The IH&R team must then communicate any updates and new implementations to clients, customers, management, and other stakeholders.

The figure shown on the above slide displays the overall process flow of post-incident activities.





Incident Documentation

As stated above, the IH&R team should document various processes while handling and responding to an incident. The documentation should describe the security breach and detail the measures taken in response, such as who handled the incident, when the incident was handled, and the reasons behind the occurrence of the incident. The steps taken and conclusions reached should be documented immediately after the forensic process.

In addition, management and legal representatives should properly organize, examine, review, and evaluate the document. As already noted, documenting all incident handling procedures and methods will help network administrators handle similar security issues in future. Accordingly, such documentation must include techniques used during different IR procedures, including identification, containment, and eradication, as well as any guidance the network and security administrators would require to monitor the systems and networks for future events.

The IR team must possess excellent report writing skills in order to create reports that they can use to explain the incident(s) to clients, customers, media, and stakeholders and that they can store for future reference. Management and legal representative must properly organize, examine, review, and vet these documents.

Important to note for our purposes is that organizations can produce such documentation in a court of law as proof of authentic evidence collection. Incident documentation also helps law enforcement agencies to nab the real culprits. Notably, incident handlers are responsible for producing these documents, along with other relevant evidence, to legal representatives for prosecution. Given their importance, such documents must be secured and hardened to prevent tampering or theft.

Because such proper documentation is necessary to prosecute the offender, it should be precise, clear, and verifiable. This documentation should also include the steps and conclusions of the investigation process. Along these lines, such documents should be:

- **Concise and Clear**

  Most people in the juridical sphere, including lawyers and judges, may not have a strong grasp of language related to cyber security. Therefore, incident handlers should prepare reports that everyone can read and easily understand. Never use shortcuts while preparing such reports and support them with proper screenshots and printed results.

- **Written in a Standard Format**

  Every organization should have a standard infrastructure for writing and submitting reports as maintaining a standard format makes report writing scalable, saves time, and increases accuracy. Organize the response process by generating forms, outlines, and templates and support the storage of the data related to the incident.

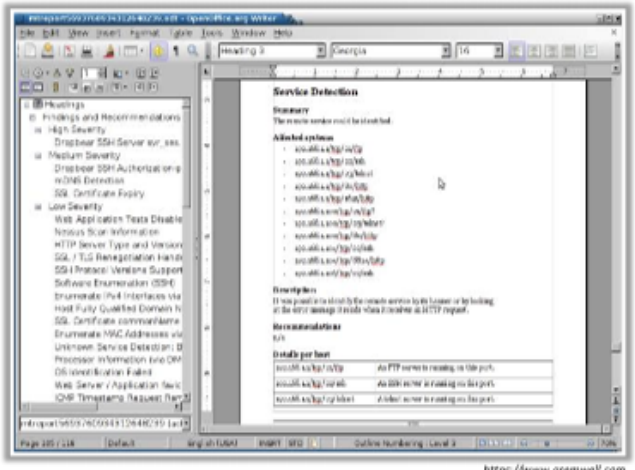
- **Reviewed by Editors**

  Hire proofreaders and seek the help of technical editors to ensure the readability of forensic reports. Moreover, because errors can diminish the integrity of a report and make it invalid in a court of law, it is crucial to ensure that all reports are free from errors. Editors can help in creating error-free reports.

Report Writing Tools: Magic Tree

- Report writing tools help incident handlers to **generate efficient reports** on detected incidents during incident handling and response process

