Module VI : Incident Response –Roles, and Responsibilities

Prepared by

Dr. P. Vijayakumar

Associate Professor / SENSE

Vellore Institute of Technology, Chennai

Content

- Incident Response
- Handling Different Types of Information Security Incidents
- Preparation for Incident Response and Handling.
- Incident Response Team
- Incident Response Team Dependencies
- Incident Response Process

Incident Response - Overview

- An incident is a set of one or more security events or conditions that requires action and closure in order to maintain an acceptable risk profile.

Incidents

- Besides attacks, known system vulnerabilities or discovered policy violations are also incidents that require a response in order to protect the business.
- When related events (e.g. attacks, vulnerabilities, and policy violations) are viewed together, the true nature (or type) of the incident becomes evident.

Introduction to Incident Handling and Response

- Computer or information security incident response has become an important **component of information technology** (IT) security programs.

- An incident response capability is therefore necessary for rapidly **detecting incidents**, **minimizing loss** and **destruction**, **mitigating the weaknesses** that were exploited and restoring IT services.

Different types of information security incidents are caused due to:

- Peripheral devices such as external/ removable media
- Attrition (brute force methods that compromise, degrade, or destroy systems, networks or services)
- Website or web based application
- Email message or attachment
- Improper usage of an organization’s acceptable usage policies by an authorized user
- Loss or theft of equipment
- Other factors

Incidents can be classified into:

- Malicious code
- Network reconnaissance
- Unauthorized access
- Inappropriate usage
- Multiple component

Impact of information security incidents:

- **Functional impact** (current and likely future negative impact to business functions)
- **Information impact** (effect on the confidentiality, integrity, and availability of the organization’s information)
- **Recoverability from the incident** (time and types of resources that must be spent on recovering from the incident)

Need for incident response

- to respond quickly and effectively when security breaches occur.

- to be able to use information gained during incident handling to better prepare for handling future incidents.

- to provide stronger protection for systems and data.

- to help deal properly with legal issues that may arise during incidents.

- to comply with law, regulations, and policy directing a coordinated, effective defense against information.

Goals of incident response

- formal, focused, and coordinated approach to responding to incidents.

- adhere to organization’s mission, size, structure, and functions.
- formulate policy, plan, and procedure creation to counter adverse events.

- to provide stronger protection for systems and data.

- to minimize loss or theft of information and disruption of services.

- to respond quickly and effectively when security breaches occur.

How to identify an incident

- incident analysis hardware and software to identify an incident.

- appropriate incident handling communication means and facilities.

- incident analysis resources to identify an incident.

- incident mitigation software to identify an incident.

- different response strategies to identify incidents through attack vectors, such as external/ removable media, attrition, web, email, impersonation, improper usage by organization’s authorized users, loss or theft of equipment and others that are beyond the scope of the above mentioned.

Signs of security incident

- **Precursors:** a sign that an incident may occur in the future.
- **Indicator:** a sign that an incident may have occurred or may be occurring now.

Some of the common signs of security incident are:

- web server log entries that show the usage of a vulnerability scanner.

- announcement of a new exploit that targets a vulnerability of the organization’s mail server.

- threat from a group stating that it will attack the organization.

- network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.

- antivirus software alerts when it detects that a host is infected with malware.

Some of the common signs of security incident are:

- system administrator sees a file name with unusual characters.

- host records an auditing configuration change in its log.

- application logs multiple failed login attempts from an unfamiliar remote system.

- email administrator sees a large number of bounced emails with suspicious content.

- network administrator notices an unusual deviation from typical network traffic flows.

Incident Information

- **Alerts:** reviewing alerts based on supporting data from sources such as Intrusion Detection and Prevention Systems (IDPS); Security Information and Event Management (SIEM) alerts;

- Antivirus and anti-spam software; file integrity checking software; third-party monitoring services etc.

- **Logs:** analyzing logs from sources such as operating system, service and application logs and network device logs in correlation with event information.

- **Network flow:** using routers and other networking devices to provide information and locate anomalous network activity caused by malware, data exfiltration and other malicious acts.

Incident Information

- **Publicly Available Information:** updating and integrating new vulnerabilities and exploits published by authorized agencies such as National Vulnerability Database (NVD).

- **People**: validating reports registered by users, system administrators, network administrators, security staff, other people within the organization and reports originating from external sources or parties.

Handling Different Types of Information Security Incidents

Handling incidents

There are five important incident handling phases:

- **Preparation**: establishing and training an incident response team, and acquiring the necessary tools and resources.
- **Detection and analysis**: detecting security breaches and alerting organization during any imminent attack.
- **Containment:** mitigating the impact of the incident by containment.
- **Eradication and recovery:** carrying out detection and analysis cycle to eradicate incident and ultimately initiate recovery.
- **Post-incident activity:** preparing detailed report of the cause and cost of the incident and future preventive measures against similar attacks.

This is similar to the tasks contained within incident management plans:

- identify
- contain
- cleanse
- recover
- close

Incident Response Plan

- Incident Response Plan is an organization’s foundation to a formal, focused and coordinated approach for incident response.

Purpose of incident response plan

- The objective of instating an incident response plan is to provide the roadmap for implementing the incidence response capability.

