CHAPTER 4. VARIOUS SECURITY MODELS FOR INCIDENT HANDLING
4.1 Introduction

Computer security incident response has become an important component of information technology (IT) programs. Security-related threats are not only numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently (NIST in its publication SP 800-61, defines incident a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices) [68]. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response mechanism is therefore necessary for minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. For effective and efficient response mechanism, there are various security incident handling models that have been developed such as SANS, NIST, ISO, CERT and RSP. The security incident handling models generally follow a five stage process. The commonly used stages are illustrated below [69]:

1. *Preparation and Planning Stage* involves preparation of the process for detection and reaction to the security incidents.
2. *Detection and Analysis stage* involves assessment and identification of potential security breaches.
3. *Containment Stage* ensures that the impact of the security abuse on the organization is minimized.
4. *Eradication Stage & Recovery Stage* aims to eliminate the causes of the security attack and plans for improvement in network defenses to counter security vulnerability. During this phase, the recovery of the Information and Communication Technology (ICT) components and restoration of its operational status are done.
5. *Post Incidence and Follow up Stage* involves preparation of report and analysis of the progress of detecting and reacting to security incidents.
These security incident handling models help in analyzing incident-related data and determining the appropriate response to each incident. Each model has advantages and disadvantages over the other model as they have been developed over the time, as well as, there are security issues in the existing incident handling models.

This chapter presents the detailed analysis of various security models for incident handling such as SANS, NIST, CERT, ISO and RSP. Advantages and disadvantages of the existing incident handling models have been discussed. This chapter also describes the security issues related to the existing incident handling models.

### 4.2 Overview of Security Incident Handling

Security incident handling is a set of continuous processes governing the activities before, during and after a security incident occurs. A well-defined security incident handling plan is vital to the efficient and effective handling of security incident, minimising impact and damage, and rapidly restoring operation of a computer system. The major guidelines and preparedness for security incident handling are given below [68]:

- i. Ensure that the required resources are available to deal with the incidents, including manpower, technology, etc.
- ii. Ensure that all responsible parties have clear understanding about the tasks they should perform during an incident by following predefined procedures
- iii. Ensure that the response is systematic and efficient and there is a prompt recovery for the compromised system
- iv. Ensure that the response activities are recognised and coordinated
- v. Minimise the possible impact of the incident in terms of information leakage, corruption and system disruption etc.
- vi. Share experience in incident response within the organisation
- vii. Prevent further attacks and damages
- viii. Deal with related legal issues
There are three major steps involved in security incident handling as shown below in figure 4.1 and the processes involved in each of the steps are briefly described [68][70][71].

**Stage 1: PLANNING AND PREPARATION**
- Security Incident Handling Plan
- Reporting Procedure
- Escalation Procedure
- Security Incident Response Procedure
- Training and Education
- Incident Monitoring Measure

**Stage 2: RESPONSE TO SECURITY INCIDENT**
- Identification
- Escalation
- Containment
- Eradication
- Recovery

**Stage 3: AFTERMATH**
- Post-incident analysis
- Security Incident Report
- Security Assessment
- Review Existing Protection
- Investigation & Prosecution

*Figure 4.1: Security Incident Handling Steps*

### 4.2.1 Planning and Preparation (Stage 1)

Proper and advanced planning ensures the incident response activities are known, coordinated and systematically carried out. It also facilitates the organisations concerned to make appropriate and effective decision in tackling security incident, and in turn minimises the possible damages. Major activities involved in planning and preparation are as follows:

i. Security Incident Handling Plan
ii. Reporting Procedure
iii. Escalation Procedure
iv. Security Incident Response Procedure
v. Training and Education
vi. Incident Monitoring Measure

i. Security Handling Plan

In general, a security incident handling plan should cover the following major items:

1. Scope:
   The scope will define the functional area that the security incident response team will be responsible for. It may be for the whole organization or for a specific information system or application within the organization.

2. Goals and Priorities:
   A set of goals under the security incident handling plan should be clearly defined in advance and prioritised according to the system and management requirements.