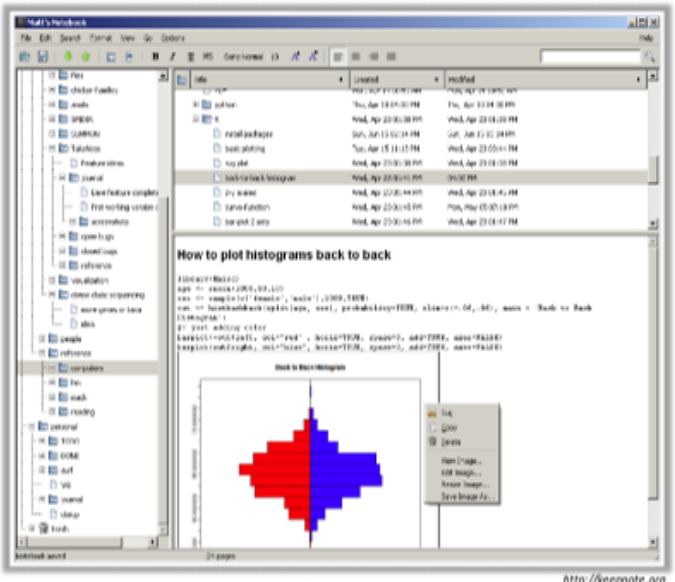
- MagicTree stores data in a **tree structure**
- This is a natural way of representing the information gathered during a network test: a host has ports, which have services, applications, vulnerabilities, etc.



https://www.gremwell.com

Report Writing Tools: KeepNote

- KeepNote is used to store class notes, TO-DO lists, research notes, journal entries, paper outlines, etc. in a simple **notebook hierarchy** with rich-text formatting, images, and more
- It is designed to be **cross-platform** (implemented in Python and PyGTK) and stores your notes in simple and easy-to-manipulate file formats (HTML and XML)



http://keepnote.org

Report Writing Tools

Report writing tools help incident handlers generate efficient reports on detected incidents during the IH&R process.

The following are some important report writing tools:

- **MagicTree**

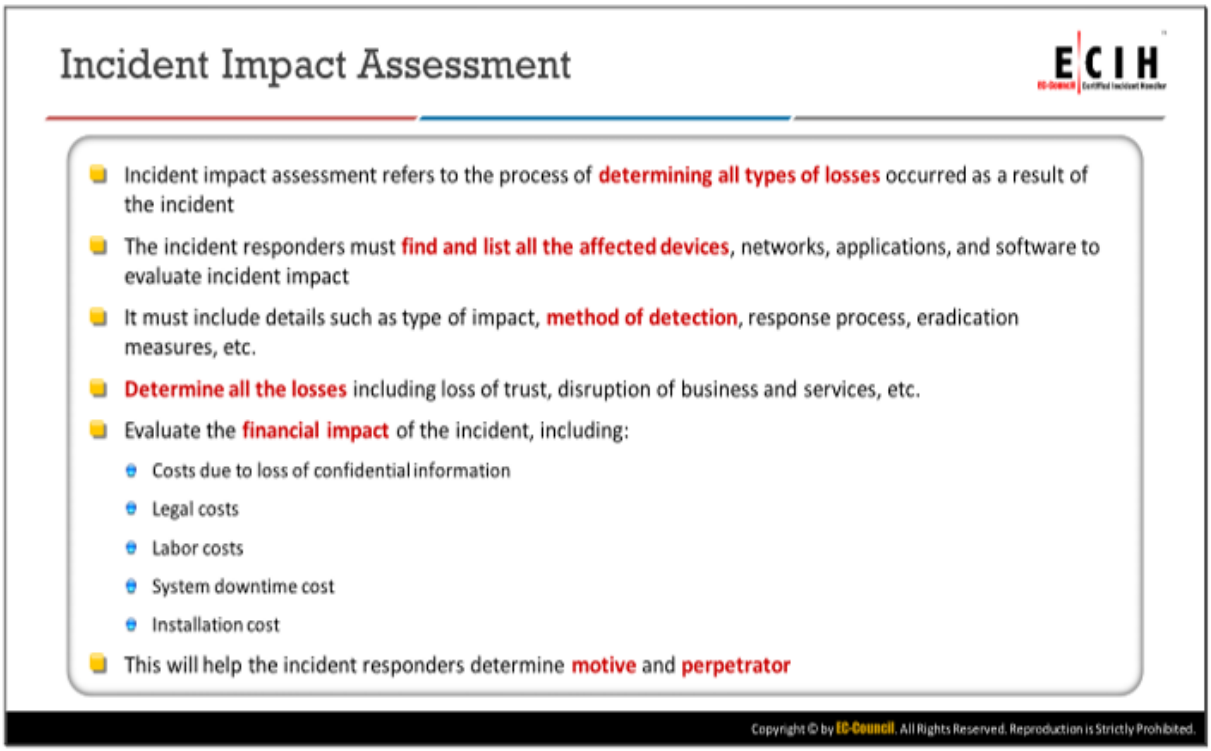
  Source: *https://www.gremwell.com*

  MagicTree stores data in a tree structure. This is a natural way of representing information gathered during a network test: a host has ports, which have services, applications, vulnerabilities, and so on. The tree-like structure is also flexible in that it can add new information without disturbing the existing data structure: at some point, if you decide that you need the MAC address of the host, you just need to add another child node to the host node. While such a tree structure is a natural way of representing information, it is not very convenient for actually using the data. To feed data to programs, we generally want lists or tables of items. Accordingly, MagicTree allows users to extract data in tables (or lists); the query interface uses XPath expressions to extract data.

- **KeepNote**

  Source: *http://keepnote.org*

  KeepNote is a note-taking application that works on Windows, Linux, and MacOS X. With KeepNote, you can store your class notes, TODO lists, research notes, journal entries, paper outlines, and so on in a simple notebook hierarchy with rich-text formatting, images, and more. Using a full-text search, you can retrieve any note. KeepNote is designed to be cross-platform (implemented in Python and PyGTK) and stores your notes in simple and easy-to-manipulate file formats (HTML and XML). Archiving and transferring your notes is as easy as zipping or copying a folder.



Incident Impact Assessment

"Incident impact assessment" refers to the process of determining all types of losses that occur due to an incident. Incident responders must find and list all affected devices, networks, applications, and software to evaluate the impact of the incident. An incident impact assessment must include details such as type of impact, method of detection, response process, and eradication measures.

Incidents can also result in the loss of customers as well as customers filing lawsuits against the organization over its negligence regarding customers' personal information. The estimation of losses must include the damage costs as well as the cost incurred to recover from the incident.

An incident impact assessment must address:

- Financial losses incurred due to leakage of confidential information
- Legal costs for investigating the case, lawyer's fees, and so on
- Costs pertaining to analyzing the incident and recovering and installing software and hardware
- Losses and costs related to system downtime
- Implementation costs
- Costs related to repairing and replacing damaged systems and physical security
- Costs related to the damage of goodwill and, along these same lines, the loss of customer trust and reputation

The response team must determine all losses, including loss of trust and disruption of business, and include them in the assessment. Notably, incident damage and recovery costs play an

important role in legal actions against perpetrators. An impact estimation helps in identifying the motives behind the attack and the attackers. As already noted, the IH&R team must use the gathered information to secure targeted data, systems, networks, and other resources from future attacks.