- The incident response plan acts as a defense mechanism against hackers, malware, human error and a series of other security threats.

Requirements of incident response plan

- The intervention of an incident response plan can be the structure to building an organization’s incident response capability.

- Emphasis on computing security policies and practices are the main objectives of most organization in their overall risk management strategies.

Elements that are recommended as important to an incident response plan are:

- organization’s mission towards the plan
- organization’s strategies and goals to determine the structure of incident response capability
- senior management approval in the structuring of the proposed plan
- organizational approach to incident response
- incident response team’s communication with the rest of the organization and with other organizations
- metrics for measuring the incident response capability and its effectiveness
- roadmap for maturing the incident response capability (regular reviews, audits and tests etc.)
- how the program fits into the overall organization

Incident response plan checklist

- Developing an incident response plan checklist can minimize the threat of security breach in the form of attacks in websites and servers, or inadvertent leakage of share sensitive data etc.

- Instating a structure that ensures the latest developments are captured, understood, evaluated as threats to the business, documented and distributed will help ensure an effective incident response.

An incident response plan checklist should be an amalgamation of the following key practices:

- provides a roadmap for implementing an incident response program based on the organization's policy.

- organize both short and long-term goals program, including metrics for measuring the program.

- highlight incident handler's training needs and other technical requirements.

- address existing and new cyber technologies are adequately addressed in policies and procedure.

An incident response plan checklist should be an amalgamation of the following key practices:

- conduct regular reviews, audits and tests to protect against security breach.

- classify business data in the order of its sensitivity and security requirements.

- selecting of appropriate incident response team structure.

- complying with security-related incident regulations and law enforcement procedures.

Preparation for Incident Response and Handling

Create a core team

- Integrity of business security demands the presence of an effective incidence response team and the latter can be achieved through the selection of appropriate structure and staffing models.

- Typically, a designated incident response team or personnel function as the first point of contact (POC) in a situation involving security breach in an organization.

- The incident handlers may then analyse the incident data, determine the impact of the incident, and act appropriately to limit the damage and restore normal services.

Preparation for Incident Response and Handling

- The incident response team’s success depends on the participation and cooperation of individuals throughout the organization.

- Therefore, an organization must create a core team, identify suitable individuals, discuss incident response team models, and provide advice on selecting an appropriate model.

A team model may be based on the following models:

- **Central Security Incident Response team:** a functional model for small organizations with limited or no geographic presence wherein a single incident response team handles core security computing.

- **Distributed Security Incident Response team:** this model is effective for large organizations (e.g. one team per division) and for organizations with major computing resources at distant locations (e.g. one team per geographic region, one team per major facility).

A team model may be based on the following models:

- **Coordinating team:** an incident response team provides advice to other teams without having authority over those teams.

- For example, a department wise team may assist individual agencies' teams and it is almost modelled as a CSIRT for CSIRTs.

- **Create tool kit, systems and instrumentation:** a jump kit is a portable case instrumental to incident response teams and it contains items such as laptop, appropriate software such as packet sniffers, digital forensics, back up devices, blank media etc.

Listed below are range of various tool kit, systems and instrumentation that may be useful in an incident response:

- **Incident handler communications and facilities:** these may include contact information of team members and others within the organization and external, on-call information matrix, incident reporting mechanisms such as phone numbers, email addresses, online forms, etc.

- Incident tracking systems; smartphones for round-the-clock communication; use of encryption software for internal team members; security materials storage facility etc.

