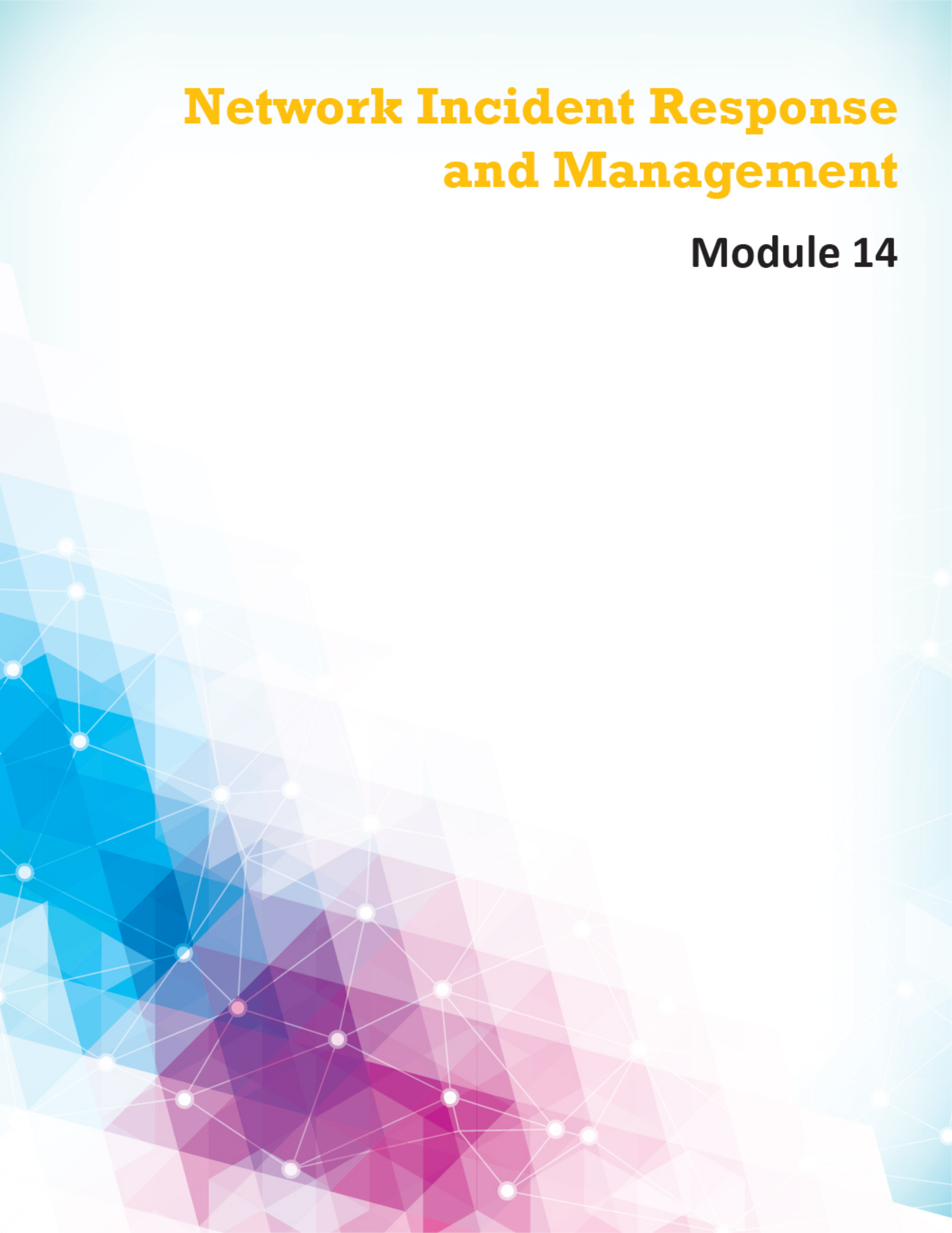


Network Incident Response and Management

Module 14



Network Incident Response and Management

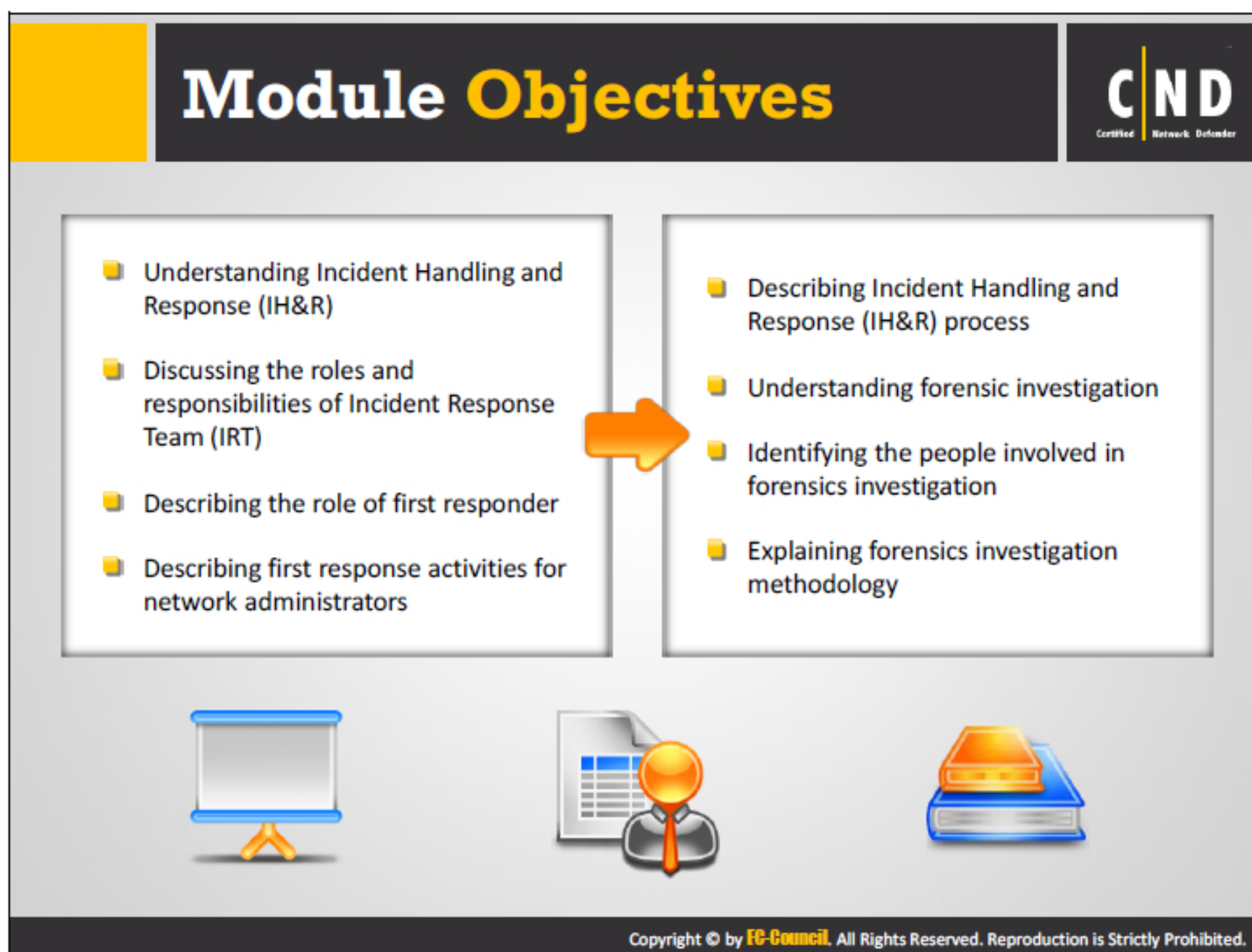
Module 14



Certified Network Defender

Module 14: Network Incident Response and Management


Exam 312-38



Organizations must deal with various security incidents which may compromise their network, data or physical security. These security breaches decrease an organization's brand value and cost the company millions of dollars. These negative repercussions often are responsible for the loss of prospective customers. A proper incident handling and response management plan will help an organization handle and recover from security incidents. This saves an organization from financial loss and reputation damage.

This module focuses on incident response and management. It will teach you the various steps involved in incident response and the management required to deal with problems. This module also describes the importance of the first responder in an incident response and management process.

Incident Handling and Response



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

Involving a sequence of steps beginning when an incident is first **identified** and **reported**

IH&R processes differ from organization to organization according to their business and operating environment

The **Incident Response Team (IRT)** works on an incident response plan when dealing with a security incident

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident handling and response is a set of procedures, actions and measures taken against an unexpected event occurrence. The purpose of incident handling and response is to quickly and efficiently recover from a security incident. It is required to identify any attacks which have compromised personal and/or business information.

Incident response is required to:

- **Protect systems:** Protect the computers used either by an organization or an individual from future incident attacks.
- **Protect personnel:** Protect the personal information and data stored in the compromised system.
- **Deal with legal issues:** To efficiently handle legal issues to stop future incidents.
- **Efficiently use the resources:** Ensures organizational resources are used efficiently by legitimate users.

Incident handling and response involves three major actions:

1. **Incident analysis:** The detection and confirmation of incidents.
2. **Reporting Incident:** Reporting the incident to management, in-house staff or an external IRT.
3. **Incident response:** A series of steps to contain, investigate, eradicate and recover from security incidents.

Incident handling and response (IH&R) goals and advantages:


- **Goals:**

- To detect if an incident occurred and if it is an actual security incident or a false positive.
- To maintain or Restore Business Continuity.
- To reduce the impact of an incident.
- To analyze the cause of an incident.
- To prevent future attacks or incidents.
- To improve security and incident response.
- To prosecute illegal activity

- **Advantages of Incident Handling and Response:**

- Equips the organization with safe procedures to be followed when an incident occurs.
- Saves time and effort, which is otherwise wasted when fixing an encountered incident.
- Helps the organization learn from past experiences, and then recover from losses more quickly.
- The skills and technologies required to tackle an incident are determined in advance.
- Saves the organization from legal consequences arising from a severe incident.
- Helps determine similar patterns in incidents and handle them more efficiently.

Incident Response Team Members: Roles and Responsibilities



Depending on the organization, an **in-house** or an **external IRT team** will hold different titles, roles and responsibilities for an incident response.

Management	A individual or group of individuals from a management team who has leadership and decision-making authority
Information Security Team	An individual from the information security team who has experience in discovering and containing incidents
IT Staff	An individual who is aware of the information system and network areas. They may be system or network administrators
Physical Security Staff	An individual who is responsible for the physical security and identifying the extent of any damage
Attorney	An individual responsible for providing legal advice
HR Representative	An individual responsible for handling employee issues who were involved in an incident

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

An IRT is responsible for handling and responding to security incidents. The IRT is broadly classified into in-house IRT (internal) and External IRT.

Internal IRT

An internal IRT offers its incident response services to its own organization.

National IRT

A national IRT focuses on providing its complete services for its nation. For example: The Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).

Coordination centers

Work across various IRTs to coordinate and facilitate incident handling. They do this for any particular country, state, research network, or entities.

Analysis centers

The main aim of an analysis center is to find out the latest trends and patterns occurring in incident activities and for creating data points across various sources. This information helps predict future activities and/or provides a warning when present activities match up to the previous determined characteristics.

Vendor teams

Vendor teams coordinate with the organizations who report and track vulnerabilities. There are also vendor teams that provide incident handling services internally for their particular organizations.

Incident response providers

Incident response providers grant assistance regarding incident handling services to paid clients.

Incident Response Plan

The IRT team creates an incident response plan before handling and responding to the incidents. An Incident Response Plan (IRP) is a set of guidelines which are required when responding to an incident in a dedicated and formal manner. The plan contains the elements required for executing the incident response effectively. These plans include response instructions for any detected incidents. The IRP includes the company requirements such as size, structure and functions. The plan identifies the resources required for managing the incidents.


- An IRP should include:
 - Aim of incident plan
 - Objectives and approaches
 - Methodology to incident response
 - Standards to assess incident response efficiency
 - Observing the current status of incident response
- Components of an IRP:
 - Name and contact information of the incident response team
 - System details such as data flow diagrams and network diagrams of the incident
 - The complete process required while recording and handling an incident
 - Report security incidents to the Information Security and Policy (ISP), who appoints a security analyst to handle the incident
 - Respond to the incident in a timely manner

The IRT team works on the pretext of the first responder of the incident. Typical roles and responsibilities of IRT members may vary based on the organization's incident handling and response activities.

- **Management:** In an organization, management is the top-most authoritative decision makers. It may include a single entity or a group of entities who are required to make decisions during the time of an incident. Management should be the first entity aware of

when an incident occurs. The management decide the steps to be taken after the detection of an incident is confirmed.

- **Information Security Team:** The team consists of the group of individuals who have the skills to detect and analyze security incidents. They can easily identify the nature, category, and scope of the incident.
- **IT Staff:** IT Staff are the individuals who are either a system or a network administrator. They detect the incident by analyzing network traffic, system logs, service packages and patches, etc. and report it to management or IRT. They can execute first response step to avoid further damage.
- **Physical Security Staff:** The Physical security staff contributes to the handling and response to physical security incidents. They can also be a first responder to a physical security incident. The staff actively report the occurrence of the physical security incident such as fire, theft, damage, and unauthorized access to management.
- **Attorney:** Attorney is a legal advisor for the organization. An attorney plays a major role in dealing with making sure any evidence collected is admissible in a court of law. They can also help an organization recover from a financial loss due to an incident.
- **HR Representative:** An internal employee may be involved in a security incident. In these situations, HR becomes involved when the IRT detects an internal employee is involved in the security incident. HR provides IRT with a best possible solution for dealing with any employee involved in an incident.

Incident Response Team Members: Roles and Responsibilities (Cont'd)		CND Certified Network Defender
PR specialist	An individual responsible for conveying company details after an incident	
Financial Auditor	An individual who assesses the financial loss to a company from an incident	
IR Officer	An individual responsible for all actions of the IR Team and IR Function. They may be an executive level employee, such as a CISO, or another corporate representative	
IR Manager	An individual who receives the initial IR alerts and leads the IR Team in all the IR activities	
IR Assessment Team	A group of individuals who make decisions on the classifications and the severity of the incident identified. The team is comprised of representatives from IT, Security, Application, Support and other business areas.	
IR Custodians	An individual responsible for the remediation and resolution of the incident which occurred. They are made up of technical experts and application support representatives	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

PR Specialist

This department serves as a primary contact for the media and informs the media about an event. They update the website information, monitor media coverage, and are responsible for stakeholder communication including:

- Board
- Foundation personnel
- Donors
- Suppliers/vendors

Financial Auditor

The Financial Auditors are the individuals who assess the financial loss of the organization after an incident. It is the responsibility of the auditor to include each and every loss which occurred as a result of the incident. The Auditor is responsible for reporting the financial imbalance in the organization's account.

IR Officer

The IR officer is an individual who oversees all the incident response activities in an organization. IR officers are an executive employee who is responsible for how the IR Team functions. Every action conducted by the IR Team is reported back to the IR Officer who further reports to the management of the organization.

IR Manager

The incident manager must be a technical expert who understands security and incident management. The Incident Manager focuses on the incident and analyzes how to handle it from a management and a technical point of view. They are responsible for the actions performed by the incident analysts and report the information to the incident officer.


IR Assessment Team

They are the individuals who prioritize the occurrence of an incident on the amount of loss it caused to the organization. The team comprises individuals from various domains such as, IT, security, application support and other business areas.

IR Custodians

They are either technical experts or application support representatives. The role of IR custodians comes into picture during a time of an application incident. To provide a remedy of the incident, IR custodians create an action framework which is further shared to the management.

First Responder



- A First Responder is an individual who arrives first to the crime scene and **brings the incident to the attention of others**
- They could be an end user, network administrator, law enforcement officer and/or an investigation officer.
- The first response includes the following roles and responsibilities: (depending on who is the first responder)

I Reporting the incident	IV Identifying the crime scene	VII Documenting all the findings
II Alerting the management and incidence response teams	V Collecting the complete information about the incident	VIII Preserving temporary and fragile evidence
III Containing intrusion	VI Protecting the crime scene	IX Packaging and transporting the electronic evidence

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The term first responder refers to the people who arrive first at the crime scene and gain access to the victim's computer system after the incident report. A first responder may be a user, network administrator, law enforcement officer, or investigation officer. They are responsible for protecting, integrating, and preserving any evidence obtained from the crime scene.

The time gap between the occurrence of an incident and transference of evidence is an important aspect in incident response. It is the responsibility of the first responder to keep up the reliability and liability of the evidence. The method accepted by any first responder is very important in preserving the evidence and finding the attackers. The first responder needs to have a dedicated and well-organized plan when responding to any type of incident. It is the first responder who collects the initial information, determines the extent and impact of the attack or incident. This allows other people involved in handling the incident to determine other courses of action which may be required for investigating the incident.

An experienced first responder can easily apply good forensic techniques when they respond to an incident in the initial stages. They can predict the extent to which any change in the evidence may affect the further investigation. This proficiency is an extra add-on in maintaining the availability, integrity and reliability of the evidence. The first responder needs to always understand the importance of their role as it highly affects the security and efficiency of the organization.

The role of any first responder is to prioritize according to the severity of the incident, gather evidence for the incident which has occurred, and conduct fewer experiments on the suspected devices. This will ensure enough data is provided for the other investigators to solve the issue.


Also, the first responders should be trained to gather evidence without changing any of the services running at that moment. Evidently, this is a critical task for the first responders as they have to gather evidence before it is lost.

It is not mandatory that every evidence gathered may lead to a complete investigation of the incident. However, first responders need to have the complete picture of the methods used in handling the incident in the initial stages, as different incidents require different methods of approach.

First Response Rule

- Under no circumstances should anyone, except the forensic analysts, make any effort to collect or recover the data from any computer system or electronic device that holds electronic information.
- Remember, any information present inside the collected electronic devices is probable evidence and should be treated accordingly.
- Any attempts to retrieve data by unqualified individuals should be avoided. These attempts could either compromise the integrity of the files or result in the files being inadmissible in legal or administrative proceedings.
- The workplace or office must be secured and protected to maintain the truthfulness and quality of the crime scene and the electronic storage media.

Network Administrators as First Responder



- Network administrators spend a lot of time in **network environments** and are familiar with the network traffic, performance and utilization, network topology, location of each system, security policy, etc.
- They play a **key role** as a first responder when security incidents occur. They can detect the source of the incident and determine the systems which are affected.
- If they are not aware of the incident response procedures, any response to the incident will be **delayed**. This can and most often does **increase the potential impact** and evidence is more often than not corrupted and/or lost

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Network administrators generally act as first responders to many security incidents in an organization. The main responsibilities of the first responder include finding the source of the incident and preventing the infection from spreading to other systems. The role as a first responder can be hectic. However, the decision taken by any first responder can prevent an attack going haywire.