Review and Revise Policies

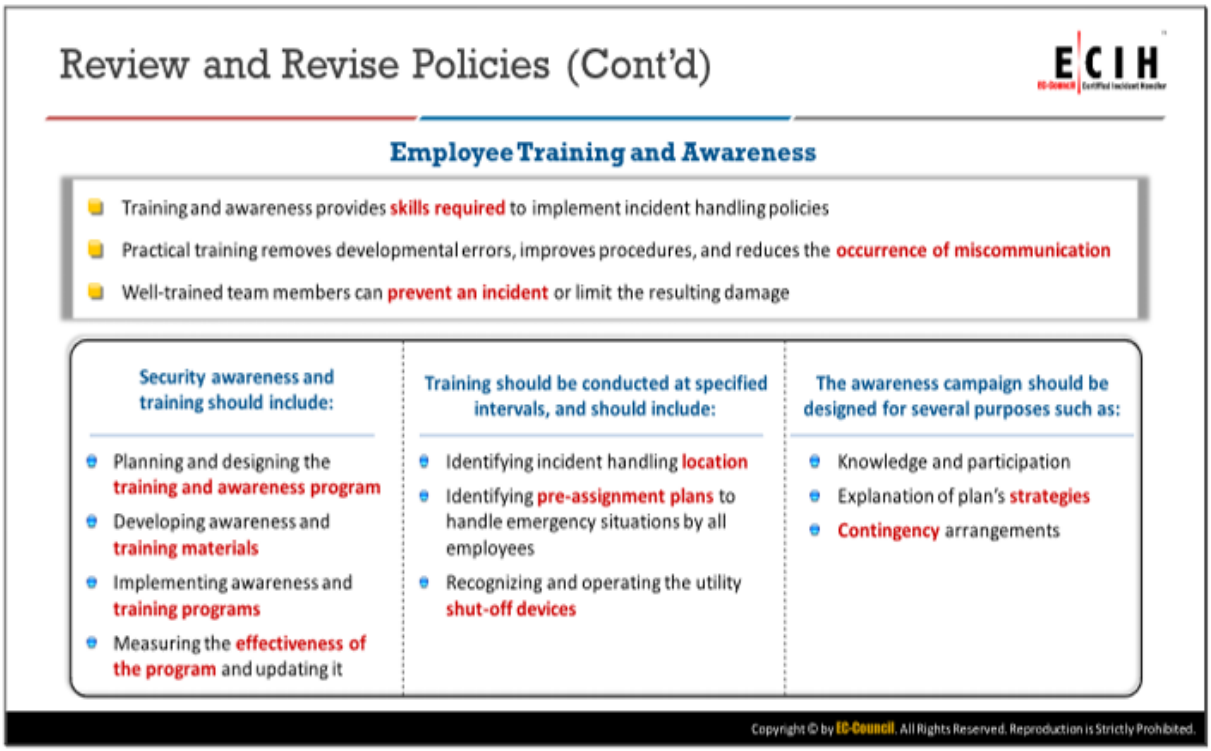
Review

1. Review the response and handling process after completion of both **documentation** and **recovery** steps
2. Discuss the steps that were **helpful** and **difficult** to implement with team members
3. **Evaluate** the **time and cost** of each response process
4. Assess the **vulnerabilities in security policies**, practices, and other aspects of the organization that led to the incident
5. Determine the **reasons** for any delays during the response
6. Create a document containing the review results and suggest methods to **strengthen the security** and incident response processes in an organization

Review and Revise Policies (Cont'd)

Revise

- The organization must revise all the policies, procedures, and practices to strengthen security
- Update these based on **feedback from users** and **incident response teams**
- Improve the security of devices that are susceptible to attacks and replace obsolete technologies with up-to-date systems
- Update the security solutions with attack signatures to **rapidly identify similar attacks** in future
- Inform the concerned authorities, including the **application developers** and **device manufacturers** about the vulnerabilities found in their products and request patches as early as possible
- Implement strict account, password, access, and **privilege policies** across the organization
- Impart training and awareness to the employees about the **new policies** and **practices**
- Consider revising the **security configuration controls** and **baseline configurations** based on the lessons learned



Review and Revise Policies

Reviewing and revising security policies is a key step in the IH&R process that helps prevent future incidents. Helpful to note is that the review and revision of security policies is simply the implementation of the lessons learned from previous incidents.

Review—Policies, Procedures, Preparation, and Protection

IH&R professionals must review the complete response process after completing both the documentation and recovery phases. At this point, they must discuss the steps that were successfully implemented and the mistakes that were committed during the response with all team members. They should also ask the team to provide suggestions and feedback that may help speed the process, reduce lags, eliminate pitfalls, and improve the complete IR process.

Evaluating the time and cost of each response process is the next step. Moreover, IH&R professionals should also assess all vulnerabilities in security policies, practices, and other aspects of the organization that have led to the incident; determine the reasons for any delays during the response; and create a document containing the review results that suggests ways to strengthen the organization's security and IR processes.