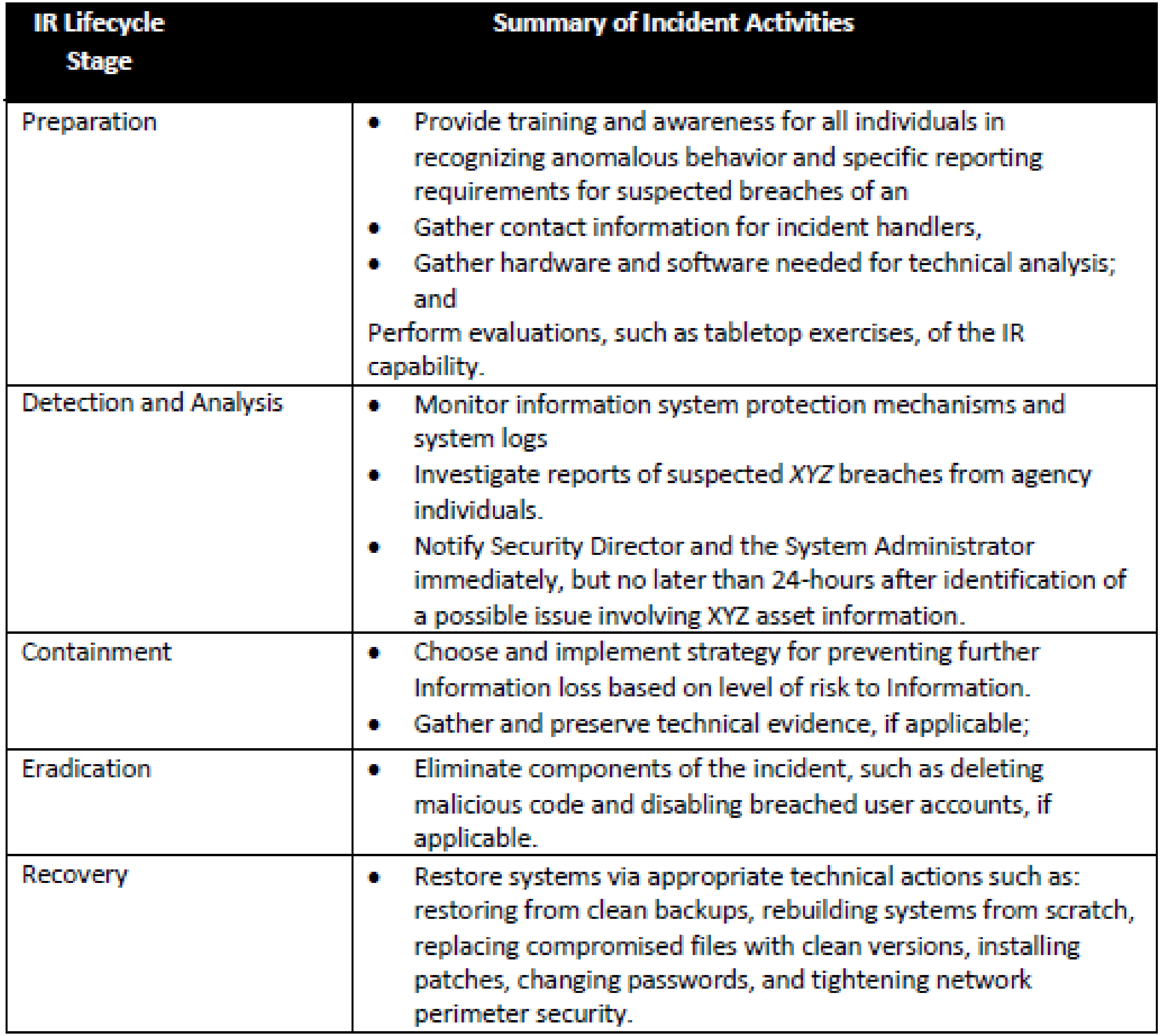
- **Incident analysis hardware and software**: digital forensic workstations and/ or backup devices to create disk images, preserve log files and save other relevant incident data etc. Laptops; spare workstations; servers; networking equipment or the virtualized equivalents for storing and trying

Listed below are range of various tool kit, systems and instrumentation that may be useful in an incident response:

- out malware; blank removable media; packet sniffers and protocol analyzers; digital forensic software; evidence gathering accessories such as digital cameras, audio recorders, chain of custody forms etc.

- **Incident analysis resources:** port lists, including commonly used ports and Trojan horse ports; documentation for Oss; applications; protocols etc. Network diagrams and lists of critical assets such as database servers; current baselines of expected network system and application activity; cryptographic hashes of critical files to speed incident analysis, verification and eradication.

- **Incident mitigation software:** access to images of clean OS and application installations for restoration and recovery purposes.



IR Lifecycle Stage	Summary of Incident Activities
Preparation	• Provide training and awareness for all individuals in recognizing anomalous behavior and specific reporting requirements for suspected breaches of an • Gather contact information for incident handlers, • Gather hardware and software needed for technical analysis; and Perform evaluations, such as tabletop exercises, of the IR capability.
Detection and Analysis	• Monitor information system protection mechanisms and system logs • Investigate reports of suspected *XYZ* breaches from agency individuals. • Notify Security Director and the System Administrator immediately, but no later than 24-hours after identification of a possible issue involving XYZ asset information.
Containment	• Choose and implement strategy for preventing further Information loss based on level of risk to Information. • Gather and preserve technical evidence, if applicable;
Eradication	• Eliminate components of the incident, such as deleting malicious code and disabling breached user accounts, if applicable.
Recovery	• Restore systems via appropriate technical actions such as: restoring from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security.

Sample Incident Response Evaluation Scenarios

***XYZ* Breach Scenario**	**Tabletop Exercise Objectives**
Through a routine evaluation of system logs, a system administrator discovers that XYZ's data has been exfiltrated from the system by an unauthorized user account.	• Determine the actions that would help prevent this type of incident (preparation). • Determine the controls in place that would help identify this incident, along with procedures on how to report the incident (detection and analysis). • How to prevent further damage (containment), • How to clean the system (eradication). • How to restore the system in a secure manner (recovery).
A remote user has lost his/her laptop. The user's job function required that XYZ's information be stored on the laptop.	
After a recent office move, it is discovered that a locked cabinet containing XYZ's information is missing.	

Incident Response Team

- **Incident response team members**
  - A single employee, with one or more designated alternates should be in charge of incident response.
  - In a fully outsourced model, this person oversees and evaluates the outsourcer’s work.
  - All other models generally have a team manager and one or more deputies who assume authority in the absence of the team manager.
  - Every team member should have good problem solving skills and critical thinking abilities.

Incident response team: roles and responsibilities

- An incident response team member should possess technical skills, such as **system administration**, **network administration**, **programming**, **technical support** or **intrusion detection**.