It is the network administrator who has the knowledge of network topology, network traffic, important assets and information system of the organization. They can easily detect the type of incident, severity, and location in an organization. They are expected to be completely equipped with all the tools and knowledge required for dealing with an incident as a first responder. This is a major reason why network administrators must have good knowledge regarding incident response and forensic investigation procedures. Ultimately, a first responder is responsible for gathering all the information and preventing evidence tampering. This is to ensure any evidence collected can be useful during legal proceedings.

Responsibilities of a network administrator as a first responder include:

- Monitor network and systems for intrusions.
- Identify all vulnerabilities in the network and systems.
- Create a set of rules and procedures in order to handle incidents.
- While handling an incident, they must have knowledge regarding legal proceedings.

What Should You Know?



You should review the organizational **incident response plan**, which contains the following:

- ✓ Names and contact information of the **local IRT**
- ✓ **Escalation** procedures
- ✓ Procedures for **reporting** and **handling** a suspected incident
- ✓ **Containment** actions for various types of Incidents

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

An organization should have an incident response plan which includes a set of procedures and actions required when responding to security incidents. The administrator must review the incident plan of their organization and suggest or implement changes to the incident response plan as required.

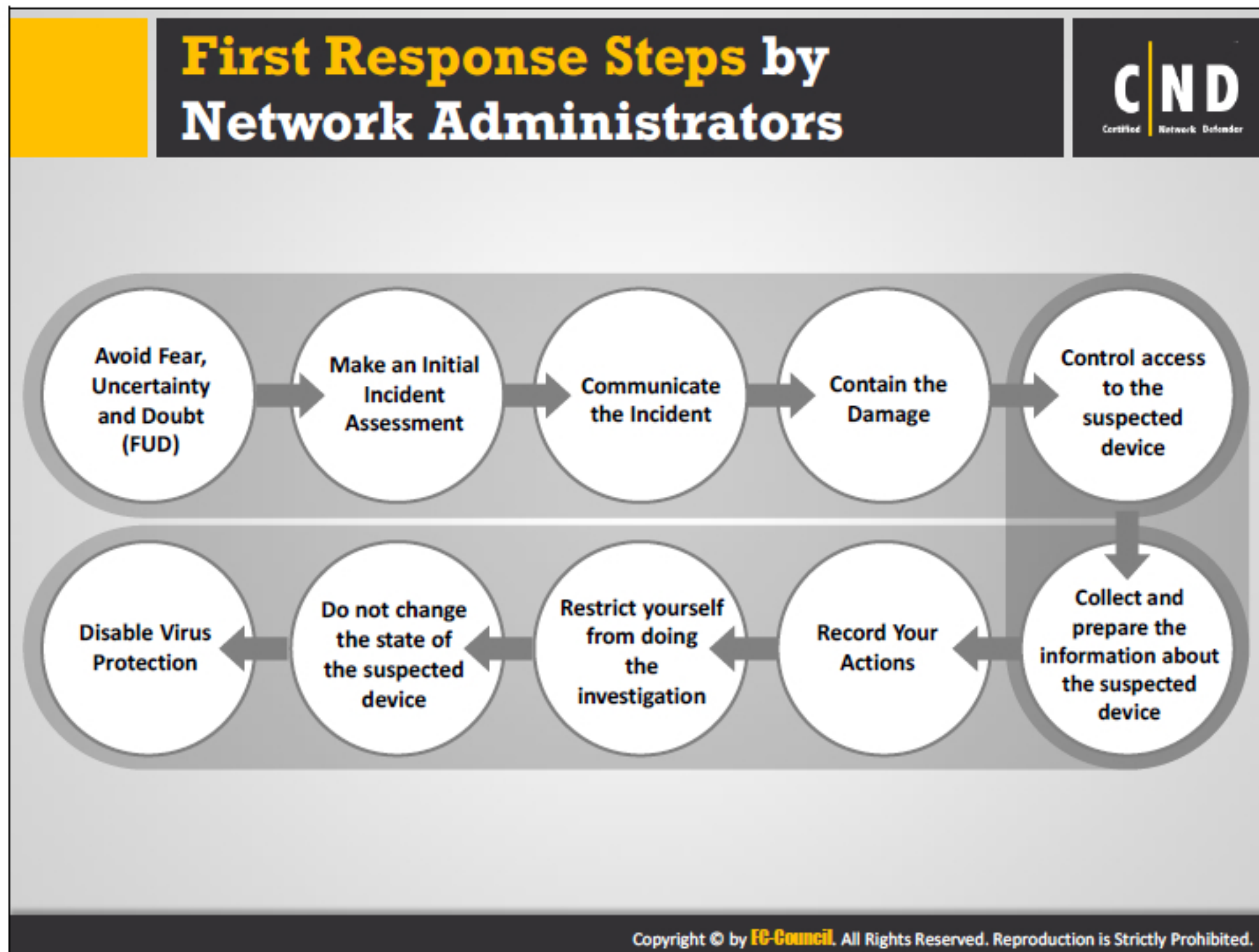
A typical incident response plan includes:

- **Contacts of IRT:** Contact information for the IRT team. It will help a first responder to immediately contact the IRT team when an incident occurs. Having IRT immediately on the location of the incident will help minimize any delay in responding to an incident.
- **Escalation Procedures:** First responders must know who to contact and report the incident to. There will be certain escalation procedures for the first responder which will help them report the incident without any delay.

Administrators collect and document certain information before escalating the incident. It includes:

- IP address and physical location of the affected systems
- Type of data on the systems
- Timeline of activities the system/user went through before the incident
- How the incident was detected
- Number of users affected

- **Procedure for reporting and handling an incident:** Network administrators must be aware of reporting and incident handling procedures.
- **Containment actions:** The incident response plan includes containment actions for all types of security incidents. Different containment actions are required for different types of incidents. Network administrators should be aware of containment actions for various types of security incidents. It helps to prevent further damage to an organization. Network administrators ensure evidence is not tampered with or completely lost during containment activities.




The biggest challenge facing an organization is the unavailability of a first response after the incident has occurred. Lack of knowledge or skills required for a first response will only make things worse for the organization.


If the first responder is not adequately trained or not aware of first response procedures, they will not be able to:


- Provide the expected first response to an incident.
- Escalate the incident properly.
- Contain the incident properly.

Avoid Fear, Uncertainty and Doubt (FUD)

CND
Certified Network Defender

 If you have discovered an incident, **do not panic**

 **Do not perform** actions which will damage the integrity of the evidence

 **Escalate** and **consult** with management or in-house computer forensics investigation team quickly


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

FUD is not a new concept for organizations. Any incident can create an environment of fear and anxiety among the team. A security incident outbreak is often very stressful, combined with lots of doubt and uncertainty. The decisions made in fear and anxiety will worsen the situation. Usually, small-sized companies do not have an incident response team. In such scenarios, the first responders usually lack the confidence required in dealing with an incident.

Providing a first response in fear or uncertainty can forego certain important and resourceful information related to the incident. If this happens, it can mislead the investigation team, causing delays in finding the reason the incident occurred. A decision made while panicking can affect the evidence quality.

You should be proactive and confident while providing a first response to an incident. If you are unsure about the decision to make during a first response, you should consult with top management, the information security team or the in-house IRT.

Make an Initial Incident Assessment



- If you found any indications of a security incident on your network
 - Check whether it is an **actual incident** or a **false positive**
 - Identify the **type** and **severity** of the security incident

Types of Incidents	Description
Unauthorized Access	An attacker gains unauthorized access to system resources
Denial of Service (DoS)	An attack resulting in the unavailability of services for authorized network users
Malicious Code	Malware (e.g. virus, worm, Trojan horse, keyloggers, spywares, rootkits, backdoors, etc.) infecting operating systems and/or applications
Improper Usage	Individuals in the organization using system resources against acceptable usage policies
Scans/Probes/Attempted Access	Activities undertaken by attackers to identify open ports, protocols, services, etc. for later exploit of an information system
Multiple Component	An incident which encompasses two or more incident types mentioned above

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The network administrator should conduct an initial assessment upon the occurrence of an incident which has been identified. An initial assessment helps you determine the following points:

- Source of the incident.
- Whether the incident occurred is a false positive or an actual incident.
- Able to decide the severity of the incident further helping to take immediate actions and minimizing the risk.
- Note down all the actions performed during the occurrence of the incident.

An initial assessment provides an outline for the type of attack that occurred. The information recorded in this stage is useful in containing the damage and avoiding risk. Further handling of the incident depends on the facts developed in the initial assessment phase.

Administrators should record information such as:

- Features of the incident
- Date and time the incident occurred
- Incident indication list
- Impact scope of the incident
- Nature of the incident or the type of attack

Determining Severity Levels

Low-Level Incidents

The least-severe incidents that are supposed to be handled **within one day** after the incident occurs

- Loss of personal password
- Unsuccessful scans and probes
- Request to review security logs
- Presence of any computer virus or worms
- Failure to download antivirus signatures
- Suspected sharing of the organization's accounts
- Minor breaches of the organization's acceptable usage policy

Middle-Level Incidents

Comparatively more serious than low level incidents and thus should be handled the **same day** the event occurs

- In-active external/internal unauthorized access to systems
- Violation of special access to a computer or computing facility
- Unauthorized storing and processing data
- Localized worm/virus outbreak
- Computer virus or worms of comparatively larger intensity
- Breach of the organization's acceptable usage policy

High-Level Incidents

Should be **handled immediately** after the incident

- Denial of Service attacks
- Suspected computer break-in
- Computer virus or worms of highest intensity; e.g. Trojan, back door, etc.
- Changes to system hardware, firmware, or software without authentication
- Destruction of property exceeding \$100,000
- Personal theft exceeding \$100,000 and illegal electronic fund transfer or download/sale

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Severity of an incident is an important measure of the impact on the security of an organization. It determines the urgency in handling an incident, level of expertise required in handling the incident and the extent of the response.

Severity of an incident is determined by:

- **Impact of the incident:** Determines the extent of the damage or impact of the incident on the organization.
- **Criticality of the service:** Determines the level of dependency of other services on the affected service.
- **Confidentiality of the information:** The severity of the information stored in the incident service.
- **Probability of spread:** The rate at which other systems or services are affected by the incident.

Organizations categorize the severity of incidents as:

- **High – Level Incidents:**
 - The incident has more chances of affecting a large number of systems or services in an organization.
 - The impact of the incident may lead to a financial crisis.
 - Affects the major functioning and operations of the organization.

▪ **Medium-Level Incidents:**

- The incident has a chance of affecting at least half of the systems or services in an organization.
- Affects a non-critical system or service.
- Disrupts the normal working of the organization.
- The incident has a tendency in propagating to other systems or service.

▪ **Low-level Incidents:**

- Affects only a few systems or services in an organization.
- Less chance of affecting the functional and operational aspects in an organization.
- No chance of propagating to other systems or services.

Communicate the Incident

CND
Certified Network Defender

If you suspect a **security incident** has occurred, you should be able to quickly identify who must be contacted inside and/or outside of an organization

You should quickly communicate the breach to the **in-house IRT Team** or **Management**

Your quick response will **minimize** the extent of the damage

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident response plan will include procedures and point of contact for communication of incidents. It may include:

- Clear idea of who to contact
- The contact team or person should be an expert in handling the incident
- A dedicated team for contacting any external team for incident handling

They contact these people or teams through phone, SMS, e-mail mentioned for immediate communication.

**Contain the Damage:
Avoid Further Harm**

CND
Certified Network Defender

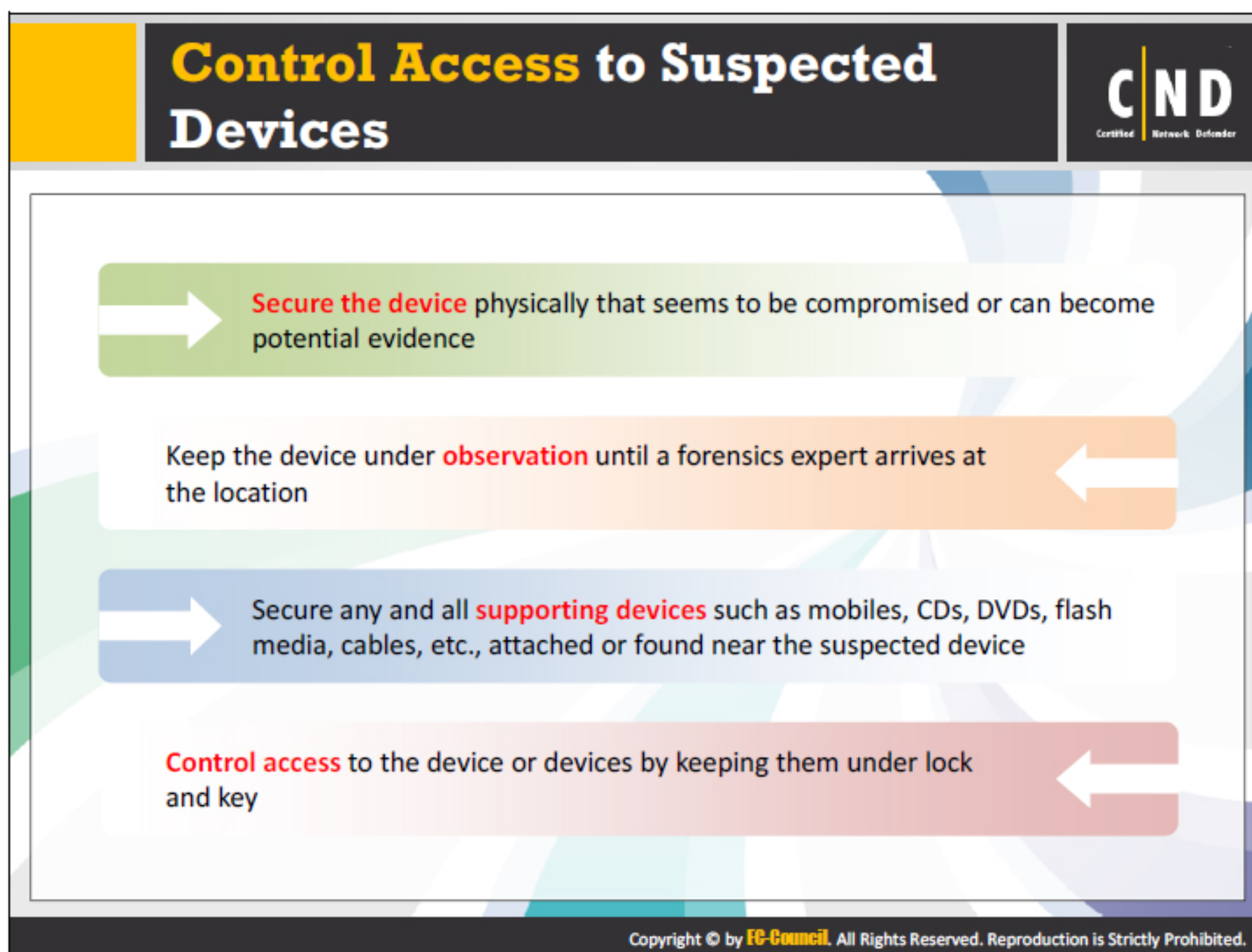
- Whether to disconnect the suspected device from the network or let it stay connected with the network. This must be decided by the forensic examiner or incident response team
- Both course of action may have **adverse** side effects on the forensics investigation
 - If you disconnect the device from the network when an attack is in progress, the forensic investigator may not find any evidence when it would have been found if connected
 - If you allow the device to stay connected to the network, it may cause further harm to your network, as the attack proceeds and is successful
- You should **coordinate** with the forensic investigation team to find any evidence and at the same time you should ensure it will not cause any further harm

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Administrators have to take appropriate care while containing the incident. The process for containing the incident may take on different approaches for different types of incidents.

Common actions that help administrators avoid further harm to the organization:

- Prioritizing components.
- Figuring out the sensitive data, hardware and software.
- Do not notify all employees regarding the incident.
- Distinguish the instances wherein the incidents need to be handled offline or online.
- Determine all the areas that are more likely for attack and implement methods to prevent it.
- Build a new system with all services and requirements with new administrative and service account passwords.




The administrators should understand the importance of securing the evidence during their first response. They should implement and execute certain preventive measures to control access to a suspected device:

- **Secure the device:** The administrators should securely maintain the devices that were compromised or was the source of the incident. These devices can be potential evidence during the time of an incident investigation.
- **Scrutiny of devices:** Administrators should keep the devices under observation and should not tamper with the devices until the forensic team arrives. Tampering with the devices can lead to loss of evidence thus affecting the incident investigation.
- **Secure supporting devices:** Apart from the suspected device, administrators should also gather all the other devices or media that were found near the suspected devices. Leaving any such evidence behind can change the course of an investigation action plan.
- **Control access to the device:** No other user or employee should have the access to the suspected or the evidence device.

The scrutiny of the devices depends on the first responder, any damage or tampering with the devices can affect the investigation procedure. If the premises can be locked down, the first responder should lock the premises, until the arrival of the forensic team.

Collect and Prepare Information about Suspected Device



- Note down all Information related to the suspected device
- It will help the investigator with the forensics investigation

You want to note the following information:

- Who, what, when and how the problem was discovered
- IP address
- System time
- System Name
- Services or applications running on the system
- Any other relevant information about the crime

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Administrators should collect and prepare any and all information relevant to the incident during their first response. Gathering firsthand information during this time is useful in the forensics investigation. It will be helpful for investigators if the first responder documents the changes the affected system went through from the time the incident occurred until the arrival of the forensic team. If the system is still on, administrators should note down all the information gathered related to the incident. This information can help the forensic team during their investigation.

- **Who, what, when and how the problem was discovered:** By notating this information it will help the investigator investigate the initial findings of the incident.
- **IP address:** An investigator is required to keep records of all IP addresses for all the affected machines. Such machines should not be connected to the network to avoid, replication of data.
- **System time:** Knowing the system time when the incident occurred is vital to an investigator. Using this information, they can monitor the changes the system is going through across the entire timeframe.
- **Running services or applications:** Incidents can be caused because of running applications or services on the system. It is necessary to keep a record of the services and applications as a result.

- **Any other relevant information about the crime:** An administrator must save any findings relevant to the incident. If any handwritten notes were found near the suspected device, the first responder should preserve the note and record the content as a copy, per the incident response procedures.

Record Your Actions





- Note down all actions you have taken upon discovering the incident
- It must be done for an **actual attack** as well as any **false positives**

The information you should take note of:

- Date/time of action
- Witnesses to support your action


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


The logs of the first responder should be in a descriptive manner. The responder should record the actions in a series. If the actions are not in chronological order, it confuses the investigator. Responders should avoid writing any speculations in their record. Only facts should be notated. As these are the most vital to uncovering the incident.