Revise—Policies, Procedures, Preparation, and Protection

Incident responders must use the knowledge and experience gained from the IR functions to suggest revisions to various security policies, configurations, settings, procedures, and practices. Along these lines, the IH&R team must conduct a post-incident feedback session involving all the users and employees. During this session, the team should ask the following questions:

- What have you learned from the incident?

- How could this be avoided in the future?
- How can we assess what is working and not working?
- What conclusions can be drawn from the incident?
- What other changes are required to polices, programs, or plans?

Based on the suggestions of the IR team and the feedback from the users, the organization must revise all policies, procedures, and practices to strengthen its security. The IH&R team must also consider revising its security configuration controls and baseline configurations based on the lessons learned from the incidents.

The organization must improve the security of devices that are susceptible to attacks. Along these lines, it must replace all obsolete systems and technologies with the latest equipment; update its security solutions with attack signatures to identify similar attacks in future; inform the concerned authorities, including application developers and device manufacturers, about the vulnerabilities found in their products; and request patches as early as possible; implement strict account, password, access, and privilege policies across its departments; and impart training and awareness to all employees about the new policies and practices.

Employee Training and Awareness

Training and awareness not only enhance employees' security knowledge, they also help change lackadaisical attitudes toward organizational security. The human factor in security can be far more formative than any software or hardware enhancement. Crucially, training significantly enhances employee understandings of organizational policies and can thus increase security. Put differently, employee training and awareness is necessary to facilitate general incident handling operations, the identification of different levels of importance, incident handling know-how, and so on. A "security awareness program" is a two-way information flow that uses various types of communication media such as audio, video, text, and practical training sessions.

Incident handlers should use knowledge from the incident to make employees, clients, stakeholders, and other involved personnel aware of the indicators of compromise, fair usage policies and procedures, and the process of reporting an issue with networking devices or applications. As noted above, such user awareness will help reduce the frequency of incidents and enable their early detection.

In short, a training and awareness program educates employees on how to handle computer-related incidents and provides them with the skills required to implement incident handling policies. All teams should be trained according to their roles, responsibilities, and specific tasks. To be sure, training should include a report of actions that may adversely impact the organization. Practical training removes developmental errors, improves procedures, and reduces the occurrence of miscommunication: well-trained IH&R team members can significantly limit damage or prevent an incident. However, it is important to note that a training program's effectiveness increases only with proper program planning, implementation, maintenance, and evaluation.

Some important factors in a training and awareness program's success include:

- Identifying the scope, goal, and objective of the program
- Identifying the training staff
- Identifying the people to be trained
- Inspiring employees and management to adhere to security awareness norms
- Effectively managing the program
- Program maintenance
- Continuous evaluation and enhancement of the program

Security awareness and training should include:

- Planning and designing the training and awareness program
- Developing awareness and training materials
- Updating and analyzing the efficacy of the training program
- Implementing the program
- Building study material
- Measuring the effectiveness of the program and updating it

A comprehensive training program for all employees is necessary after updating the incident handling plan. The purpose of conducting training and exercises is to ensure that first responders are adequately prepared by up-to-date and quality training material. The following are several practices essential for the quality control of training materials.

Conduct training at specified intervals and educate employees in:

- Identifying incident handling locations
- Identifying pre-assignment emergency handling plans for all employees
- Recognizing and operating the utility shut-off devices

Conduct internal and external awareness campaigns to:

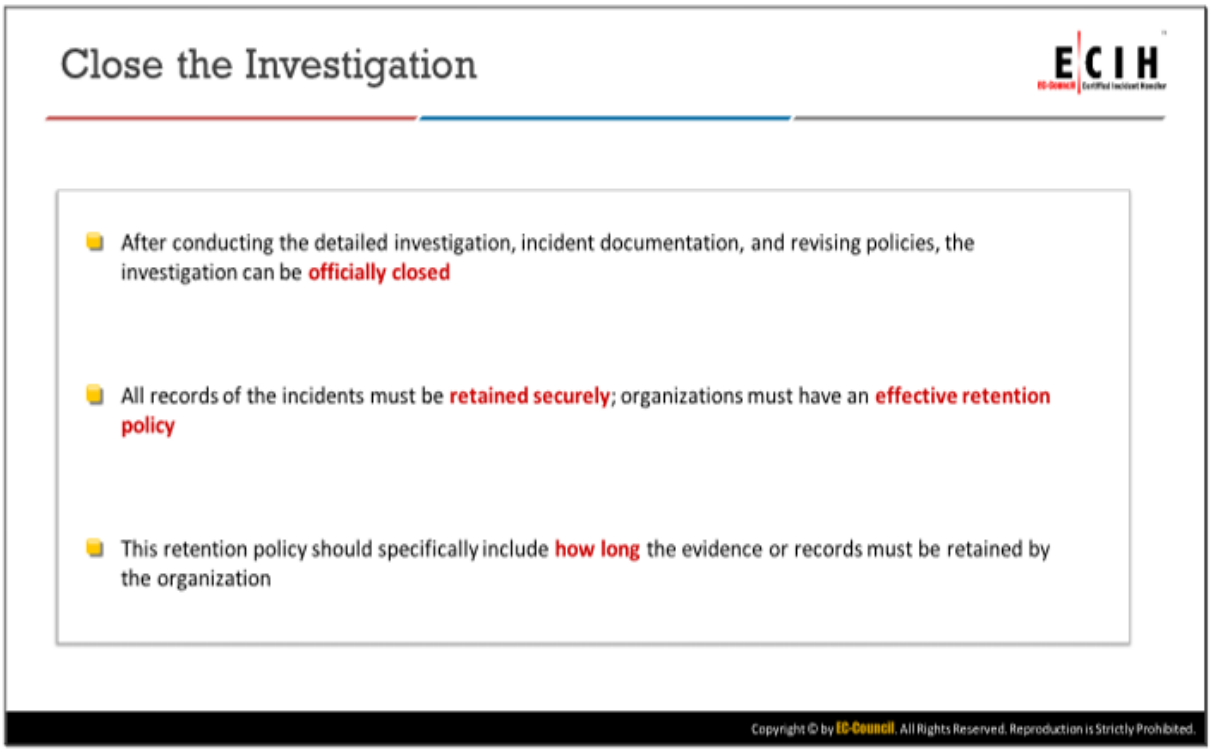
- Generate awareness among all parties
- Provide knowledge and encourage all parties to participate in the events
- Teach the plan strategies

Design the awareness campaign to facilitate:

- Participation
- Knowledge of the plan's strategies
- Knowledge of contingency arrangements

Generate awareness among employees with the following considerations in mind:

- Training is necessary to create awareness and preparedness among staff and team members
- Testing procedures can generate awareness among employees and executives



Close the Investigation

After conducting a detailed investigation, documenting the incident, and revising relevant policies, the investigation can be officially closed; management should be informed that the investigation has closed.

All records of the incidents must be securely retained and the organization should have an effective retention policy. This retention policy should specifically include how long evidence and records should be retained by the organization.