- An incident response team should be a combination of skilled members in the **area of technology** (e.g. operating systems and applications) and other technical areas such **as network intrusion detection**, **malware analysis** or **forensics**.

Roles and responsibilities

- A team member in an incident response unit is expected to have the basic understanding of the technologies used and their applications.
- The individual should be capable of comprehending and handling the following security incidents:
  - the **type of incident activity that is being reported** or seen by the community.
  - **the way in which incident response team services** are being provided (the level and depth of technical assistance provided to the constituency).
  - **the responses that are appropriate for the team** (e.g. what policies and procedures or other regulations must be considered or followed while undertaking the response).
  - **the level of authority the incident response team** has in taking any specific actions when applying technical solutions to an incident reported to the incident response team.

Developing skills in incident response personnel

- maintain, enhance and expand proficiency in technical areas and security disciplines as well as less technical topics such as the legal aspects of incident response.
- incentivize participation in staff conferences.
- promote deeper technical understanding.
- engage external technical knowledge facilitator with deep technical knowledge in needed areas to impart learning and development.

Developing skills in incident response personnel

- provide opportunities to perform other tasks in non-functional areas.

- rotate staffing of members across functions to gain new technical skills.

- create a mentoring program to enable senior technical staff to help less experienced staff learn incident handling.

- develop incident handling scenarios and conduct team discussions.

Incident response team structure

- After successfully selecting a functional core team, it is best followed that team members be further integrated and modelled into appropriate staffing based on the magnitude of incident response and size of the organization.

- Find details of the three types of staffing methods below:

- **In house employees**
- **Partially outsourced**
- **Fully outsourced**

Therefore, an organization must consider the following factors before selecting an appropriate incident response team structures:

- **The need for 24/7 availability:** real-time availability is considered one of the best for incident response options because the longer an incident last, the more potential there is for damage and loss.

- **Full-time versus part-time team members:** organizations with limited funding, staffing or incident response needs may have only part-time incident response team members, serving as more of a virtual incident response team.

- An existing group such as the IT help desk can act as a first POC for incident reporting and perform initial investigation and data collection.

- **Employee morale:** segregate administrative work and core incident response to minimize stress on employees and to help boost morale.

- **Cost:** implement sufficient funding for training and skills development of incident response team members the area of work function demands broader knowledge of IT.

- **Staff expertise:** incident handling requires specialized knowledge and experience in several technical areas.

- The breadth and depth of knowledge required varies based on the severity of the organization’s risks.

Outsourced

- In the case of outsourced work, the organization must consider not only the current quality (breadth and depth) of the outsourcer’s work, but also efforts to ensure the quality of future work.
- Document line of work or authority of outsourced incident response work appropriately and ensure actions for these decision points are handled.
- Divide incident response responsibilities and restrict access to sensitive information.
- Provide regularly updated documents that define what incidents outsources is concerned about.
- Create correlation among multiple data sources.
- Maintain basic incident response skills in-house.

Incident Response Team Dependencies

- It is important to identify other groups within the organization and rely on the expertise, judgment, and abilities of others, including response policy, budget, staffing established by management;
- information security staff members during certain stages of incident handling (prevention, containment, eradication, and recovery);
- IT technical experts (system and network administrators, legal departments to review plans, policies, documents etc.);
- public affairs;
- media relations;
- Human resources;
- business continuity planning;
- physical security and facilities management.

Different methods and techniques used when working with others

- **Incident response team services**

The main focus of an incident response team is performing incident response however it may also undertake the provision of the following services:

- **Intrusion detection**: incident response team analyzes incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies.
- **Advisory distribution:** the team also may also issue advisories within the organization regarding new vulnerabilities and threats through automated methods.
- **Education and awareness:** promote education and awareness among users technical staff know about detecting, reporting and responding to incidents through means such as workshops; websites; newsletters; posters and stickers on monitors and laptops.
- **Information sharing:** manage the organization’s incident information sharing efforts.

Defining the relationship between incident response, incident handling, and incident management

- **Incident response** means responding to computer security incidents systematically or by following a consistent incident handling methodology so that the appropriate actions are taken timely. It is a mechanism to minimize loss or theft of information and disruption of services caused by incidents.

- **Incident handling** refers to the several phases of incident response process i.e. preparation, detection and analysis, containment, eradication and recovery and post-incident activity required in adequate handling of an incident.

- **Incident management** is term used to describe the overall computing security management to detect the occurrence of incident, initiate and handle an incident response and prevent any future re-occurrences.