For example, do not document the action as, “The web browser started receiving various popups after the attack”. An ideal record of the action should be, “Unknown popups were displayed on a Google Chrome browser for thirty minutes after the incident occurred”.


If a network device or an external drive is also affected, the responder should note down the serial number or part number of the device. The first responder should also record the statements of the users whose system were affected by the incident.

Restrict Yourself from Doing Investigation







Refrain from starting the investigation too early



Evidence collection is a major part of uncovering an incident. Even though you may succeed in locating potential evidence, it will no longer be **admissible** in court



The integrity of the evidence is of utmost importance. If not collected properly it could be **lost** or even **destroyed** during evidence collection if not handled properly



A result of not doing this properly could very well put you in the direct line of fire regarding **legal punishment**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

First responders should not involve themselves in the investigation of the incident. If the first responder is not well-versed in the forensics investigation process or not trained on forensics investigation techniques, any attempt towards performing forensics can and most often leads to damage of any potential evidence. Even though the first responder might be aware of the reason for the incident, they should not proceed on their own. First responders should wait till the time they are authorized by the forensic team or management.

Even though the first responder carried out the forensics investigation and collected the evidence, the integrity of the evidence will no longer be valid in the court. This is because a first responder is not an expert with performing a forensics investigation. There is a chance the integrity of the evidence will be lost or tampered with. The evidence collected will no longer be accepted in court as it is not collected by an expert forensics investigator who normally ensures the evidence is collected in a forensically sound manner. Moreover, if first responders do so, the organization will be authorized to take legal action against the first responder.

Do Not Change the State of Suspected Device

Don't **change** the state of the suspected device

For example,

- If the suspected device is **ON**, then leave it **ON**
- If the suspected device is **OFF**, then leave it **OFF**


Changing the **state** may destroy any valuable evidence

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Tampering with the state of the suspected device is not advisable to the first responder. Altering the state of a system leads to massive changes in the evidence collected. Actions like system restart and system shutdown force the system to make internal changes thereby making it difficult for the investigators to properly investigate the incident. Any changes made to the state of the suspected device create adverse effects on the quality of evidence or can completely destroy the evidence. Make sure as a first responder you always leave the system in the same state as when the incident occurred.

For example, if the suspected device is ON, the first responder should not turn it off, till the time advised by the forensic investigator. If the suspected device is in a shut-down state, the first responder should not turn it on.

Disable Virus Protection



1

Antivirus software can **access** files or change its time/date stamp values during its automated scanning process

2

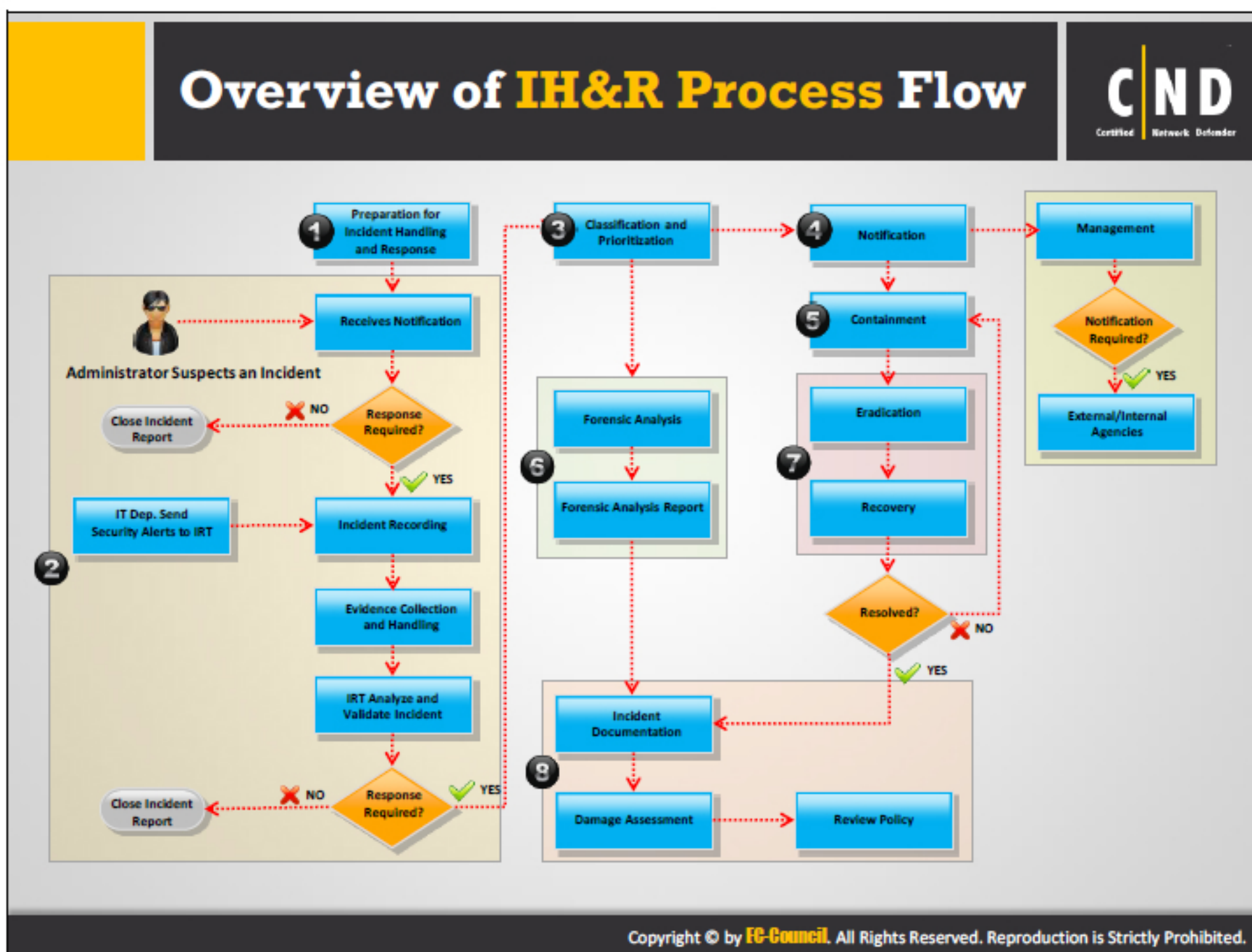
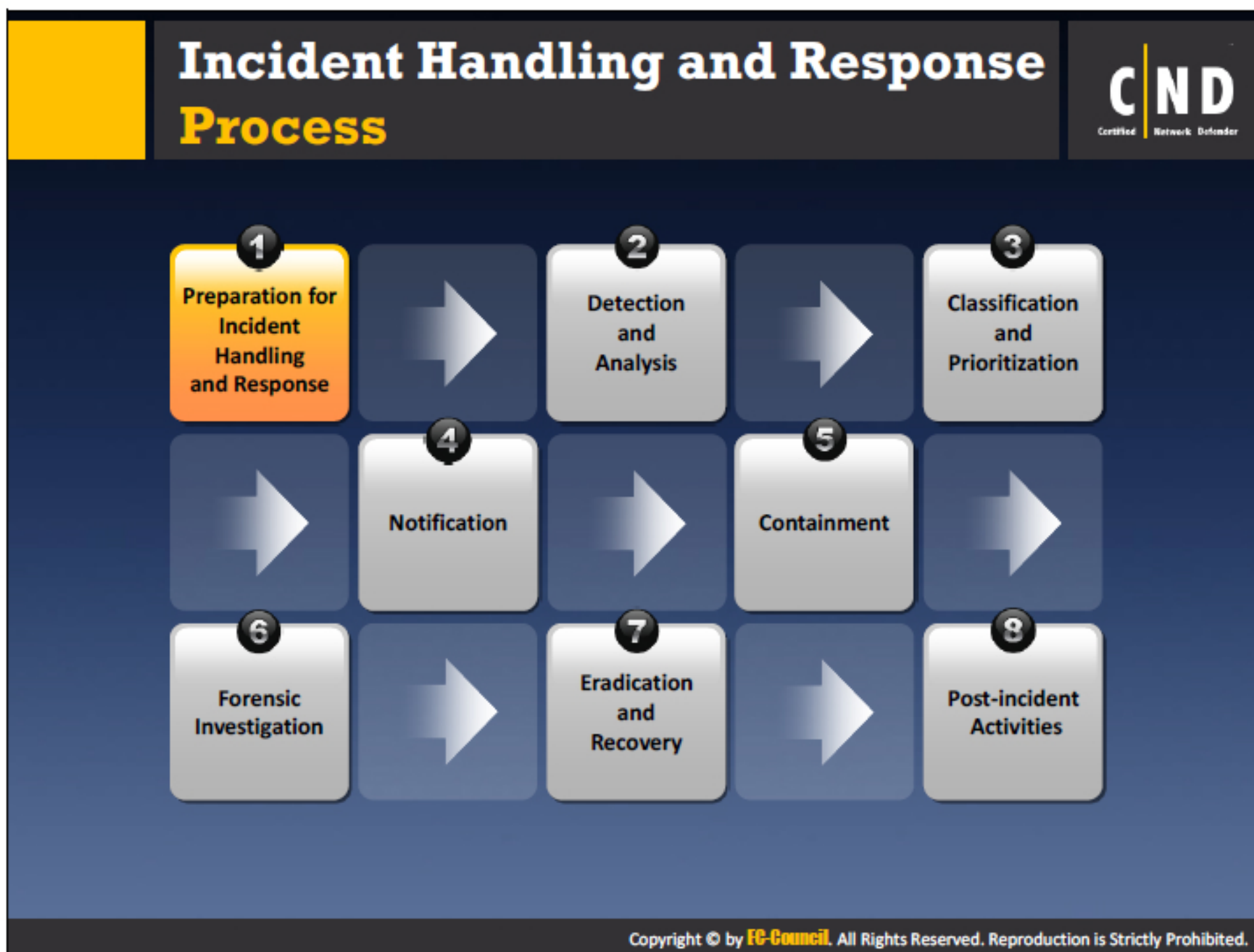
Some antivirus software can automatically **delete** suspected files, hacking tools, etc. present on the device

3

It may have **adverse effects** on the forensic investigation

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-virus software installed on a suspected system may create problems when collecting evidence during a forensics investigation. Antivirus software running on the system may delete or change the state of the evidence as it accesses each file and alters its timestamp. At times, it can even remove the files which are potential evidence. Hence, security experts suggest that a first responder should disable the virus protection systems as soon as they confront an incident.



Incident Handling and Response Process differs from organization to organization according to their business and operating environment. A framework is defined that can be utilized to create a sound incident handling response for your organization.

Every incident handling and response process clearly defines some of these rules. Some of them are:

- Restore the normal state of the system in the shortest possible time
- Minimize the impact of the incident on other systems
- Avoid further incidents
- Identify the root cause of the incident and try to rectify it in less time
- Assess the impact and damage of the incident and try to recover the corrupted or deleted data
- Update security policies and procedures as needed
- Collect evidence to support the succeeding investigation

Determining the Need for Incident Handling & Response (IH&R) Processes

Organizations determine the need of an incident handling and response (IH&R) process based on the current security scenario, risk perception, business advantages of having such processes, legal compliance requirements, other organizational policies, previous incidents, etc.

Cyber-attacks have increased in number as well as in diversity, and have become more damaging and disruptive. Since these types of attacks can be harmful and can gather all the personal and business sensitive data, it has become necessary to effectively and timely respond to these incidents.

The incident handling and response (IH&R) process will allow the organization to design preventive activities based on the results of risk assessments, but cannot prevent the occurrence of all incidents. IH&R processes are necessary for detecting the incidents, reducing any loss and destruction, mitigating the exploited weaknesses, and restoring IT services.

Inputs, complaints and queries from all the stakeholders involved in the organization's business processes affect the decision to establish an IH&R process. The organization's IRT development project team, executive manager, head of the information security department or any other person exclusively designated by the management can initiate the IH&R process.

The main purpose of incident response management and process is to:

- **Protect systems:**

It is difficult to place high levels of security and special access controls on various computing resources due to high costs and other constraints. The best strategy for computer systems and network protection is to quickly detect and recover from the security incident. An efficient incident response procedure ensures that critical business operations run as they would normally before, during and after an incident.

- **Protect personnel:**

A swift incident response helps in ensuring that no physical damage occurs to human resources due to any workplace incident.

- **Efficiently use resources:**

The resources available for handling an incident used by both technical and managerial personnel are always limited. The best way to utilize these resources is to respond to the incidents as quickly as possible. Information gained from the incident handling process helps prevent incidents or better handle future incidents and implement strong security for systems and data.

- **Address legal issues:**

Incident response is also necessary for legal compliance with different laws and acts such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA). Efficient incident procedures ensure that the organization remains safe against legal and public liabilities.

It is necessary to adhere to the legal principles and practices while responding to incidents. According to the US department of justice, it is illegal to use certain monitoring techniques for identifying the incident. The procedures to respond to an incident should guarantee non-violation of legal statutes.

Defining the IH&R Vision

The IH&R vision includes the purpose and scope of the planned incident handling and response capabilities. This vision features a set of instructions to detect, manage and respond to an incident. It defines the areas of responsibility and the procedures for handling various security incidents.

The vision includes the preparation of proper documentation and outlines a well-defined approach for handling incidents by taking the necessary preventive actions against any potential threats that may affect the information system. The incident response plan covers:

- How information passes to the appropriate personnel?
- How to assess an incident?
- Incident containment and response strategy.
- How to restore systems and resources in case of an incident?
- Documentation of the incident.
- Preservation of the evidence.
- How to report the incident to the appropriate personnel?

Key elements in the IH&R vision statement include:

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

Communicate the vision to all stakeholders and make sure it is published in an easily accessible repository after appropriate approvals.

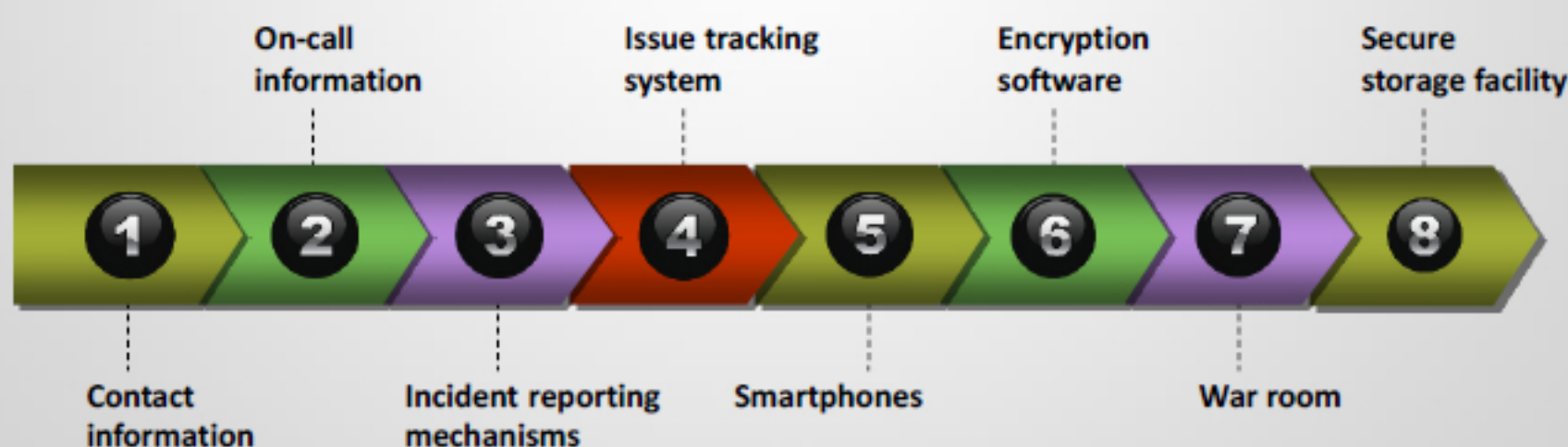
Preparation for Incident Handling and Response



- This is the initial phase involving the **establishment** and **training** of an incident response team as well as acquiring all the necessary tools and resources
- Per the results of a risk assessment, the organization **minimizes** the occurrence of certain **incidents** through the selection and implementation of specific controls
- There may still be a **residual risk** after implementing the controls, which is why organizations must be notified when incidents occur. Because detecting security breaches will still be required

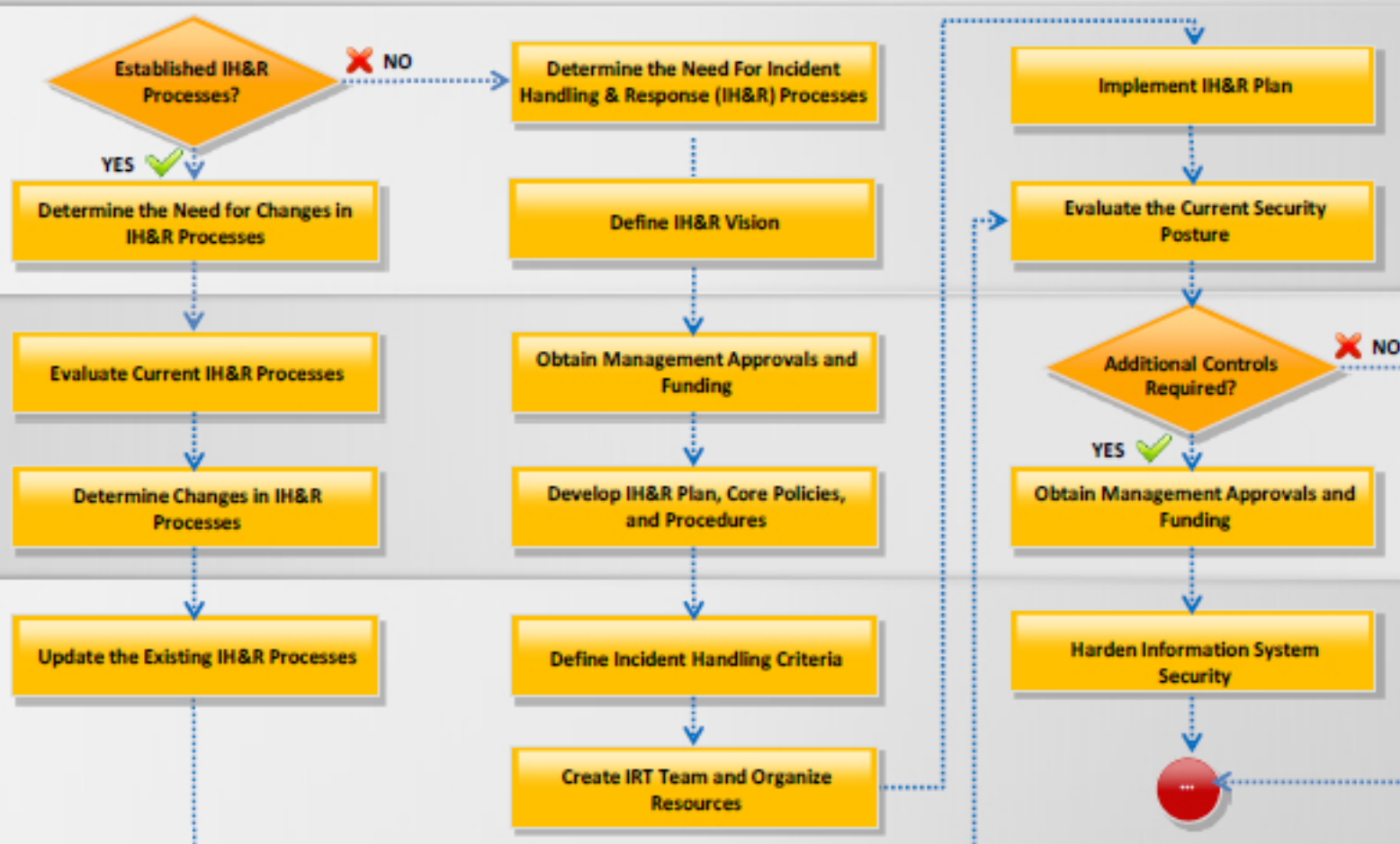
Preparing to Handle Incidents

The following are a list of tools and communication resources an incident handler needs:



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation for Incident Handling and Response (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Preparation for Incident Handling and Response

Preparation is the readiness to respond prior to an actual occurrence of an incident event. Requirements for preparation include:

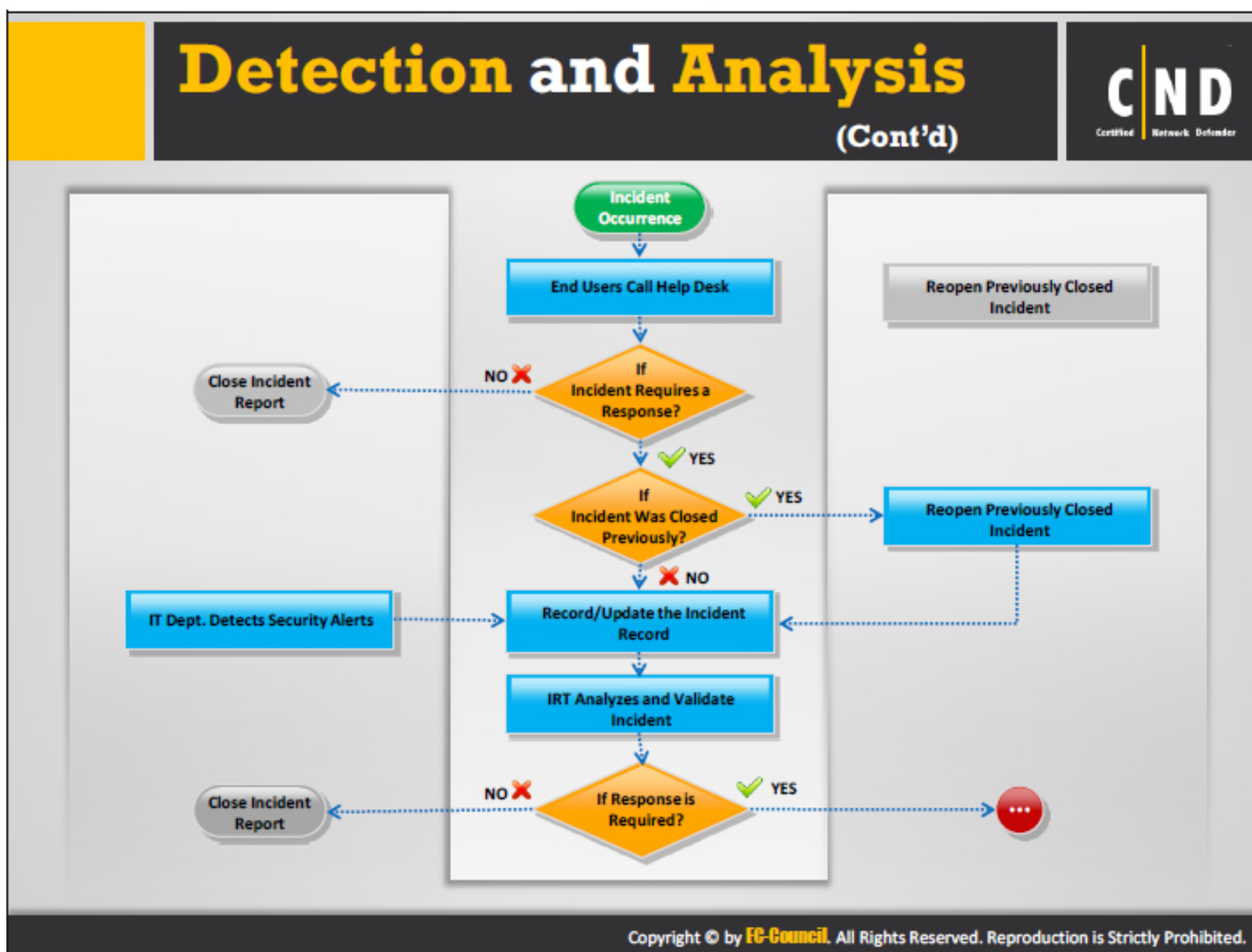
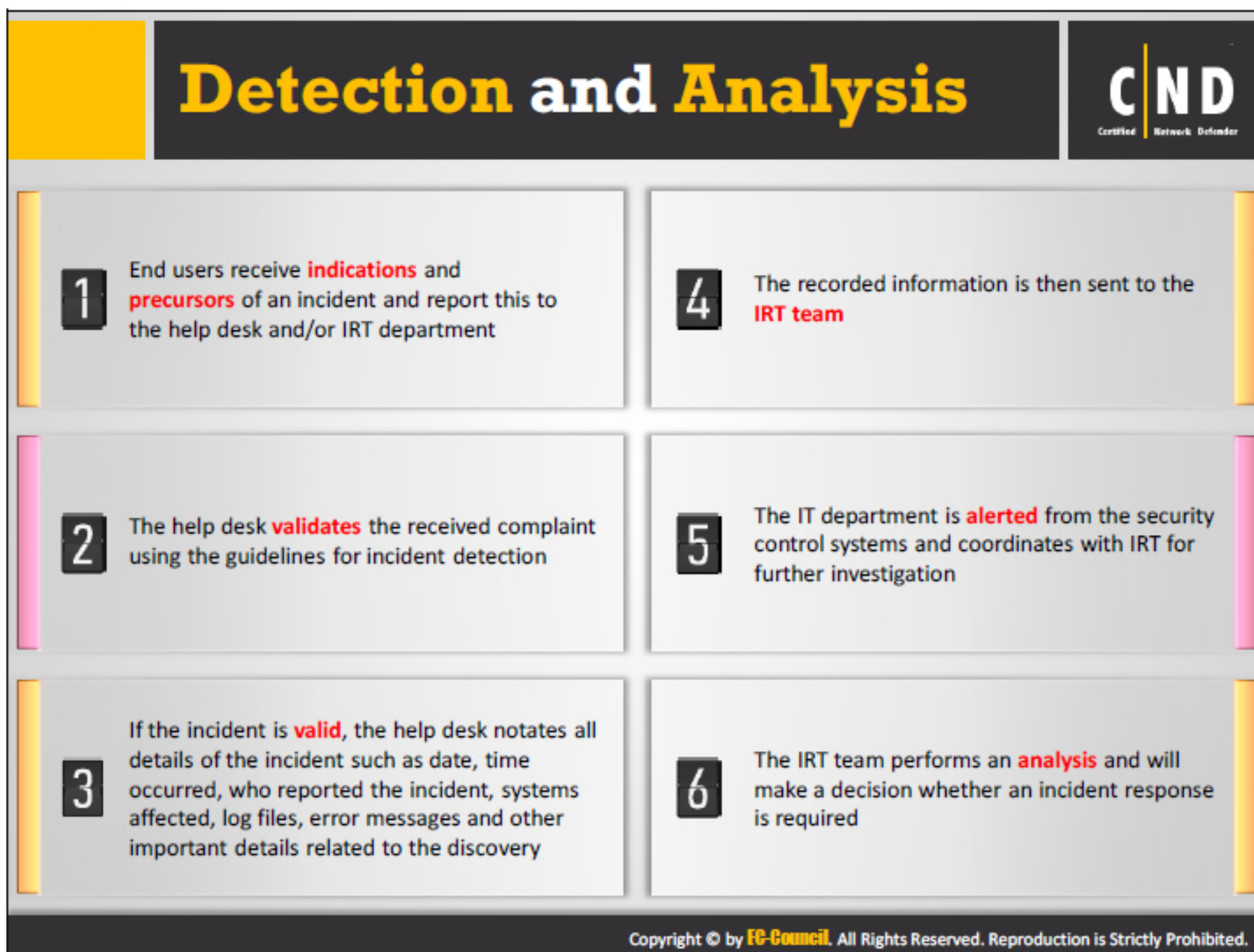
- Establishing a reasonable group of defense/controls depending on threats posed on:
 - Open systems that are vulnerable to attacks
 - Secured systems with no incident response
 - Systems dealing with incidents that are to be secured
- Developing a group of methods to deal with incidents:
 - Measures to be considered in different situations by the staff
 - Contact information
 - Keeping information from other neighboring organizations
 - Assigning people to participate in the incident response effort
 - Determine risk levels and limits
- Acquiring resources and people to solve problems:

Monetary resources are required for hardware, software, training, and special equipment for analysis and forensics. Examples of resources include: PDAs, safe vaults, IDS software, and database server software.
- Developing an infrastructure that supports incident response:

Overall business strategy should be developed to incorporate mechanisms into processes in order to respond to incidents:

 - Line of authority and management are to be in place
 - Defenses/controls specifically matching the resources of the network are to be chosen
 - Incident response procedures are to be well followed
 - Resources should be provided with proper finances
 - Maintenance of contact details
 - Evidence of incident responses are to be stored
 - Proper addressing of legal issues
 - System administrators are responsible for the preparation stage. Their responsibilities include:
 - Ensuring password policies
 - Disabling default accounts
 - Configuring appropriate security mechanisms
 - Executing and enabling system logging and auditing

- Patch management
- Ensuring proper backups
- Ensuring the integrity of file systems
- Identifying abnormal behavior in the system



Detection is identification of various types of security incidents for an organization. After an incident is detected and confirmed. The first responder collects the information and all details of the incident and communicates to IRT. For a meaningful incident response, detection and analysis of the incident is critical.

Sometimes it is useful to use certain detection software to detect security incidents. It may include IDS, antivirus, integrity checking software, etc. However, there are certain incidents that are clearly noticeable, so specific software is not required to detect them.

Some of ways for identifying the incident are as follows:

- Detection of anomaly in data packets sent across the network through the alarm generated by the IDS and firewall
- Displaying of antivirus alert while scanning a computer system
- System and network logs show repeated, unsuccessful login attempts.
- Data is unexpectedly corrupted or deleted.
- Unusual system crashes can indicate attacks. Attackers or intruders can damage the system that contains data important to the network.
- Audit logs show suspicious activity on the systems or network.
- System and security log files, log suspicious activity either on the network or security devices.
- Staff identifies unusual or suspicious activity on the computer system.
- Staff identifies content on a colleague's computer that violates the organization's security policy.
- Receiving of phishing emails or the company's website is defaced.
- History of activities during non-working hours shows that unauthorized access to systems has occurred
- Social engineering attempts

Incident analysis is performed after detection of an incident. Incident analysis may vary depending on the incident discovered.

Steps involved in incident analysis are:

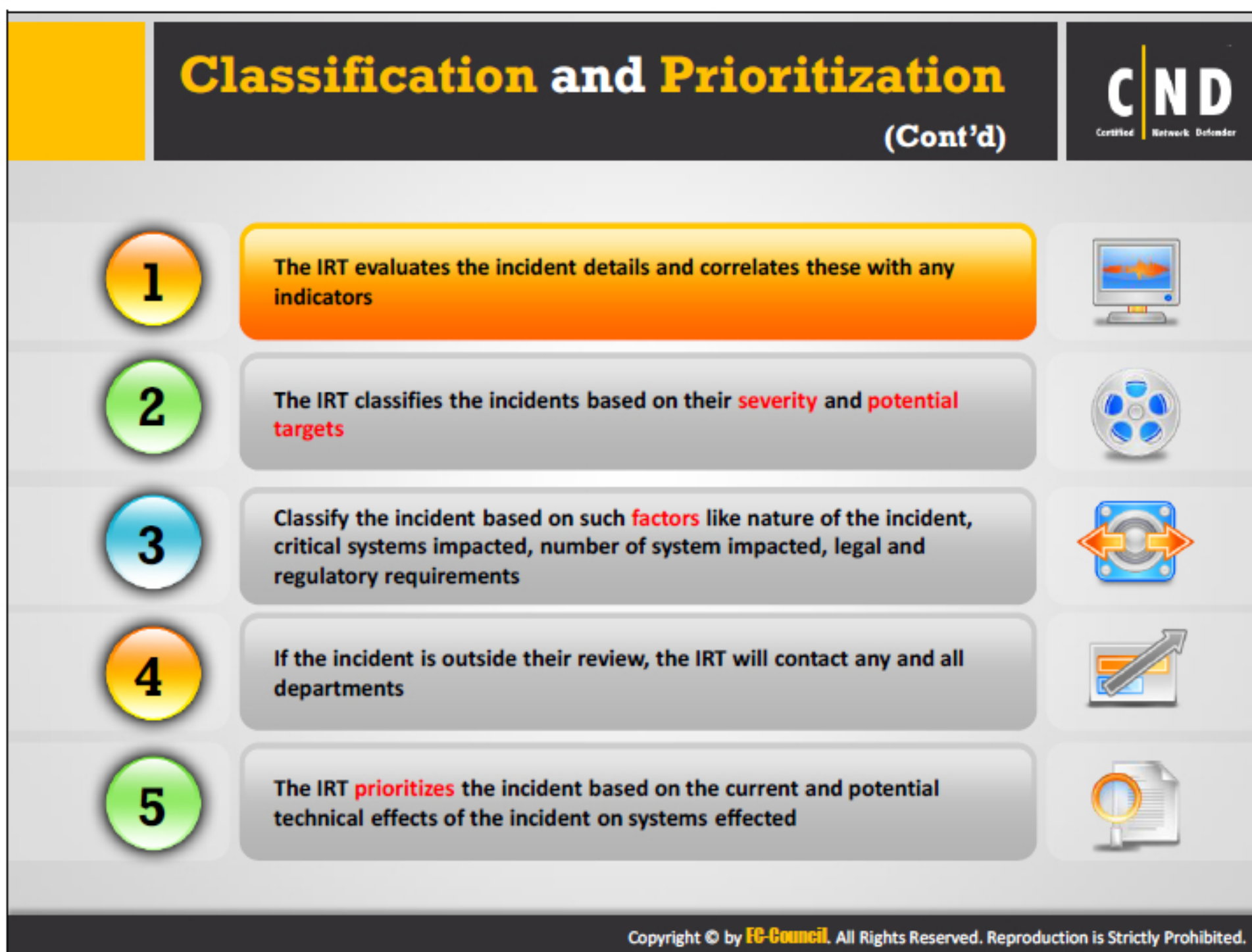
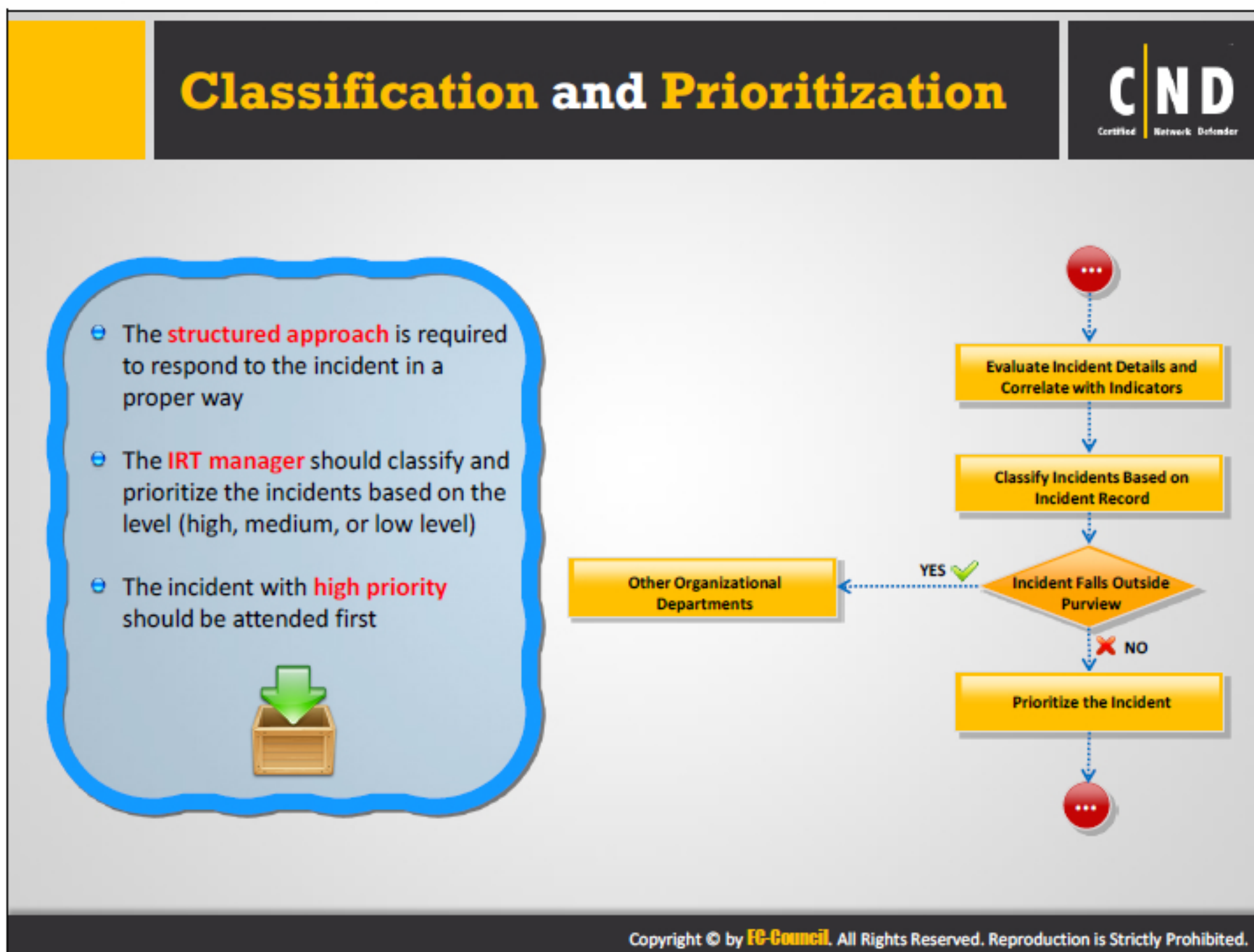
- Analyzing every anomaly found
- Auditing anomalies and maintaining a copy of compromised files for analysis
- Documenting the incident information for clear understanding

The information collected in this phase includes:

- The date and time the incident occurred as well as detection.
- Details of the person who reported the incident.