3. Roles and Responsibilities:
   The roles and responsibilities of all parties participating in the security incident handling process should be clearly defined.

4. Constraints:
   Constraints like resources, technology and time should be considered. This may affect the result of the security incident handling process. For example, if there is a lack of internal technical expertise, it may be necessary to acquire external consultants or service contractors.

ii. Reporting Procedure

The reporting procedure should clearly define the steps and processes in reporting any suspicious activities to all parties involved in a timely manner. Comprehensive contact information, such as telephone numbers (office hours, non-office hours and mobile), email address, and fax number, should be set out in the reporting procedure to ensure effective communication among responsible personnel.

iii. Escalation Procedure

The escalation procedure defines the way to escalate the incident to management and relevant parties to ensure that important decisions are promptly taken. In the course of an incident, when many urgent issues have to be addressed, it could be difficult to find the proper person to handle a variety of matters. Important contact lists for addressing legal, technical, and managerial issues should be prepared in advance to facilitate different
stages of security incident handling. As such, establishing an escalation procedure contributes a major task in the preparation and planning stage.

iv. Security Incident Response Procedure

The security incident response procedure defines the steps to be followed in case an incident occurs, which aims at minimising damage, eradicating the cause of the incident and restoring the system to normal operation etc., in accordance with the predefined goals and priorities.

The system or functional area's Manager should establish a security incident response procedure to guide the security incident response team through the handling process. The procedure should be made known to all staff, including management personnel, for their reference and compliance. It should be clear, straightforward and easily understood so that all the personnel have clear knowledge about what they need to do. The procedure should be regularly tested (e.g. drill) and updated.

v. Training and Education

It is essential to provide adequate staff training to ensure all concerned staff and management is capable of handling security incidents. Staff should be familiar with the procedures to handle the incident from incidents reporting, identification, and taking the appropriate actions to restore the system to normal operation. Drills on incident handling should also be organised regularly for staff to practice the procedures.

In addition, sufficient training to system operation and support staff on security precaution knowledge is also important, in order to strengthen the security protection of the system or functional area, and reduce the chance that an incident may occur.
vi. Incident Monitoring Measure

A sufficient level of security measures for incident monitoring should be implemented to protect the system during normal operation as well as to monitor potential security incidents. The level and extent of measures to be deployed will depend on the importance and sensitivity of the system and its data, as well its functions. Some typical measures for security incident monitoring are listed below:

1. Install firewall device and apply authentication and access control measures to protect important system and data resources.
2. Install intrusion detection tool to proactively monitor, detect and respond to system intrusions or hacking.
3. Install anti-virus tool and malicious code detection and repair tool to detect and remove computer virus and malicious codes, and prevent them from infecting system operations.
4. Perform periodic security check by using security scanning tools to identify existing vulnerabilities and perform a gap analysis between stated security policy and actual security arrangement.
5. Install content filtering tool to detect malicious contents or codes in emails or web traffic.
6. Enable system and network audit logging to facilitate the detection and tracing of unauthorized activities.
7. Develop programs and scripts to assist in the detection of suspicious activities, monitoring of system and data integrity, and analysis of audit log information.

4.2.2 Response to Security Incident (Stage 2)

Response to security incident involves developing procedure to evaluate incidents and to respond in order to restore affected system components and services as soon as possible. The procedure is broadly categorised into five stages: Identification, Escalation, Containment, Eradication and Recovery. Understanding the activities of each stage can facilitate the development of an effective security incident response procedure. The response procedure may not strictly follow the order of the five stages, which has to be customized to suit
practical needs. For instance, escalation may have already taken place for some incidents as soon as they are reported.

4.2.3 Aftermath (Stage 3)

Restoring a system to normal operation does not mark the end of a security incident handling process. It is also important to perform the necessary follow up action. Actions may include evaluation of the damage caused, system refinement to prevent recurrence of the incident, security policies and procedures update, and case investigation for subsequent prosecution.