Routine operational procedures and tasks required to co-ordinate and respond to information security incidents

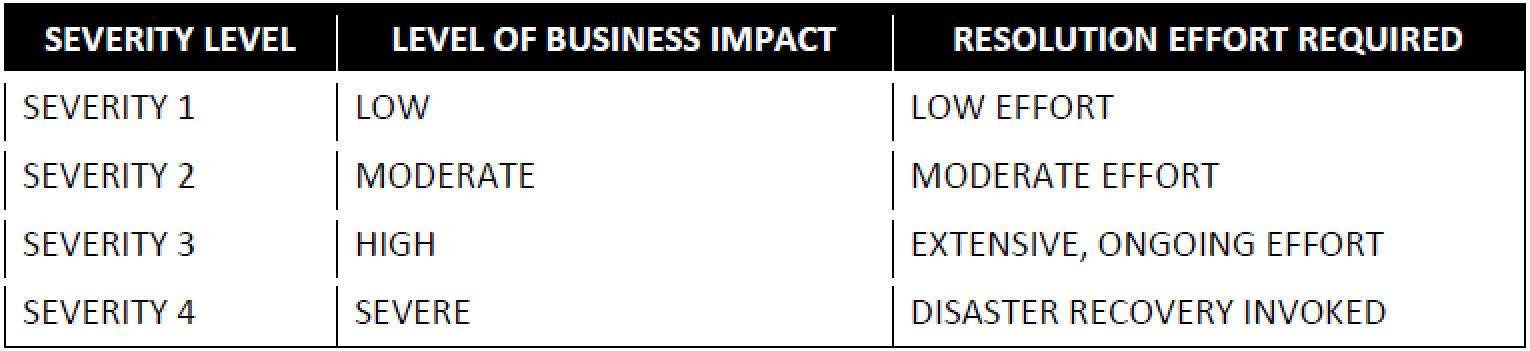
- Prepare to handle incidents.
- Use incident analysis hardware and software.
- Use incident analysis resources.
- Use of incident mitigation software.
- Management responsible for coordinating incident response among various stakeholders, minimizing damage, and reporting to Congress, OMB, the General Accounting Office (GAO), and other parties.
- Information security staff members may be needed during certain stages of incident handling (prevention, containment, eradication and recovery). For example, to alter network security controls (e.g. firewall rule sets).

Continued……

- IT technical experts (e.g. system and network administrators) can ensure that the appropriate actions are taken for the affected system, such as whether to disconnect an attacked system.
- Coordinate with relevant legal experts to review incident response plans, policies and procedures to ensure their compliance with law and federal guidance, including the right to privacy.
- Coordinate and inform the media and, by extension, the public.
- Ensure that incident response policies and procedures and business continuity processes are in sync.
- Coordinate with Physical Security and Facilities Management to access facilities during incident handling.

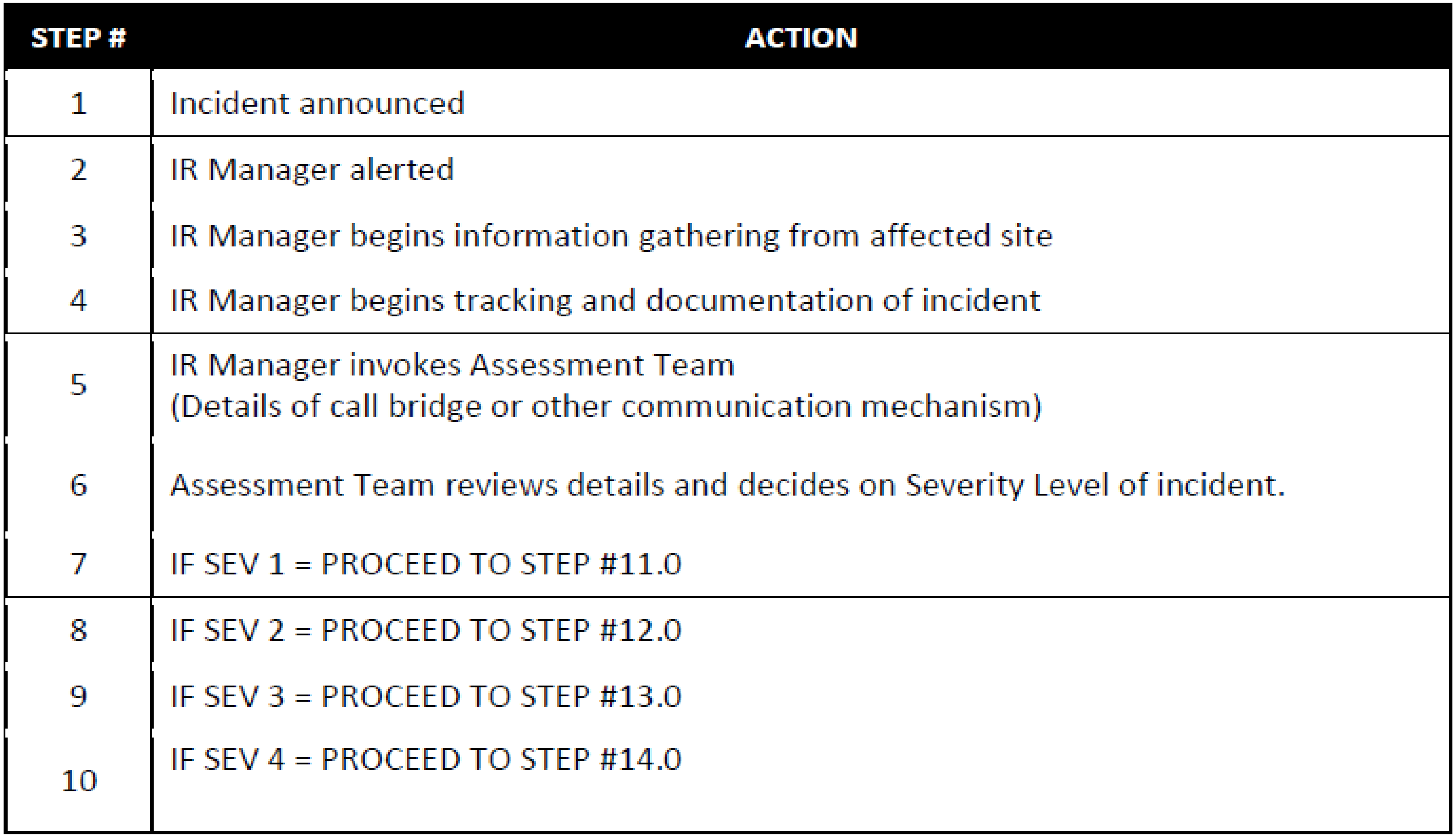
- A part of outlining the incident response framework involves the identification of IR Severity Levels.