- Details of the incident, including:
 - Description of the incident.
 - Details on the systems effected.
 - Backup information such as error messages, log files, etc.
- Forward the recorded information to the IRT.

The IRT performs an analysis and decides whether an incident response is required.



The IRT evaluates the incident details obtained in an incident detection and analysis phase and correlates it with indicators. An IRT classifies and prioritizes a security incident based on the following factors

- Nature of the incident
- Incident severity and potential targets
- The criticality of the systems being impacted
- Current and potential technical effect of the incident and the criticality of the affected resources
- Number of systems impacted by the incident
- Incident falls outside the IRT's purview
- Legal and regulatory requirements

Upon detection of an incident, the IRT should categorize it appropriately based on its type, severity, and impact. Incident classification helps the IRT in taking appropriate necessary responses. Incident classification is done based on an incident categorization and incident severity rating.

Incident categorization

Incident categorization helps the IRT team keep incidents under a certain single category which provides better coordination and consistent incident handling and responses.

Incident severity rating

A Severity rating adds a sense of *urgency* to the detected incidents.

Incident classification helps the IRT quickly respond to incidents by avoiding any Operational mix-up.

According to the NIST, incidents can be categorized into seven categories. The NIST taxonomy for incident categorization is shown below:

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes /Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

*Defined by NIST Special Publication 800-61

FIGURE 14.1: Incident categorization according to NIST

According to FIRST, incidents can be categorized as shown in the figure below:

Incident Category	Description
Denial of service	DOS or DDOS attack.
Forensics	Any forensic work to be done by CSIRT
Compromised Information	Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	Spoofed email, SPAM, and other email security-related events.
Consulting	Security consulting unrelated to any confirmed incident.
Policy Violations	Sharing offensive material, sharing/possession of copyright material. Deliberate violation of InfoSec policy. Inappropriate use of corporate asset such as computer, network, or application. Unauthorized escalation of privileges or deliberate attempt to subvert access controls

FIGURE 14.2: Incident categorization according to FIRST

Incident severity rating:

The severity rating assists the IRT in categorizing incidents. Impact and Likelihood are the elements which form the building blocks for severity ratings. The following matrix is constructed using these two elements:

IMPACT	LIKELIHOOD				
	Rare	Unlikely	Possible	Likely	Almost Certain
Catastrophic	Medium	Medium	High	Critical	Critical
Major	Low	Medium	Medium	High	Critical
Moderate	Low	Medium	Medium	Medium	High
Minor	Very Low	Low	Medium	Medium	Medium
Insignificant	Very Low	Very Low	Low	Low	Medium

TABLE 14.1: Severity rating matrix

Advantages of an effective incident classification

- Every incident is correctly forwarded to the respective department.
- Enhances response times as the incidents are routed to the respective department.
- Aids in the development of an effective knowledge base.
- Increased customer satisfaction.

The graphic is titled "Incident Prioritization" in a large, bold, yellow font. It features a dark blue background with a grid of puzzle pieces. A large orange puzzle piece is in the center, containing a white funnel icon. To the left of the orange piece is a grey piece with a person icon, and to the right is a grey piece with a gear icon. Above the orange piece is a grey piece with a checkered flag icon. Below the orange piece is a grey piece with a funnel icon. The text "Incident Prioritization" is at the top left. The "CND" logo is at the top right. The text "Prioritizing the handling of the incident is critical for the process" is in the top left. The text "Incidents should not be handled on a first-come, first-serve basis" is in the top middle. The text "Prioritize the incidents based on two factors" is in the top right. The text "Current and potential technical effect of the incident" is in the middle left. The text "Criticality of the affected resources" is in the middle right. The text "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited." is at the bottom.

Incident Prioritization

CND
Certified Network Defender

- **Prioritizing** the handling of the incident is critical for the process
- Incidents **should not be handled** on a first-come, first-serve basis
- Prioritize the incidents based on two factors
 - Current and potential technical effect of the incident
 - Criticality of the affected resources

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

After classifying the incidents, the IRT should prioritize the incidents. The high impact incidents which could severely sabotage an organization's network should be attended first and their effects mitigated in the early stages.

The IRT should consider two basic elements in prioritizing incidents:

1. **Impact:** Gives an account of how severe an incident can be on the organization. It is measured in terms of the number of systems, impacted by the incident which in turn increases the number of employees being idle which directly affects the organization productivity.
2. **Urgency:** Is usually defined in terms of service level agreement (SLA). If an incident is raised within an organization, it should be resolved at the earliest opportunity.

The values for impact and urgency can vary from organization to organization. But generally, we can have three levels, which are high, medium, and low, both for Impact and urgency.

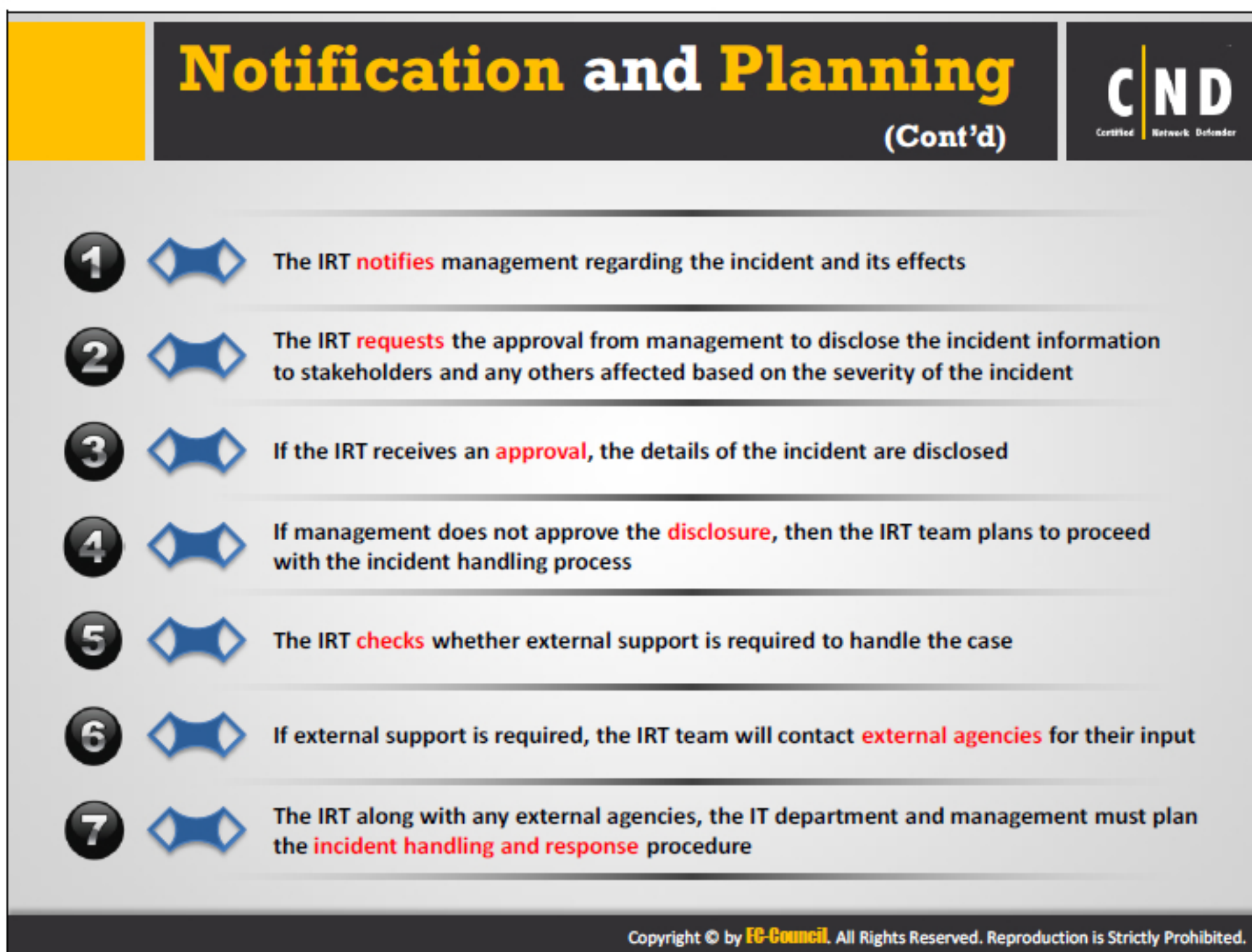
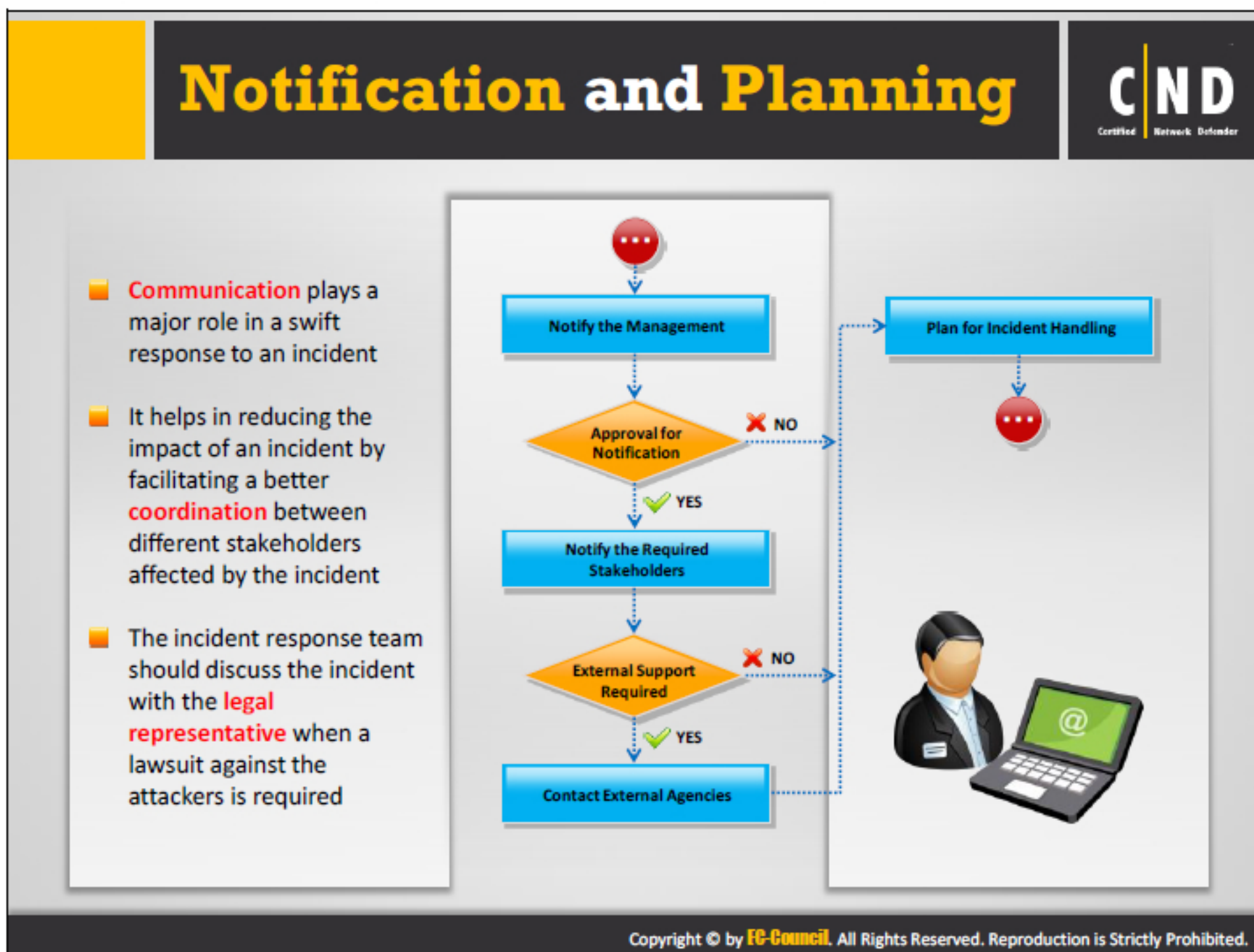
The IRT should construct an impact urgency matrix based on three levels of high medium and low as follows:

Impact → Urgency ↓	High	Medium	Low
High			
Medium			
Low			

TABLE 14.2: Impact urgency matrix

The priorities should be addressed by the IRT in the following order:

1. Red
2. Light yellow
3. Dark yellow
4. Light green
5. Dark green




An organization which is suffering from a security incident needs to notify the appropriate internal and external IRT to minimize any repercussions of the security event.

The IRT's role in the notification and planning includes the following:

- **Notifying management:** It is the responsibility of the IRT to notify management about the incident which occurred. The management should also be informed about the effects the incident caused.
- **Broadcasting the incident:** Before broadcasting any information about the incident, the IRT should have documented approval from the management. The incident information should not be hidden from the stakeholders and other people. People that are likely to be affected by the incident need to be informed about the incident.
- **Disclosing the details of incident:** Apart from broadcasting about the incident, the IRT should also seek approval for disclosing the details of the incident. Disclosing the details of an incident is important, as certain stakeholders of the organization are required to be kept in loop.
- **Approval denied:** If management does not give their approval for disclosing the incident details, the IRT should proceed with the procedure of incident handling.
- **External support:** Before proceeding with the in-depth investigation of the incident, the IRT checks if external support is required to handle the case.
- **External support required:** If external support is required, the IRT contacts external agencies for input.
- **IRT and external support:** Once the external support joins the investigation of the incident, the IRT and the management team proceeds with handling the incident and response plan.

Containment



1

2

3

4

5






1 The IRT, **technical**, **management** and the **legal** team prepares a containment strategy to control the effects of the incident and requests input from the external support agencies (if required)

2 Once containment strategy is prepared, the IRT **checks** if the incident is actually contained or not

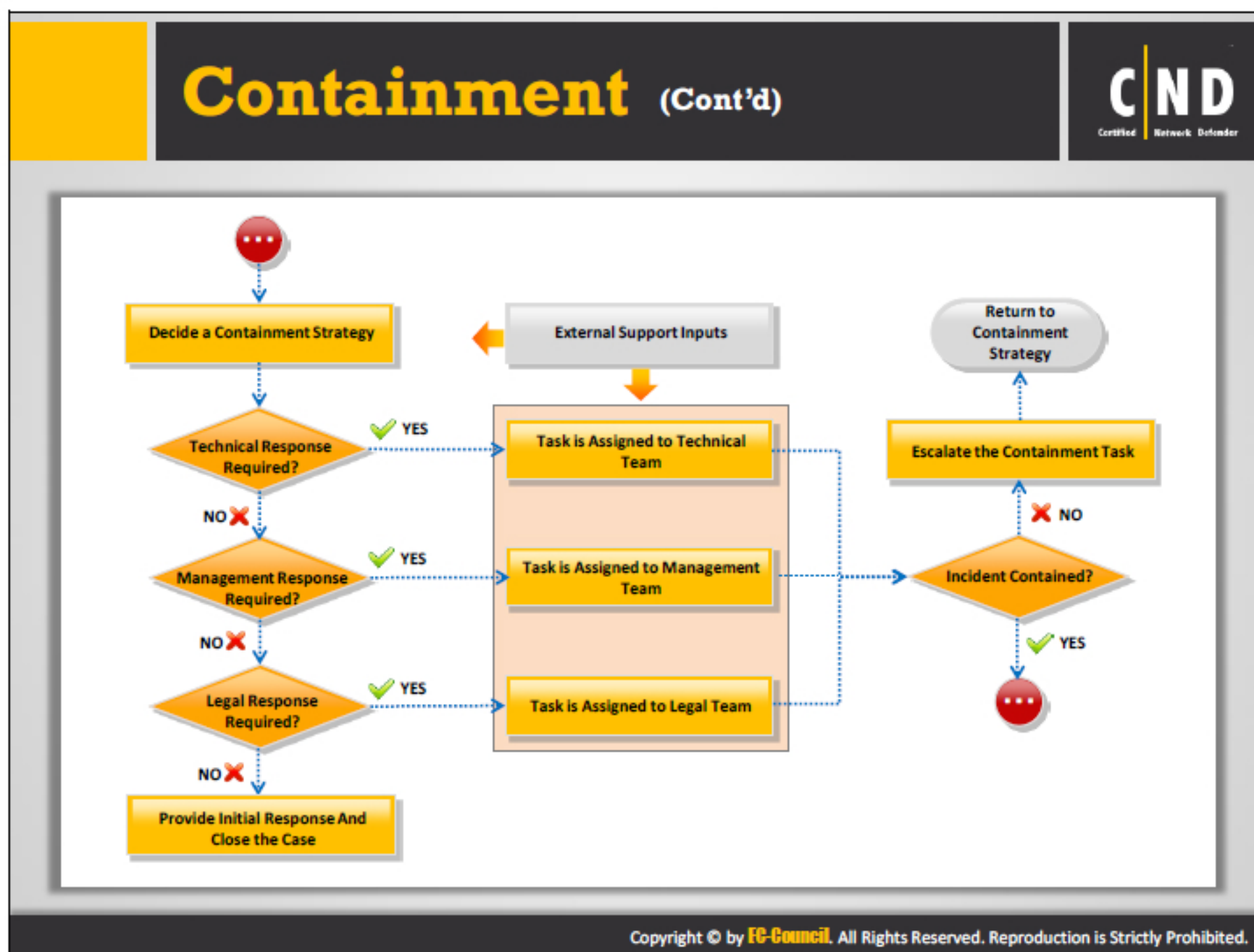
3 The IRT checks the type of **response** required to contain the incident. The containment task is then assigned to the **correct team**

4 If the incident is not contained, the IRT will **review** and **update** the containment strategy and follow the same processes again

5 If the incident is contained, the IRT will **escalate** the containment task and move to the next level of the incident handling and response process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.