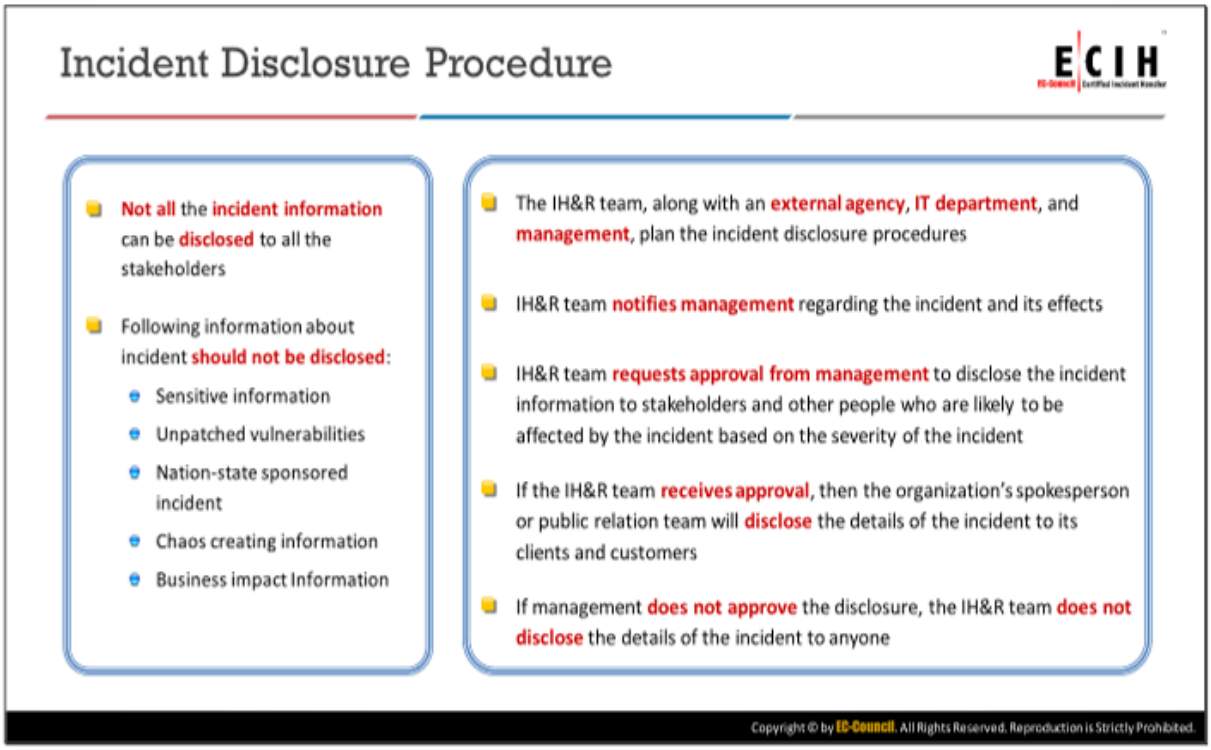
This stage will be followed by the disclosure of the details of the incident to public parties.

Incident Disclosure

After closing the investigation, the incident disclosure takes place. An organization hit by a security incident needs to disclose the incident's details to various entities. Ultimately, at this stage an organization will decide what details to disclose to respective stakeholders. The disclosure procedure varies by company and stakeholders. An IH&R team must consult its legal department before sharing any information with external entities.

The following is a list of possible entities that may be interested in information related to such a cyber incident:

- Law Enforcement
- Regional Judiciary
- Regulatory Authorities
- Media
- Stakeholders
- Stockholders
- Breach Victims
- Vendors
- Customers
- General Public
- Third Parties
- Other CERTs/CSIRTs