- These levels will help the team understand the severity of an event and will govern the team’s response.
- Some suggestions for these levels are the following:



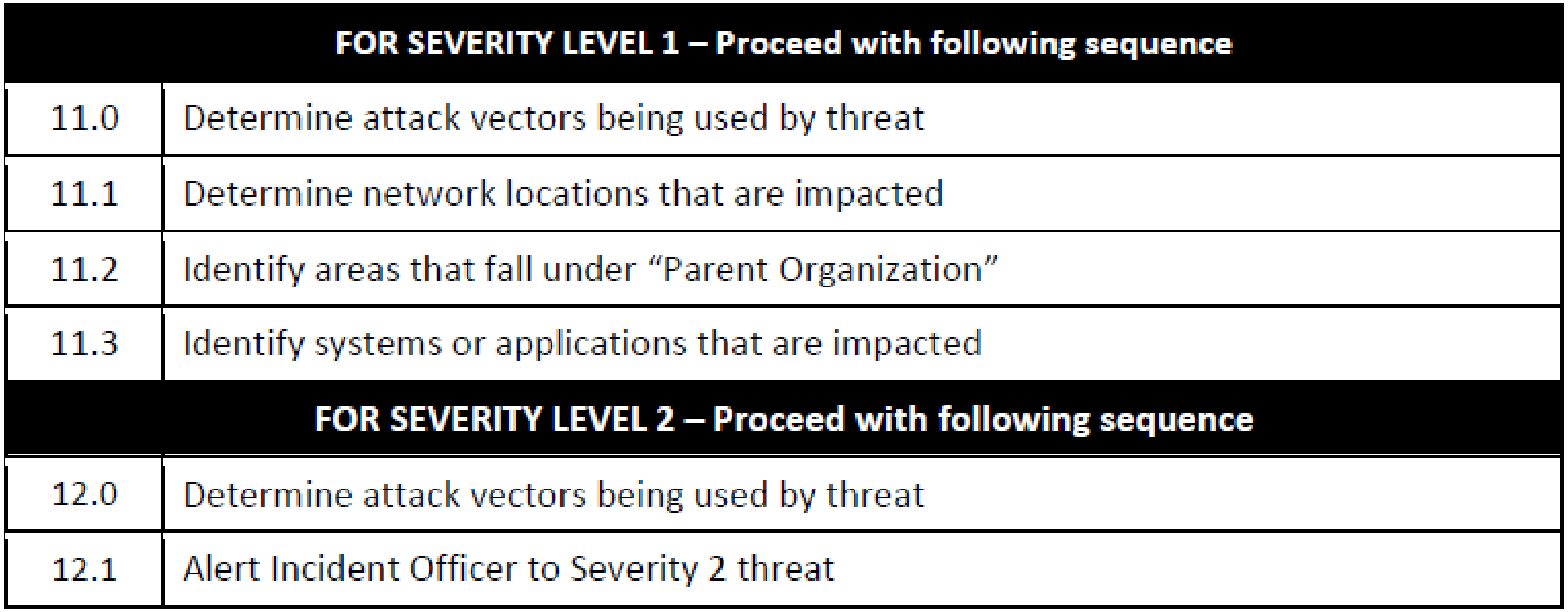
SEVERITY LEVEL	LEVEL OF BUSINESS IMPACT	RESOLUTION EFFORT REQUIRED
SEVERITY 1	LOW	LOW EFFORT
SEVERITY 2	MODERATE	MODERATE EFFORT
SEVERITY 3	HIGH	EXTENSIVE, ONGOING EFFORT
SEVERITY 4	SEVERE	DISASTER RECOVERY INVOKED

Start to create a documented action script that will outline your response steps so your IR Manager can follow them consistently. Your script should show steps similar to the following:



STEP #	ACTION
1	Incident announced
2	IR Manager alerted
3	IR Manager begins information gathering from affected site
4	IR Manager begins tracking and documentation of incident
5	IR Manager invokes Assessment Team (Details of call bridge or other communication mechanism)
6	Assessment Team reviews details and decides on Severity Level of incident.
7	IF SEV 1 = PROCEED TO STEP #11.0
8	IF SEV 2 = PROCEED TO STEP #12.0
9	IF SEV 3 = PROCEED TO STEP #13.0
10	IF SEV 4 = PROCEED TO STEP #14.0