The IRT plays a significant role in reducing an incident's magnitude or complexity in preventing further damage to the organization. Containment focuses on limiting the scope and extent of an incident. The aim of the containment stage is to reduce any losses and/or damages from attacks, by eliminating the threat sources. If the systems, networks, or workstations are compromised by a security incident, the IRT has to determine whether to shut down the system, disconnect the network, or continue with operations in order to monitor the system's activities. The response to all of these situations depends on the type and magnitude of the incident.

The common techniques used in the containment phase are:


- **Disabling of specific system services:**
 - Disable system services temporarily in order to reduce the impact of the incident and to continue system operations.
 - When an unknown vulnerability affects a computer, it is then removed from the network until the problem is rectified.
 - Changing the passwords and disabling the account.
 - Change passwords on all the systems which interact with the affected system, so there are no more infections.
- **Complete backups of the infected system:**
 - Back up data on the affected systems to reduce the damage during an incident response. Use a system backup for further investigation of the incident.
- **Temporary shutdown of the compromised system:**
 - If the compromised computer systems have no alternate options to handle the situation, then shut down temporarily. This shutdown limits the damage caused by the incident and gives extra time to analyze the problem.
- **System restoration:**
 - Replace the recovered computers with a trusted and clean backup copy.
 - Identify the incident sources such as vulnerabilities, threats, access paths, etc. and patch everything before restoring the system.
- **Maintaining a low profile:**
 - When detecting network-based attacks be careful to not tip off the intruder. Because the intruder might do more harm to other systems in the network and/or erase everything they can to remove the chance of being traced. Maintain standard procedures, including continuing to use the intrusion detection systems and the latest antivirus and anti-spam software.

Guidelines for Incident Containment



- ⚙️ Compromised code can undermine security, maintain a **level of caution**
- ⚙️ Data must be **forensically** backed up to a proper storage device
- ⚙️ Data should be **stored** in a safe location
- ⚙️ **System** and **router logs** must be acquired and reviewed
- ⚙️ If **operations** are continued, any and all risk must be identified
- ⚙️ **Administrators** and **system** owners must be informed and kept current on the information concerning the security incident
- ⚙️ Establish a **strong password policy** and then change all passwords following this new or updated policy
- ⚙️ **Records** should be maintained for every action taken

- ⚙️ A team must be **dedicated** to containing any type of security issue
- ⚙️ The affected area(s) must be **contained** and **secured** to avoid having things changed
- ⚙️ Information must be reviewed from the start of the **identification phase**
- ⚙️ **Honey pots** also play a vital role in enhancing security
- ⚙️ Avoid conventional methods to **trace**, this tends to alert the attackers
- ⚙️ Standard **procedures** should be followed
- ⚙️ **System alteration** has the potential to be risky unless a complete backup is first done



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The main purpose of the containment strategy is to control the effects of the attack and restore the information system to its normal state. This is vital so that business continuity of an organization is maintained. A few key considerations for an IRT in this crucial stage are:


- **Compromised code:** A compromised code can lead to a data breach increasing the chances of an intrusion. It is important for the IRT to be cautious while working with the compromised code. A minor mistake can lead to the replication of the code and can further affect the network and functioning of the organization.
- **Safe storage:** Data should be stored in a safe location so that any intrusion or external threat does not affect or alter it.
- **Acquiring logs:** The IRT team must actively acquire and retrieve all the system and router logs before, during and after the time of incident. This will help the team analyze the changes the network or system went through that caused the incident to occur.
- **Identifying risk factors:** It is important to identify the various risks if operations are continued.
- **Informing administrators and system owners:** The IRT should communicate among the administrators and system owners about the latest security threats that can affect the system. This helps to implement preventive measures, avoiding the occurrence of a major incident.


- **Strong password policy:** After the incident handling is successful, users must change their passwords. Administrators must implement a strong password policy among the organization.
- **Maintaining records:** it is important to maintain records of every action performed by the user or the system owners. Auditing and monitoring must be a key event performed by administrators on a timely basis.

Organizations face a lot of problems when incident containment guidelines are not in place. For example, an organization which is not well-prepared, gets infected and then attacked by malware, cannot handle the situation as effectively as an organization that follows incident containment guidelines. Sometimes this lack of preparedness will allow malware to spread like wildfire. In these cases, people act haphazardly to find solutions for such incidents, and nobody has any ideas on how to deal with it. This delay in finding a solution can bring an organization's network, information systems, business, and reputation to the ground. Without proper guidelines in place, network administrators implement stopgap actions trying everything they can to find the appropriate solution. This can cost the organization huge amounts of money and time. This situation can be avoided if an organization follows certain guidelines:


- **Dedicated team:** A team must be dedicated to handle any type of security issue. This team acts as a first responder during the time of an incident. Technical experts are required for this team.
- **Securing the affected area:** In order to avoid any new changes being affected, the affected area must be secured. Review the information at the beginning of the identification phase.
- **Installation of Honey pots:** Honeypots are invisible traps that play a vital role in enhancing security. Implementing honey pots in the network will help system administrators track the attacker instantly, with no data loss.
- **Avoid conventional methods:** Refrain from using conventional tracking methods when trying to identify the attacker. This will not help the investigation. It is important the team is updated on the new methods available. Attackers know the conventional tracking methods and what to look for. The last thing you want is for them to know you are looking for them.
- **Follow standard procedures:** Documented procedures are required and management, the IRT, and administrators must follow them.

Forensic Investigation







Investigation is a process of **gathering evidence** related to an incident from systems and networks




Organizations have to **discover** computer security incidents in a reasonable amount of time, in order to have enough time to decide if an investigation is required




The urgency in **making a decision** helps the investigators to determine the seriousness of the security issue and contain it




The purpose of the investigation process is to identify the incident, attacker, attack time, and mitigation steps to prevent a **future** occurrence



The forensic investigation and the containment process run at the same time



An experienced incident handler and/or computer forensic investigator **supervises** the collection of all the evidence



Data collection involves two unique **forensic challenges**: Gathering data exceeding computer storage capacity and collecting data to ensure integrity

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic Investigation

(Cont'd)





Host-based evidence: Host-based evidence consists of logs, records, documents, and any other information available on the system



Network-based evidence: Network-based evidence consists of information gathered from IDS logs, pen-register/trap and traces, router logs, firewall logs, and authentication servers



Other evidence: Other evidence that contains information and evidence gathered from the people



The incident handler creates a **chain of custody** document, which includes the detailed information about the evidence. This document includes items such as the model number, serial number, IP address, time of collection, etc. It also includes information about the people involved in the collection and evidence handling such as the name, designation, department, contact numbers, etc.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident handling helps organizations contain security events, but a computer forensic investigation lets investigators find the root cause of the security issue. Forensic investigation is the process of gathering evidence related to an incident from the systems and networks. The main goal of any of the computer security forensic investigation is to identify the incident, the time of the incident, the perpetrator of the incident, and steps to mitigate future occurrences. Forensic investigation is carried out in parallel with the containment process.

Role of Forensic Analysis in an Incident Response

Forensic analysis includes an evaluation and in-depth investigation of data related to before and after cyber-attack periods.

- Forensic analysis helps in determining the exact cause of an incident.
- It helps in generating a timeline for the incident, which will correlate different incidents.
- It helps balance operations and the security required according to the organization's budgetary constraint.
- Forensic analysis of the affected system helps determine the nature and impact of the incident.
- It helps to mitigate loss caused by a breach and to begin the recovery process.
- It helps in tracking the attackers of the crime or incident.
- It extracts, processes, and interprets factual evidence proving the attacker's actions in court.
- It saves the organization money and time by conducting a damage assessment of the victimized network.
- It also saves organizations from legal liabilities and lawsuits.

During a forensics investigation, investigators work on collecting different types of evidence, such as system based, network based, etc. It depends on what type of security incidents the investigator is dealing with.

Host-based evidence

Host-based evidence is the evidence gathered from the compromised system. It may include collecting volatile or non-volatile information such as:

- Logs, records, documents, and any other information stored in a computer system.
- The date and time of the system.
- The present applications executing on the system.
- The present network connections identified.
- Open sockets or ports currently available.
- Applications listening on open ports.
- The state of the network interface.

Network-based evidence

Network-based evidence is the information gathered from the network resources, such as:

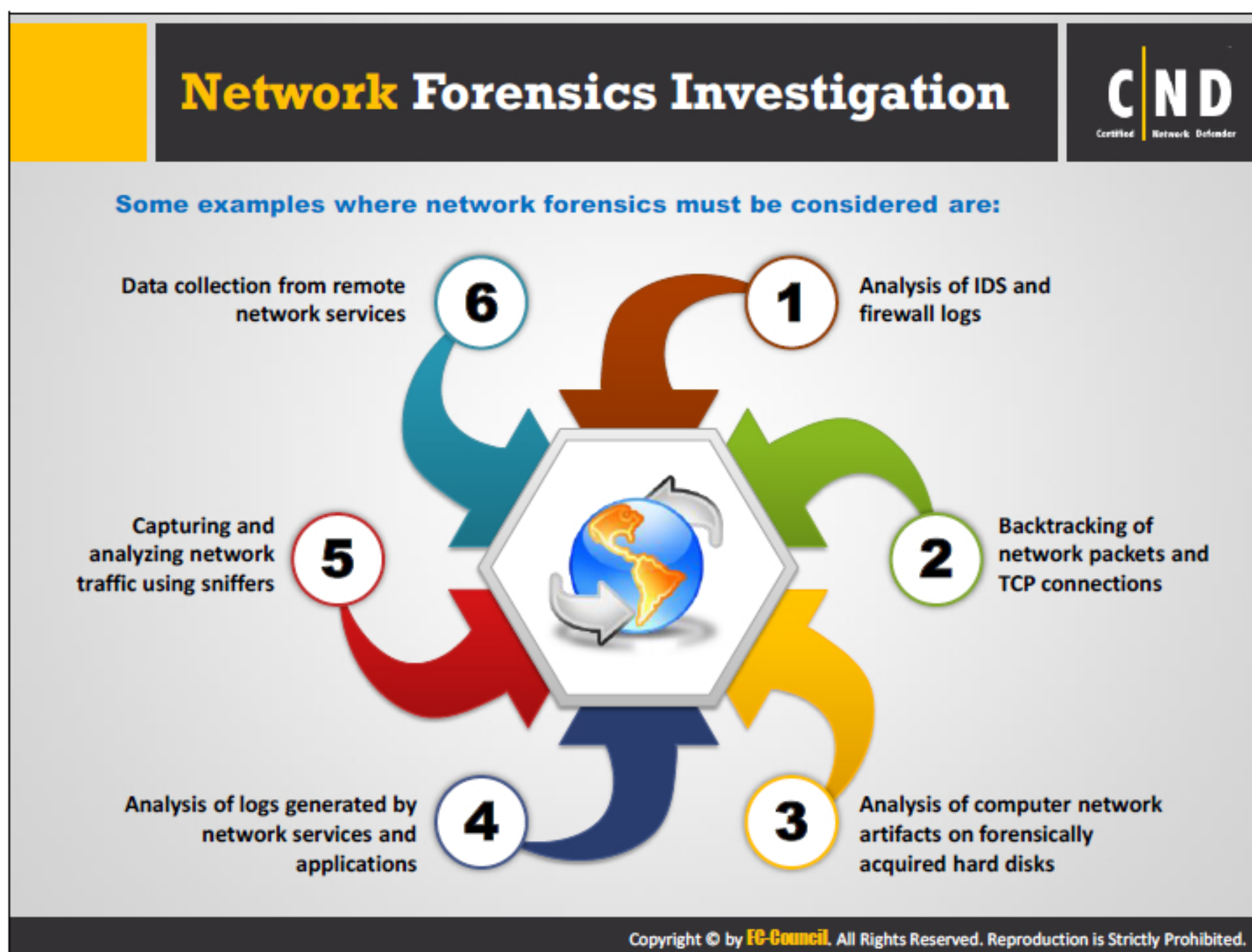
- **IDS logs:** Intrusion Detection System (IDS) logs helps in identifying the unusual level of attacks, concerted attack, unusual protocol and port combination.
- **Router logs:** Router logs helps in identifying the number of systems connected to the specific router.
- **Firewall logs:** Firewall logs displays the active and inactive sessions of a host machine.
- **Monitoring logs:** It collects the information of the systems in a network. Any suspected activity of a host machine can be analyzed through monitoring logs.
- **Wiretaps:** Wiretap gathers metadata of the device where the monitoring device is being placed.
- **Pen-register/trap and traces:** The logs of pen-register records routing information of the devices.
- **Authentication servers:** Logs generated in authentication servers helps the administrators to identify any unknown entity trying to access the network.

Other Evidence

Other evidence may consist of:

- Gathering and validating personal files, documents related with incident.
- Interviewing employees, witnesses, and character witnesses.
- Documenting the information gathered.

The incident handler creates a chain of custody document which includes detailed information about evidence such as the model number, serial number, IP address, time of collection, etc., and information about all the people involved in collection or evidence handling such as the name, designation, and contact numbers, etc.



Network forensics is a method of sniffing, recording, acquiring, and analysis of network traffic and event logs in order to investigate a network security incident. Usually, network forensics involves a pro-active investigation as it deals with network traffic that contains dynamic information.

Network forensics aims to enhance security and provide evidence for legal issues. Information is collected from the network traffic (such as packet sniffing) and remote network services (such as ftp servers, websites etc.) acting as a source for network forensic evidence.

Network forensics can reveal:

- Source of security incidents and network attacks
- IP addresses, protocols, encrypted or unencrypted messages etc.
- Path of the attack
- Intrusion techniques used by attackers

Network forensics has certain limitations due to privacy laws and other types of legal restrictions.



Based on the requirement of the organization, the primary users of forensic tools and techniques fall under three groups:

- **Investigators**: Responsible for investigating incidents.
- **IT Professionals**: Includes technical staff and administrators.
- **Incident handlers**: Responds to different computer security incidents.

A detailed discussion of the people involved in a computer forensics team is as follows:

- **Attorney**: Helps in giving legal advice about how the investigation should be carried out, and the legal issues that should be followed in the computer forensics investigation process.
- **Photographer**: Photographs the crime scene and the evidence gathered. They must be certified for evidence photography. By photographing all the evidence found at the crime scene, will record the key evidence in the forensics process.
- **Incident Responder**: Responsible for the measures taken when an incident occurs. The incident responder is responsible for securing the incident area and collecting the evidence that is present at the crime scene.
- **Decision Maker**: Authority responsible for the policy or procedure taken during the investigation process. Based on the incident type, a decision maker decides the policies and procedures and adapts them while handling the incident.

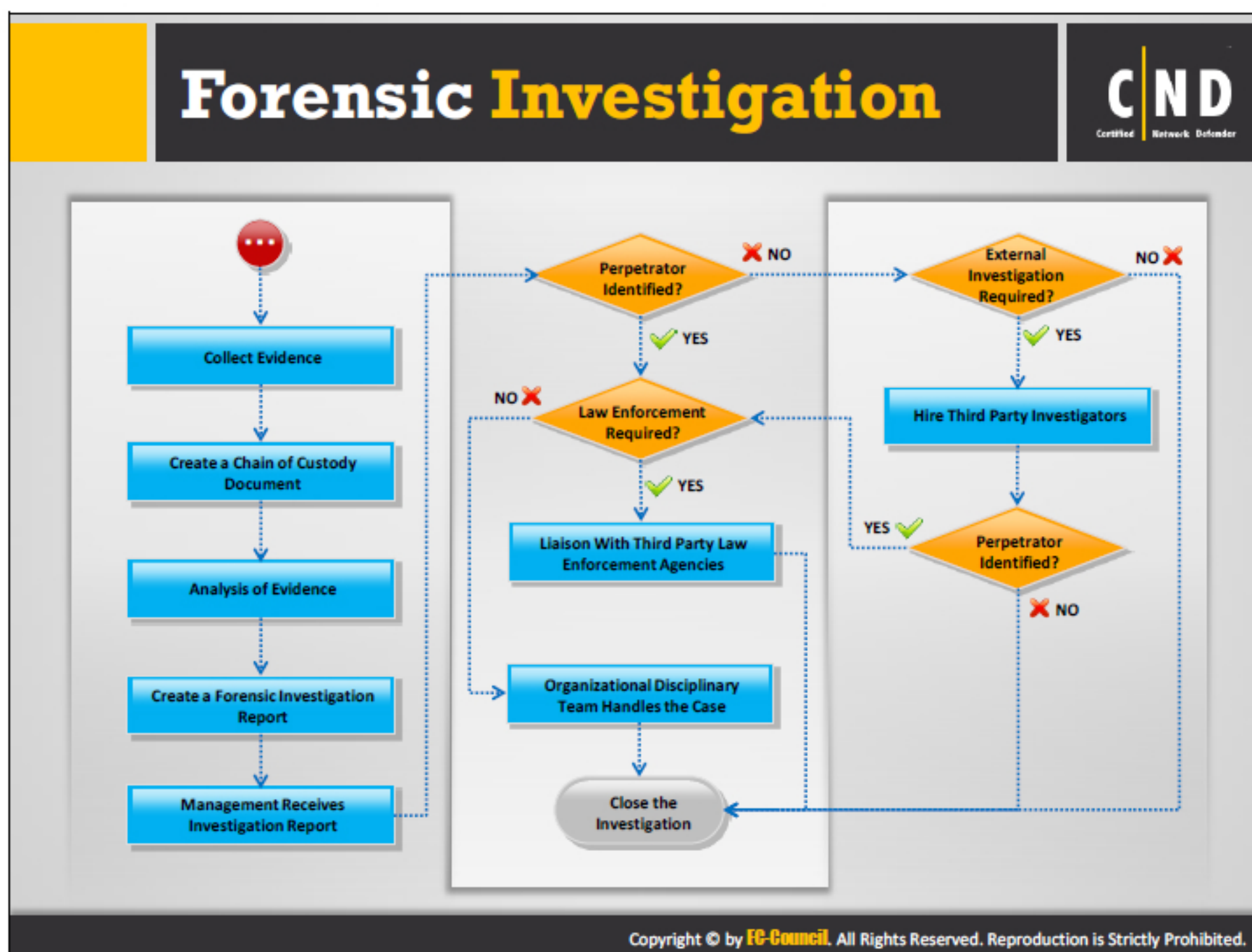
- **Incident Analyzer:** Analyzes the incidents based on their occurrence. They examine the incident with regard to its type, how it affects the system, different threats, and vulnerabilities associated with it, etc.
- **Evidence Examiner/Investigator:** Examines the evidence acquired and sorts which is useful. Examine and sort the evidence according to its relevancy to the case. By maintaining an evidence hierarchy, the evidence examiner will prioritize the evidence properly.
- **Evidence Documenter:** Documents all the evidence and the phases present in the investigation process. The evidence documenter gathers information from all the people involved in the forensics process and documents it in an orderly fashion, from the incident occurrence to the end of the investigation. The documents contain the complete information about the forensics process.
- **Evidence Manager:** Manages the evidence so it is admissible in a court of law. They have all the information about the evidence, for example, evidence name, evidence type, time, and source of evidence, etc. They manage and maintain a record of the evidence that it is admissible in a court of law.
- **Expert Witness:** Offers a formal opinion as testimony in a court of law. Expert witnesses authenticate the facts and witnesses during a complex case. Expert witnesses are often called to cross-examine other witnesses and evidence, as a normal witness may be influenced by various factors.