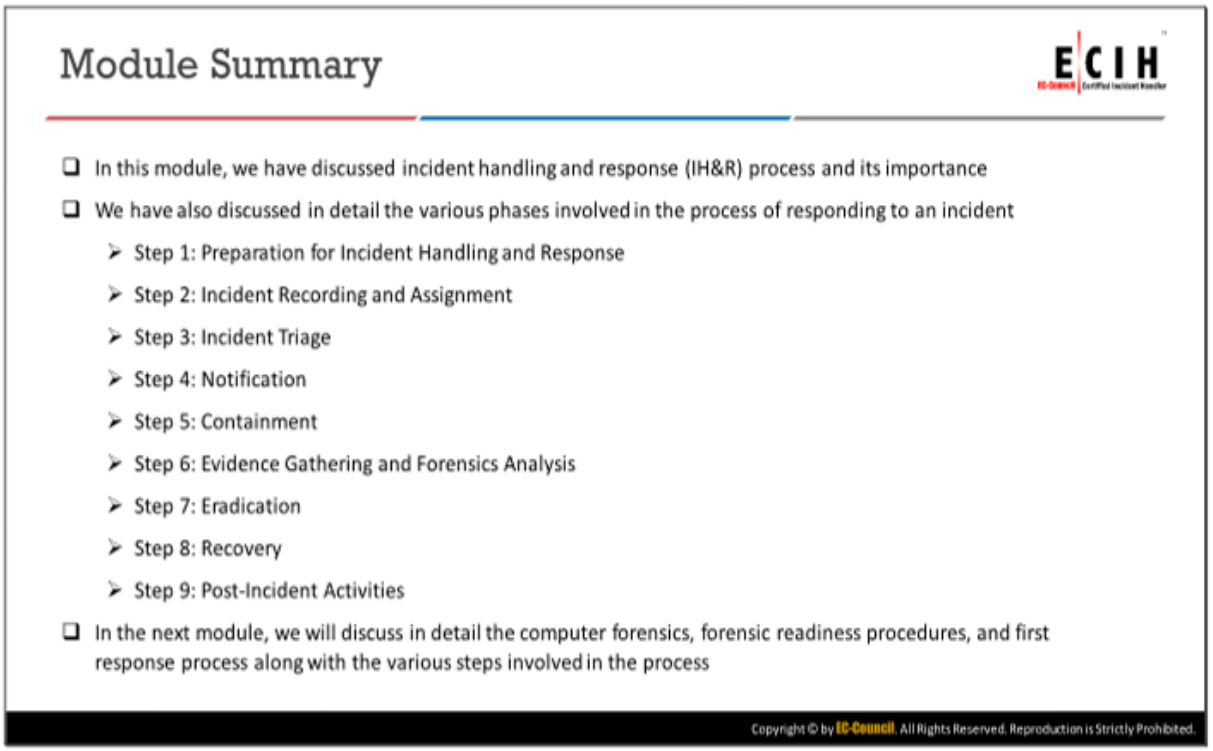
Incident Disclosure Procedure

Not all incident information can be disclosed to all stakeholders. Disclosure involves categorizing and filtering information before communicating it to different entities. Some of the measures that should be considered by an IH&R team before disclosing incident information are listed below:

- Sensitive information about the breach, which can include financial data (e.g., credit card details) and user account credentials, should not be disclosed.
- Unpatched vulnerabilities should not be disclosed.
- Nation-state sponsored incidents should not be disclosed to all stakeholders. Only limited entities should be given such information.
- Incident information, which can cause chaos among the public, should not be disclosed until and unless the information is highly necessary.
- Incident information that impacts the business should not be disclosed.

The procedure involved in disclosing the incident includes:

- The IH&R team, along with an external agency, IT department, and management plans the incident disclosure procedure.
- The IH&R team notifies management regarding the incident and its effects.
- The IH&R team requests approval from management to disclose incident information to stakeholders and others in the scope of the attack based on the severity of the incident.
- If the IH&R team receives approval, then the organization's spokesperson or public relations team will disclose the details of the incident to its clients and customers.
- If management does not approve the disclosure, then the IH&R team does not disclose the details of the incident to anyone.



Module Summary

In this module, we have discussed the complete IH&R process that organizations must implement to face, fight, and prevent different types of attacks. This module offers brief details about the process of determining the need for an IH&R process and the future course of action for establishing, managing, and strengthening IR capabilities.

This module also sheds light on the process of preparation by explaining the methods necessary for implementing an effective IR plan, using a ticketing systems, and classifying and prioritizing incidents with a structured approach.

In addition, this module clarifies the processes involved in analyzing incident indicators, containing and eradicating incidents, gathering evidence and conducting forensics investigations into incidents, and the post-incident activities that can help organizations to improve their defenses against and responses to future attacks.

In the next module, we will detail computer forensics, forensic readiness procedures, and the first response process along with the various steps involved.