Start to create a documented action script that will outline your response steps so your IR Manager can follow them consistently. Your script should show steps similar to the following:



FOR SEVERITY LEVEL 1 – Proceed with following sequence	
11.0	Determine attack vectors being used by threat
11.1	Determine network locations that are impacted
11.2	Identify areas that fall under “Parent Organization”
11.3	Identify systems or applications that are impacted
FOR SEVERITY LEVEL 2 – Proceed with following sequence	
12.0	Determine attack vectors being used by threat
12.1	Alert Incident Officer to Severity 2 threat

Incident Response Process

- Step 1: Identification
- Step 2: Incident recording
- Step 3: Initial response
- Step 4: Communicating the incident
- Step 5: Containment
- Step 6: Formulating a response strategy
- Step 7: Incident classification
- Step 8: Incident investigation
- Step 9: Data collection
- Step 10: Forensic analysis
- Step 11: Evidence protection
- Step 12: Notify external agencies
- Step 13: Eradication
- Step 14: Systems recovery
- Step 15: Incident documentation
- Step 16: Incident damage and cost assessment
- Step 17: Review and update the response policies
- Step 18: Training and awareness

Step 1: Identification

Obtaining and validating information related to information security issues

- In incident handling, detection may be the most difficult task.
- Incident response teams in an organization are equipped to handle security incidents using well-defined response strategies beginning with information gathering.
- Preparing a list most common attack vectors such as external/removable media, web, email, impersonation, improper use by authorized users etc. can narrow down to the most competent incident handling procedure.
- Therefore, it is important to validate each incident using defined standard procedures and document each step taken accurately.

Common issues and incidents of information security that may require action and whom to report

- An indicator may not always translate into a security incident given the possibility of technical faults due to human error in cases such as server crash or modification of critical files.

- Determining whether a particular event is actually an incident is sometimes a matter of judgment.

- It may be necessary to collaborate with other technical and information security personnel to make a decision.

- Therefore, incident handlers need to report the matter to highly experienced and proficient staff members who can analyse the precursors and indicators effectively and take appropriate actions.

Mentioned below are some of the means to conduct initial analysis for validation:

- **Profiling Networks and Systems** in order to measure the characteristics of expected activity so that changes to it can be more easily identified and used one of the several detection and analysis techniques.
- **Studying networks, systems and applications** to understand what their normal behavior is so that abnormal behavior can be recognized more easily.
- **Creating and implementing a log retention** policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks.
- **Correlating events using evidence of an incident** captured in several logs such wherein each may contain different types of data — a firewall log may have the source IP address that was used, whereas an application log may contain a username.
- **Synchronizing hosts clock using protocols** such as the Network Time Protocol (NTP) to record time of attack.

Mentioned below are some of the means to conduct initial analysis for validation:

- **Maintain and use a knowledge base of information** that handlers need for referencing quickly during incident analysis.

- **Use internet search engines for research** to help analysts find information on unusual activity.

- **Run packet sniffers to collect additional data** to record traffic that matches specified criteria should keep the volume of data manageable and minimize the inadvertent capture of other information.

- **Filter the data to segregate** categories of indicators that tend to be insignificant.

Step 2: Incident recording

- Any occurrences of incident must be recorded and the incident response team should update the status of incidents along with other pertinent information.

- Observations and facts of the incident may be stored in any of the following sources such as logbook, laptops, audio recorders and digital cameras etc.

Incident record samples and template

- Documenting system events, conversations and observed changes in files can lead to a more efficient, more systematic and error-free handling of the problem.

- Using an application or a database, such as an issue tracking system helps ensure that incidents are handled and resolved in a timely manner.

The following useful information are to be included in an incident record template:

- Current status of the incident as new, in progress, forwarded for investigation, resolved etc.
- Summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (system owners, system administrators etc.)
- List of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (rebuild the host, upgrade an application etc.)

Step 3: Initial response

- Commence initial response to an incident based on the type of incident, the criticality of the resources and data that are affected, the severity of the incident, existing Service Level Agreements (SLA) for affected resources, the time and day of the week, and other incidents that the team is handling.

- Generally, the highest priority is handling incidents that are likely to cause the most damage to the organization or to other organizations.

Step 4: Communicating the incident

- The incident should be communicated in appropriate procedures through the organization’s points of contact (POC) for reporting incidents internally.

- Therefore, it is important for an organization to structure their incident response capability so that all incidents are reported directly to the incident response team, whereas others will use existing support.

Assigning and escalating information on information security incidents

- Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time. This can happen for many reasons.
- For example, cell phones may fail or people may have personal emergencies.
- The escalation process should state how long a person should wait for a response and what to do if no response occurs.
- On failure to respond within a stipulated time, then the incident should be escalated again to a higher level of management.
- This process should be repeated until the incident is successfully handled.

Step 5: Containment

Containment and Quarantine

- Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment so that is an important consideration early in the course of handling each incident.
- Containment provides time for developing a tailored remediation strategy.
- An essential part of containment is decision-making where the situation may demand immediate action such as shut down a system, disconnect it from a network and disable certain functions.

Various containment strategies may be considered in the following ways:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (network connectivity, services provided to external parties etc.)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (partial containment, full containment etc.)
- Duration of the solution (emergency work around to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution etc.)