The forensic investigation methodology includes a series of steps that are followed to carry out a successful forensic investigation. It guides the investigator in the collection of potential evidence concerning the security incident and makes sure it is admissible in a court of law. A typical forensics investigation methodology includes the following steps:

1. **Obtain a search warrant:** Investigators obtain a search warrant before investigating any suspects. The warrant proves beneficial for the investigator.
2. **Evaluate and secure the scene:** Investigators evaluate and secure the scene before collecting the evidence. Tampering or damaging the devices can affect the evidential proof against the suspect.
3. **Collect the evidence:** Investigators collect all the evidence discovered from the scene. The investigators must not neglect any of the supporting items related to the incident which can act as evidence and be helpful in a court of law.
4. **Secure the evidence:** The investigator securely stores the evidence collected. Loss of evidence will weaken the case against the suspect.
5. **Acquire the data:** It is important to acquire the affected data. This will help the investigator find the reason for the intrusion.
6. **Analyze the data:** Analyzing the data also includes monitoring the target's activity before, during and after the incident. The Analysis phase is the most important phase, as the investigator gathers more evidence through the monitoring of logs.

7. **Assess Evidence and Case:** Once the investigator has done the analysis, it is important to gather the evidence and assess.
8. **Prepare the final report:** The final report will include detailed information about the actions taken by the investigator and the suspect/attacker.
9. **Testify as an expert witness:** The investigator will testify as an expert witness confirming the facts of the case.

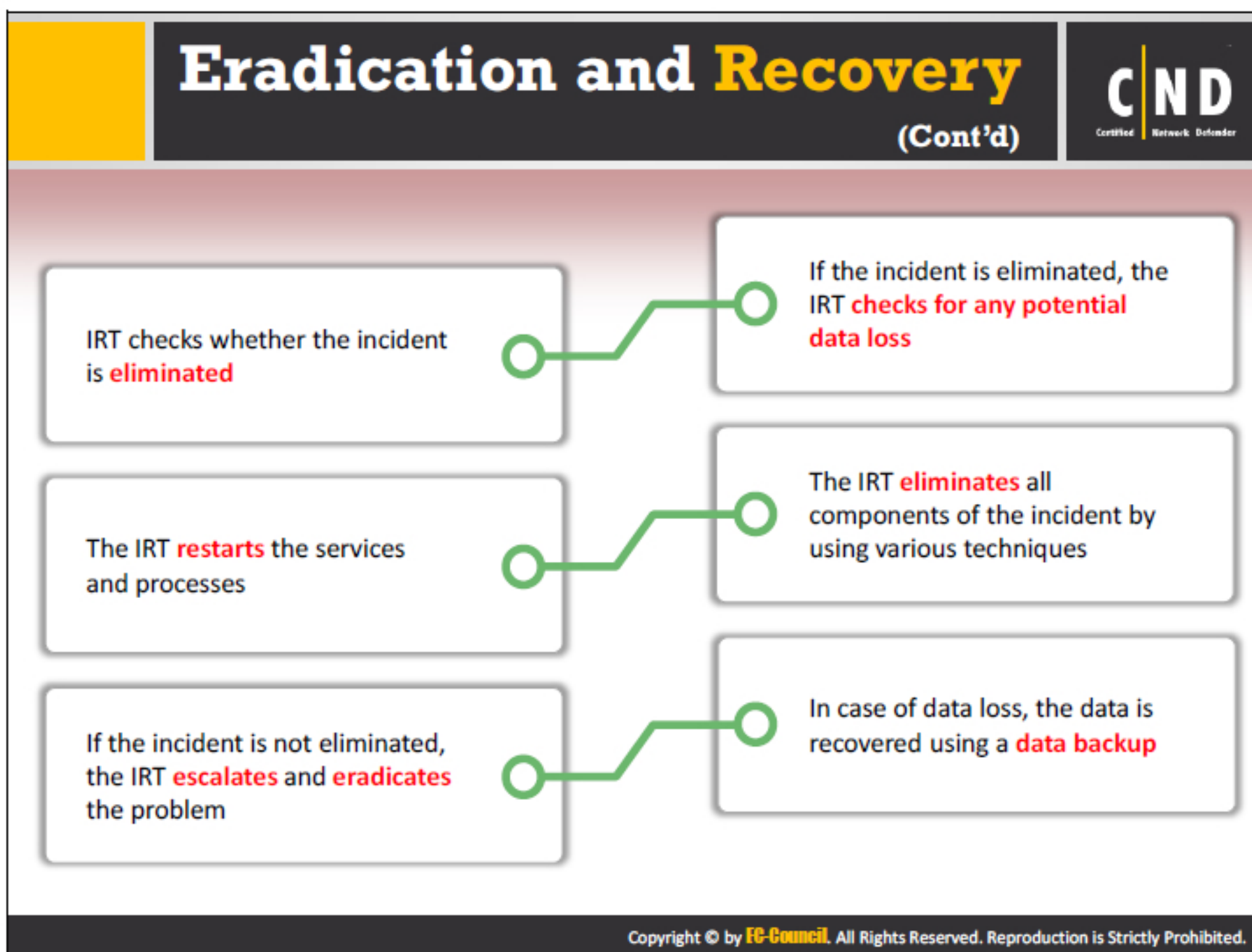
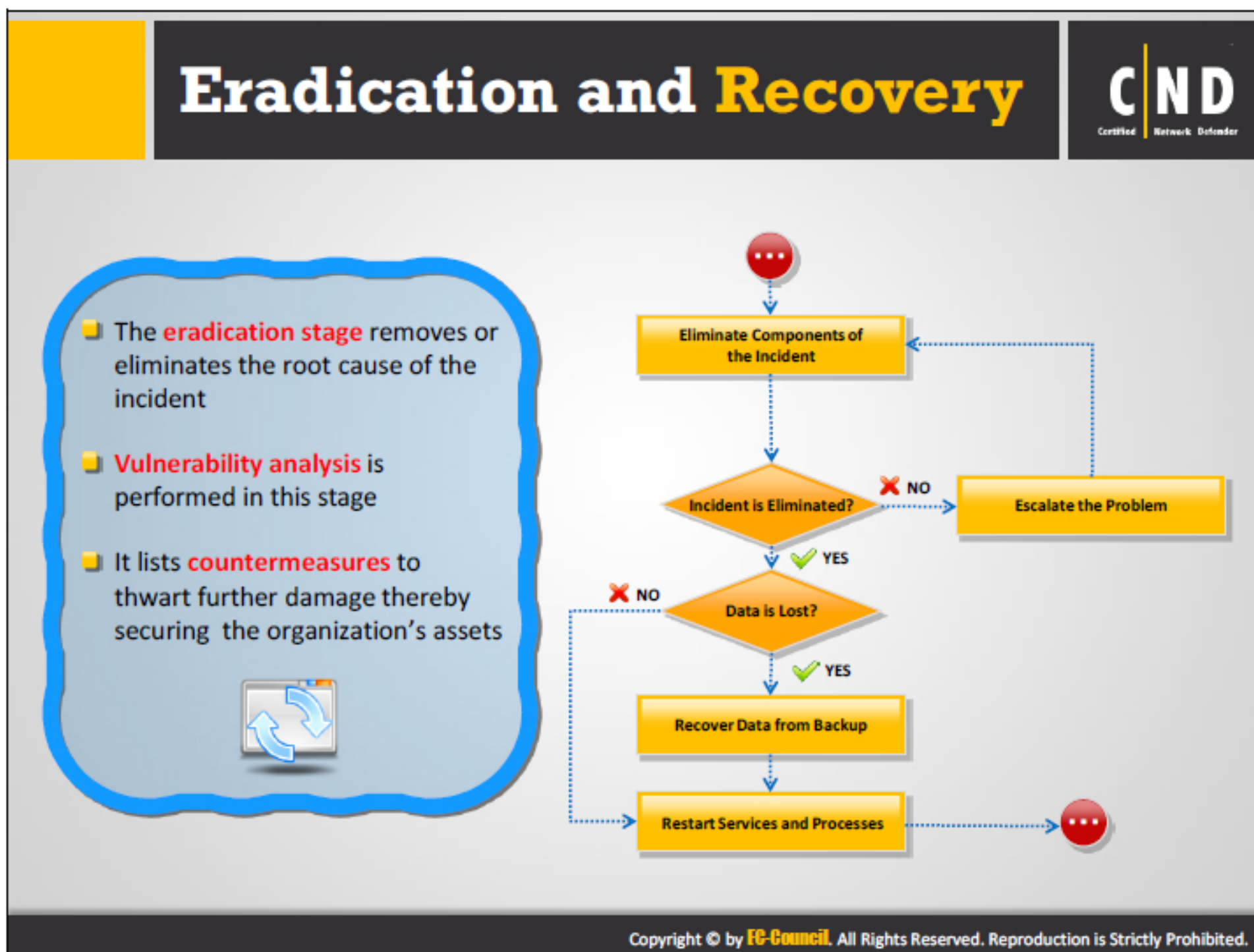


A forensic investigation involves using various processes, tools and techniques to gather valuable information. The forensics investigation team analyzes the evidence to identify the real cause and nature of the incident and trace the perpetrators after the collection and protection of the evidence. The team documents and submits the results of the forensic analysis to management.

If the perpetrator is identified in an investigation report, management then decides whether law enforcement is required to prosecute the perpetrator, or the organizational disciplinary team should handle the case. If there is the need for law enforcement, then management or a designated authority contacts a third party law enforcement agency. If the attacker is not identified, then management decides whether to close the investigation or to pass it to an external investigation agency for further investigation. If the third party investigators are able to investigate the incident and identify the attacker, it will be reported to management.


Management makes further decisions regarding the prosecution of attacker. If the third party investigators also fail to identify the perpetrator, the IRT or management will recommend an update in the IH&R processes that enable them to carry out successful investigations in the future.

Organizations need to notify external law enforcement and investigation agencies if the incident is severe and affects the employees, customers, and the general public. If the incident has caused severe damages and financial losses, the organization should report the incident to law enforcement agencies and file a case against the attackers. These agencies can be local or national law enforcement agencies, security agencies, cyber experts, etc.



Eradication and Recovery

(Cont'd)



The possible countermeasures include:

1 Using antivirus software	6 Updating security policies and procedures
2 Installing the latest patches	7 Changing the passwords of the compromised systems
3 Policy compliance checks	8 Eliminating the intruder's access and identifying any changes
4 Independent security audits	9 Reinstalling compromised systems
5 Disabling unnecessary services	10 Rebuilding systems

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The eradication and recovery from a security incident generally depends on its extent. Sometimes it is easy to contain and recover from a malware attack but in some cases, it is quite difficult and takes more time to recover if it has infected more systems in the network. In this case, the organization needs to further harden, monitor, and validate all computer and information systems against all future threats. The extent of damage to the network may be unknown in this case. Therefore, there is no other alternative than building the whole network again from scratch. This is something an organization will want to avoid at all costs. Eradication and recovery is vital to the success of an organization.

Eradication and recovery also depends on how effectively the attack is contained during the containment phase. This phase is capable of:

- Handling the problem
- Solving the problem
- Taking the necessary steps to prevent the problem from occurring again

Recovery also determines the course of action for an incident.

Determining the cause and symptoms

The data and information regarding the type of incident which is gathered during the containment phase, is useful in the eradication phase. This information will help determine the cause and symptoms of the incident and help in determining a suitable recovery method.

Improve defenses

Various kinds of protection tools and techniques such as firewalls, routers, and router filters should be used to strengthen the security of the organization. It is also important to configure network security devices and applications to block identified attack paths. Patch all the identified vulnerabilities to stop further exploitation.

In extreme cases, change network component addresses for devices which face the public. This will help ensure any established attack paths are removed.

Vulnerability analysis


Vulnerability analysis is necessary as it provides important information about the vulnerable points and areas present in the system. It reduces the damage caused by the incident and safeguards the organization, as it carries out its normal operations.

The following countermeasures prevent organizations from further security threats. The IRT should implement these countermeasures in their eradication and recovery phase.

- **Organization's priorities:** Identifying the organization's top priorities, such as restoring the system to normal operations, ensuring data integrity, determining the impact of evidence, gathering evidence, and/or avoiding public disclosure.
- **Examining the incident:** Examining the nature, severity and cause of the incident.
- **Antivirus software:** Usage of antivirus software on the system prevents intrusion to the system, which in turn prevents data loss.
- **Installing the latest patches:** Installation of the latest patches hardens system security. However, before installing patches on host machines, administrators should check the patches using a test machine.
- **Security audits:** Timely independent security audits conducted to detect all suspected activities.
- **Disabling any unnecessary services:** Administrators should disable services users do not use. Intrusion can be done through non-working services on a host machine.
- **Updating security policies and procedures:** Administrators should regularly update Security policies and procedures.
- **Changing passwords:** It is important for users to change the passwords on their systems. The passwords must follow a strong password policy deployed by the administrators.
- **Eliminating the intruder's access paths:** After the removal of the external threats, it is also necessary to eliminate the intruder's access path by changing the information system.
- **Reinstallation:** A system that was infected by an intrusion should undergo a fresh installation of the operating system and all the services.
- **Restoring:** Compromised or infected systems should be restored with an installation of secure software.

- **Corrective actions:** Corrective actions reduce vulnerabilities in the system, making them less vulnerable to intrusion.
- **Network-based countermeasures:** Network based countermeasures secure network devices in the network.

Eradiation and Recovery - Systems Recovery



- Recovering a system from an incident generally depends on the extent of **the security breach**
- In the recovery step, an affected system is restored to **normal operation**
- The computer systems and networks are **monitored and validated**
- The recovery stage determines the **course of action** for an incident
- Run a vulnerability assessment and penetration testing tools to identify possibly **vulnerabilities** which exist in the system and/or network
- Determine the **integrity** of the backup file by attempting to read its data

- Verify the successful operation of the system
- Use network loggers, system log files and potential back doors to **monitor** the system
- Actions performed in the recovery stage are:
 - Rebuilding** the system by installing a new OS
 - Restoring** user data from trusted backups
 - Examine the protection and detection methods
 - Examine the **security patches** and system log information

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Recovering a system generally depends on the extent of the security breach. In the recovery step, restoration begins for the affected systems in normal operation. When a computer security incident occurs, the IRTs should decide whether to restore the existing system or completely rebuild the system. Utilizing system backups to rebuild the compromised system.

The systems recovery steps are:

- **Determine the course of action:**

Strategies for system recovery are determined according to the impact of the incident. Select the appropriate strategy after considering the availability of resources, the criticality of affected systems, and the results of a cost-benefit analysis.

- **Monitor and validate the systems:**

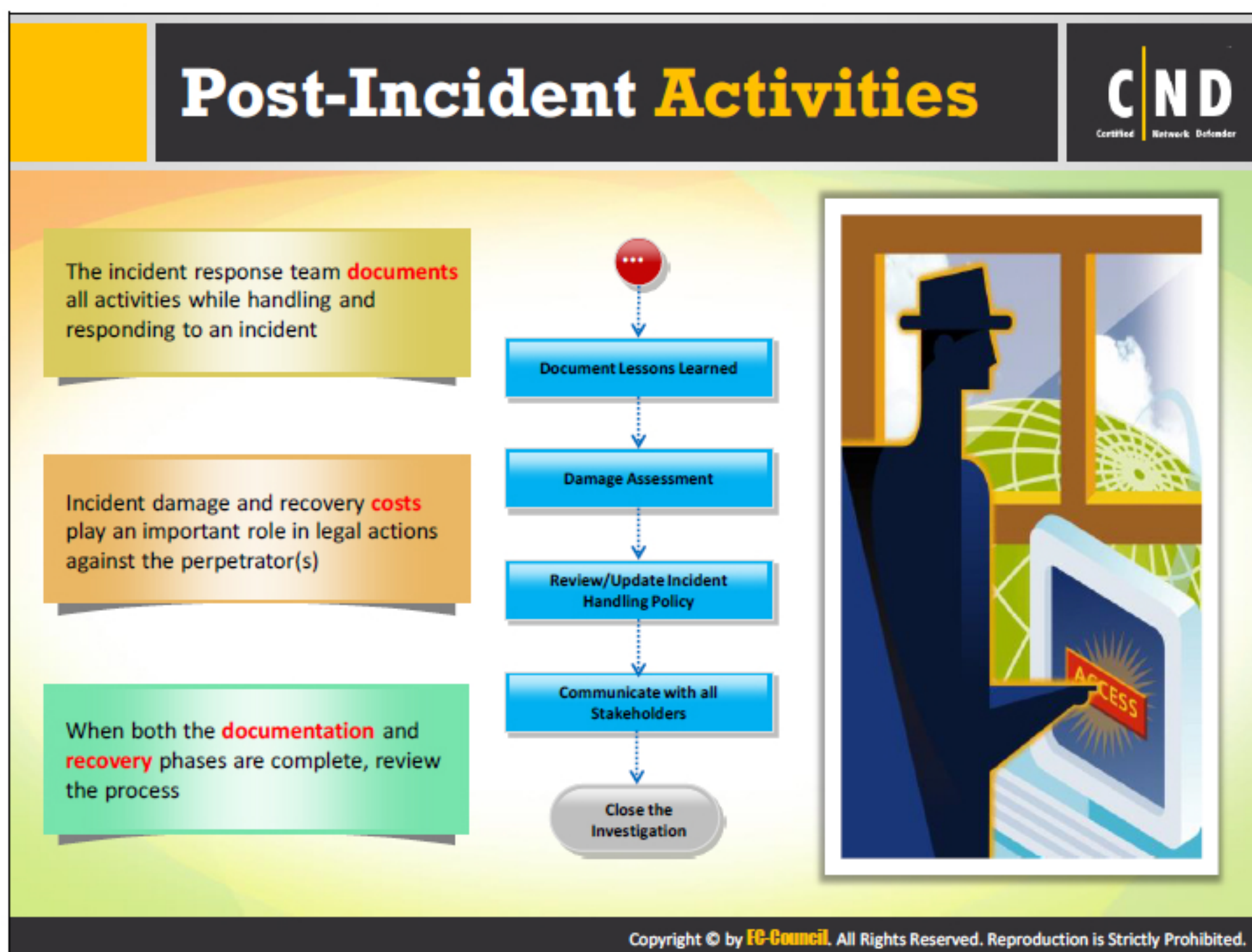
Monitoring and system validation ensures that the recovered systems are sanitized of any incident causes and are operating in normal conditions. Validation also involves checking the integrity of the restored information from a backup. Conduct regular vulnerability assessments and penetration testing to monitor the system's behavior and the possible vulnerabilities which may exist in the system or network. Monitor the system for potential back doors, which can result in the loss of data or another incident.