Quarantine

- Handling an incident may necessitate the use of strategies to contain the existing predicament and one such method being redirecting the attacker to a sandbox (a form of containment) so that they can monitor the attacker’s activity, usually to gather additional evidence.

- Hence, once a system has been compromised and if allowed with the compromise to continue, it may help the attacker to use the compromised system to attack other systems.

Understand network damage

- On the other hand, containment may give rise to another potential issue and that is some attacks may cause additional damage when they are contained.

- When the incident handler attempts to contain the incident by disconnecting the compromised host from the network, the subsequent pings will fail.

- As a result of the failure, the malicious process may overwrite or encrypt all the data on the host’s hard drive.

Identify and isolate the trust model

- Network information systems are vulnerable to threats and benign nodes often compromised because of unknown, incomplete or distorted information while interacting with external sources.

- In this case, malicious nodes need to be identified and isolated from the environment.

- The solution to insecure can be found in the establishment of trust.

- Trust model can be formed based on the characteristics, information sources to compute, most relevant and reliable information source, experience of other members of community etc.

Step 6: Formulating a response strategy

- An analysis of the recoverability from an incident determines the possible responses that the team may take when handling the incident.

- An incident with a high functional impact and low effort to recover from is an ideal candidate for immediate action from the team.

- In situations involving high end data infiltration and exposure of sensitive information the incident response team may formulate response by transferring the case to strategic level team.

- Each response strategy should be formulated based on business impact caused by the incident and the estimated efforts required to recover from the incident.

- Incident response policies should include provisions concerning incident reporting at a minimum, what must be reported to whom and at what times.

- Important information to be included are CIO, head of information security, local information security officer, other incident response teams within the organization, external incident response teams (if appropriate), system owner, human resources (for cases involving employees, such as harassment through email), public affairs etc.

Step 7: Incident classification

Classifying and prioritizing information security incidents

An incident may be broadly classified based on common attack vectors such as external/ removable media; attrition; web; email; improper usage; loss or theft of equipment; miscellaneous.

Incident prioritization

- **Functional impact of the incident** on the existing functionality of the affected systems and future functional impact of the incident if it is not immediately contained.

- **Information impact of the incident** that may amount to information exfiltration and impact on organization's overall mission and impact of exfiltration of sensitive information on other organizations if any of the data pertain to a partner organization.

Step 7: Incident classification

- **Recoverability from the incident** and how to determine the amount of time and resources that must be spent on recovering from that incident.

- Necessity to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

Step 7: Incident classification

- **Incident classification guidelines and templates**

Organizations should document their guidelines and templates to handle any incident but should focus on being prepared to handle incidents that use common attack vectors.

Capturing the attack pattern formally with required information may help understand specific parts of an attack, how it is designed and executed, providing the adversary's perspective on the problem and the solution, and gives guidance on ways to mitigate the attack's effectiveness.

- **Requirements** – identification of relevant security requirements, misuse and abuse cases.

- **Architecture and design** – provide context for architectural risk analysis and guidance for security architecture.

- **Implementation and development** – prioritize and guide review activities.

- **Testing and quality assurance** – provide context for appropriate risk-based and penetration testing.

- **System operation** – leverage lessons learned from security incidents into preventative guidance.

- **Policy and standard generation** – guide the identification of appropriate prescriptive organizational policies and standards.

Incident prioritization guidelines and templates

- Creating written guidelines for prioritizing incidents serve as a good practice and help achieve effective information sharing within an organization.

- The step may also help in identifying situations that are of greater severity and demand immediate attention.

- An ideal template for incident prioritization should be formulated based on relevant factors such as the functional impact of the incident (e.g. current and likely future negative impact to business functions), the information impact of the incident (e.g. effect on the confidentiality, integrity and availability of the organization's information) and the recoverability from the incident (e.g. the time and types of resources that must be spent on recovering from the incident).

Step 8: Incident investigation

- One of the key tasks of an incident response team is to receive information on possible incidents, investigate them, and take action to ensure that the damage caused by the incidents is minimized.

- **Following up an incident investigation**

In the course of the work, the team must adhere to the following procedures deemed appropriate to a given situation:

Step 8: Incident investigation

- receive initial investigation and data gathering from IT help desk members and escalate to high strategic level specialist if situation demands.
- use appropriate materials that may be needed during an investigation.
- should become acquainted with various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them.
- maintain record of chain of custody forms should detail the transfer and include each party’s signature while transferring evidence from person to person.
- should be careful to give out only appropriate information — the affected parties may request details about internal investigations that should not be revealed publicly.

- ensure law enforcement are available to investigate incidents wherever necessary.

- collect required list of evidence gathered during the incident investigation.

- should collect evidence in accordance with procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court.

Lessons learnt from security incident

- Handling and rectifying security incident work best in a “learning and improving” model.

- Therefore, incident handling teams must evolve to reflect on new threats, improved technology and lessons learned. Each lesson’s learned brief must include the following agenda:
  - What exactly happened and during times?
  - How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
  - What information was needed sooner?
  - Were any steps or actions taken that might have inhibited the recovery?
  - What would the staff and management do differently the next time a similar incident occurs?