A restoration process is only successful when the backup files are properly stored and preserved. The amount of data recovery, safety and preservation mainly depend on the techniques used in the recovery process. During this process, the integrity of the data can be

damaged, which can be determined using a backup file integrity check. This operation verifies the success of the operation and the normal condition of the system. Harden the network monitoring using network loggers, system log files, and potential back doors to check for any missed vulnerabilities.


Some of the actions to perform in the recovery stage are:

- Rebuilding the system by installing a new OS.
- Restoring a user's data from trusted backups.
- Examine protection and detection methods.
- Examine security patches and system log information.



It is a good habit to learn from past mistakes. The IRT as well as the organization can learn a lot from its past security mistakes and vulnerabilities. Incident handling involves more than effectively handling an incident, it also involves the process of learning and improving. Organizations who conduct a meeting with their staff after an incident, know the lessons learned have found them to be beneficial. This learning process also involves the policies which were responsible for the security failure. An update or review of all the security policies will help the organization build a robust network that is highly difficult to penetrate.

Post-Incident Activities - Incident Documentation



- The incident response team will **document** all the various processes while handling and responding to an incident
- The documentation must provide the description of the **security breach** and details of all actions which took place such as: who handled the incident, when the incident handling took place and all the reasons why the incident occurred
- Document all the **steps** and **conclusion statements**, immediately after completing the forensic process
- The document must be organized properly, examined, reviewed and vetted by the management and legal counsel
- The best way to prosecute the offender(s) is through proper documentation

The prepared document should be:

Concise and Clear
Prepare the reports in such a way that it is **clearly understood** by everyone

Standard Format
Maintain a standard format making the report writing **scalable**, which saves time and enhances accuracy

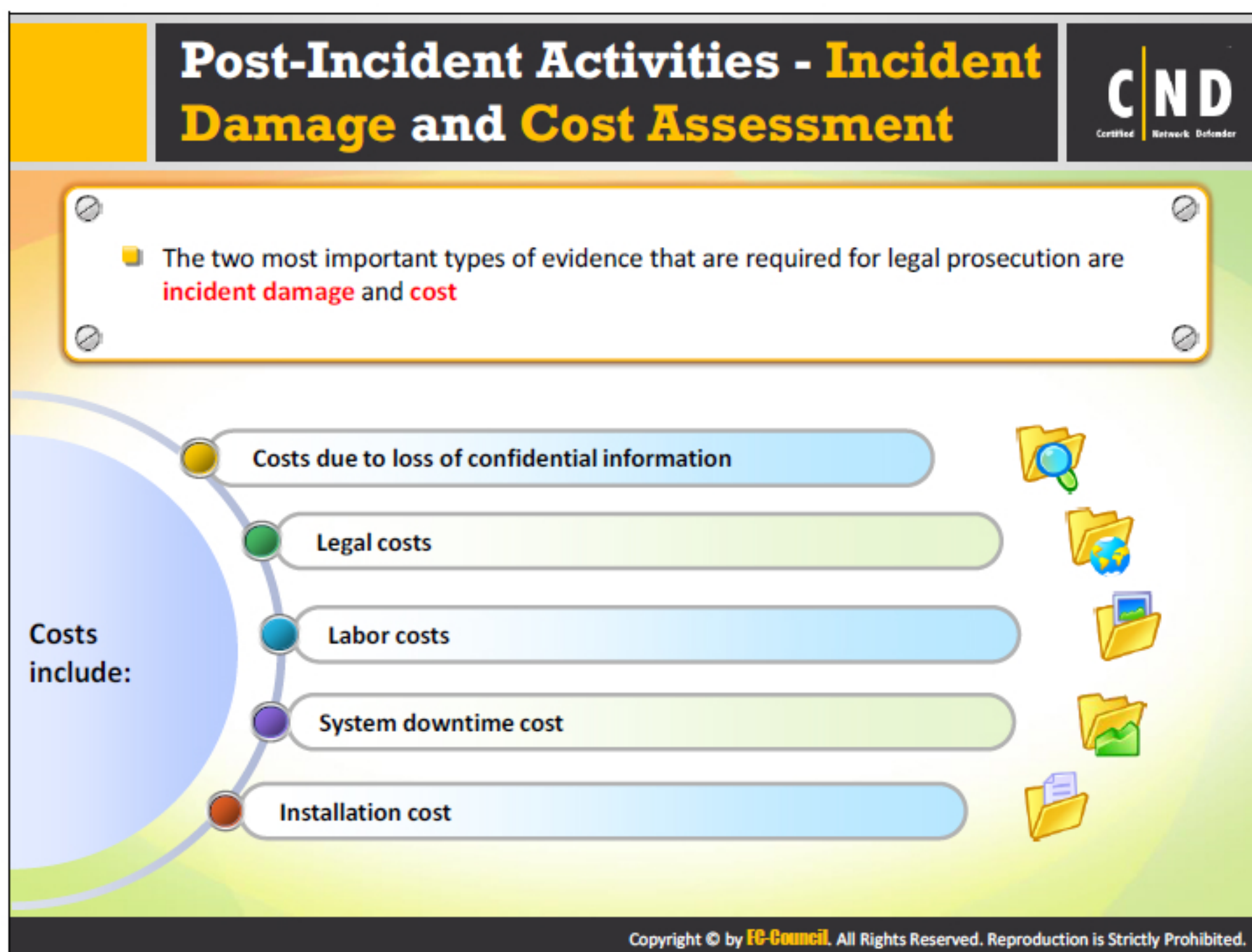
Editors
Ensure that the forensic reports are **edited properly**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The evidence gathered as well as the documents prepared should be safeguarded during the protect evidence phase.

Document the steps and conclusions during the investigation process as soon as possible. The document prepared should be:

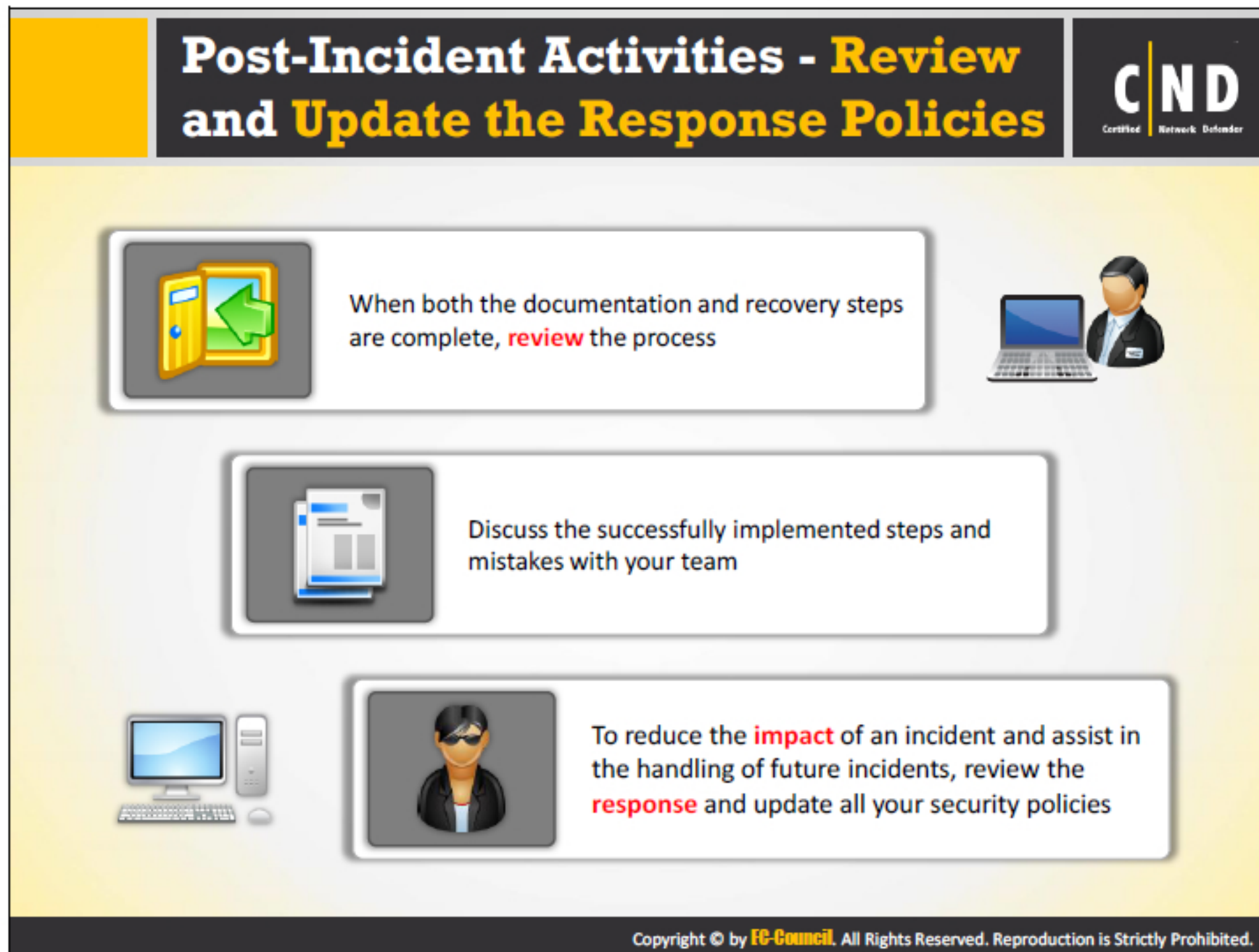
- **Concise and clear:**
Prepare the reports so that everyone can understand them. Avoid using shortcuts while preparing the reports.
- **Standard format:**
Maintain a standard format that makes report writing scalable, saves time, and supports accuracy. Organize the response process by generating forms, outlines, and templates and support the storage of the data related to the incident.
- **Error-free:**
Accept the help of technical editors to read the forensic reports. Editors provide their support in developing error-free reports.



Incidents cause extensive damage in organizations, resulting in huge losses that range from the loss of business to the loss of a customer's goodwill. Sometimes, reports of incidents result in losing prospective customers. Most importantly, lost confidential information can cost an organization millions of dollars, because customers file lawsuits over the organization's negligence handling the personal information of customers. An organization can estimate their internal losses, which provide an idea on the actual asset losses. The estimation of losses is the sum of all the damage costs as well as the cost to recover from the incident. Incident damage and recovery costs play an important role in legal actions against perpetrators.

Incident damage includes:

- The loss of confidential information.
- Legal costs for investigating the case, lawyer's fees, etc.
- Costs pertaining to analyzing the incident, recovering, and installing software and hardware.
- Loss and costs due to system downtime.
- Implementing costs.
- Repairing and replacing damaged systems and physical security costs.
- Costs due to damage of the organization's reputation, and the loss of customer trust.



The steps that prevent future incidents are as follows:

- Consider additional security policies that prevent incidents.
- Update the policies and procedures regularly.
- Examine the appropriateness of the incident response.
- Examine whether the organization's computer systems are:
 - Regularly patched
 - Properly locked down
 - Protected with encrypted passwords
 - Updated with the latest antivirus software
 - Set with email policies

Use the lessons learned from the incident for future incident response efforts.

Training and Awareness



- Training and awareness provides **skills** required to implement incident handling policies
- Practical training** removes developmental errors, improves procedures, and reduces the occurrence of miscommunication
- Well-trained members** can prevent an incident or limit the resulting damage


Security awareness and training should include:

- 1 Design and plan the **awareness** and **training program**
- 2 Development of the awareness and **training materials**
- 3 Implementation of the awareness and **training programs**
- 4 Measuring the effectiveness of the program and updating it


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Training and Awareness


(Cont'd)



- Training should be conducted at specified intervals and include:
 - The incident handling location
 - Pre-assignment plans to handle emergency situations for all employees
 - Recognition and operation of **utility shut-off** devices



- The awareness campaign is designed for several purposes, such as:
 - Knowledge and participation
 - A **plan's strategies**
 - Contingency arrangements



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Training and awareness not only enhances employee's security knowledge, but also helps change the lackadaisical attitude towards security in organizations overall. The human factor in security affects much more than any software or hardware enhancement ever could. Training provides a great deal of understanding of the policies implemented in the organization, which also increases the security. A security awareness program is a two-way information flow where the use of various types of communication media take place such as audio, video, text, and practical training sessions.

The important elements in security training and awareness programs are:

- Plan and design the training and awareness program.
- Update and analyze the efficiency of the training program.
- Implement the training and awareness program.
- Build training and awareness study material.

A comprehensive training program for all employees is necessary after updating the plan. The purpose of conducting training and exercises is to ensure that first responders have a necessary level of preparedness and updated training material that involves quality control steps.

Conduct training at specified intervals including:

- Identifying the incident handling location.
- Identifying pre-assignment plans to handle emergency situations by all employees.
- Recognizing and operating the utility shut-off devices.

Conduct internal and external awareness campaigns to:

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

To generate awareness among employees:


- Training is necessary to create awareness and preparedness among the staff and team members.

A training and awareness program educates people on how to handle computer-related incidents. It provides skills required to implement incident handling policies. Give training to all teams regarding their roles, responsibilities, and specific tasks. There is a need for specific skills during the recovery process. Training and awareness are necessary for general incident handling operations, the level of importance, incident handling know-how etc.


Practical training removes developmental errors, improves procedures, and reduces miscommunication. Well-trained members can significantly limit the damage. A training program's effectiveness increases only when there is a proper planning, implementation strategy, maintenance, and periodic evaluations of the program.

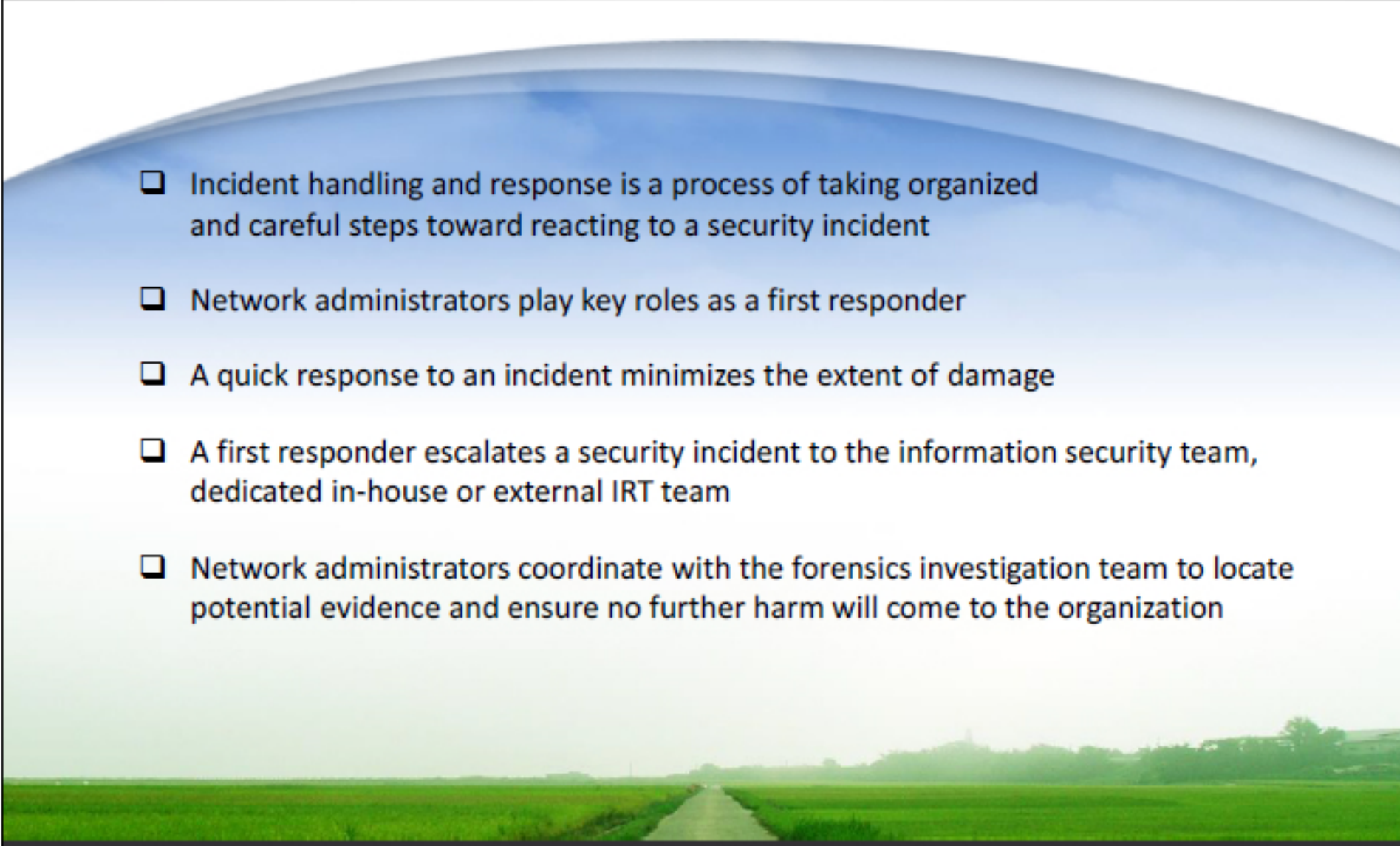
Some of the important points that constitute a training and awareness program's success are:

- Identify the scope, goal, and objective of the program.
- Identify the training staff.
- Identify the people to be trained.
- Inspire employees and management to adhere to security awareness.
- Effectively manage the program.
- Program maintenance.
- Continuous evaluation and enhancement of the program.



Module Summary





- ☐ Incident handling and response is a process of taking organized and careful steps toward reacting to a security incident
- ☐ Network administrators play key roles as a first responder
- ☐ A quick response to an incident minimizes the extent of damage
- ☐ A first responder escalates a security incident to the information security team, dedicated in-house or external IRT team
- ☐ Network administrators coordinate with the forensics investigation team to locate potential evidence and ensure no further harm will come to the organization

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

In this module, you learned how important it is to provide timely responses to incidents. The timely response prevents major losses to the organization. Network administrators play vital roles in providing a timely response for incidents as a first responder. The IRT team's investigation works with the initial information provided by the first responder concerning the incident. The module also provided an overview of the entire process for incident handling and response which the IRT follows and implements, for successful handling, eradication, containment, investigation, and recovery from all types of security incidents.