Follow up actions can lead to the following:

i. Improvement in incident response procedure
ii. Improvement in security measures to protect the system against future attacks
iii. Prosecution of those who have breached the law
iv. Familiarize others with security incident response process
v. Educate those parties involved, about the experience learnt

Follow up actions include:

i. Post-incident analysis
   Post-incident analysis involves conducting analysis on the incident and response actions for future reference. It helps to gain a better understanding of the system’s threats and vulnerabilities so that more effective safeguards can be put in place.

ii. Post-incident report
   Based on the post-incident analysis, a post-incident report should be prepared with brief description of the incident, response, recovery action, damage and experience learnt. The report should be prepared by the manager of the concerned information system and be disseminated to the Information Security Incident Response Team (ISIRT) for reference, so that prompt preventive actions could be taken to avoid the recurrence of similar security incident in other systems and services.

iii. Security assessment:
   A periodic security risk assessment and audit exercise is recommended for systems under security exposure, especially for those that have been affected by security incident. Security review and audit of a system should be an ongoing exercise to promptly identify possible security loopholes and/or areas of
improvement to the system as a result of technology advancement in both security protection as well as attack/intrusion.

iv. Review existing protection:
From the post-incident analysis and periodic security assessment exercise, areas for improvement can be identified in respect of the system's security policies, procedures and protection mechanisms. Due to rapid advancement of technology, security related policies, procedures and protection mechanisms must be updated regularly to ensure the effectiveness of the overall security protection to a computer system. In the case of a post-incident event, policies, procedure and guidelines should also be reviewed and modified as necessary in order to align with preventive measures.

v. Investigation and prosecution:
If appropriate, case investigation, disciplinary action or legal prosecution against individuals who caused the incident should also be conducted. Incidents suspected to be caused by a criminal offence should be reported to the Law Enforcement Agencies for case investigation and evidence collection.

4.2.4 Incident Response Team Structure
Incident handling requires a formation of an incident response team to handle incidents within the organization. The size of the team depends on the resources available and the services that are necessary to provide [72]. One or more team members, depending on the magnitude of the incident and availability of personnel, will then handle the incident. The incident handlers analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage and restore normal services. The incident response team’s success depends on the participation and cooperation of individuals throughout the organization. There are different incident response team models which have been proposed by NIST. The description of these response team models are given below to understand the practicality of incident handling [68].

- Central Incident Response Team: A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for organizations with minimal geographic diversity in terms of computing resources.
• **Distributed Incident Response Teams:** The organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization. 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). However, the teams should be part of a single centralized entity so that the incident response process is consistent across the organization and information is shared among teams. This is particularly important because multiple teams may see components of the same incident or may handle similar incidents.

• **Coordinating Team:** An incident response team provides advice to other teams without having authority over those teams—for example, a department wide team may assist individual agencies’ teams. This model can be thought of as a CSIRT for CSIRTs.

### 4.3 Security Incident Handling Models

Incident handling is complex and requires methodologies to evaluate incidents and to respond in order to restore affected systems, networks and services as soon as possible. There are number of incident handling models such as SANS, NIST, CERT, ISO and RSP which have been proposed for this purpose. This section discusses these models in detail.

#### 4.3.1 SANS Model

This model was proposed by the SANS Institute in 1998. This model consists of a six-stage process which is illustrated in Figure 4.2 [52]

1. **Preparation Stage** – In this stage, the process for detecting and reacting to the security incidents are prepared.

2. **Identification Stage** – In this stage, assessment and identification of potential security breaches are made.
3. **Containment Stage**– During this stage, the impact of the security abuse on the organization is minimized.

4. **Eradication Stage** – The aim of this stage is to eliminate the reasons of the Security Incident. Plans for improving network defenses to counter security vulnerability are made.

5. **Recovery Stage**– During this phase, the recovery of the Information and Communication Technology (ICT) components and restoration of its operational status are done.

6. **Follow-Up Stage**– In this phase, the preparation of report and analysis of the progress of detecting and reacting to security incidents are made.

![SANS Security Incident Handling Model](image)

**Figure 4.2: SANS Security Incident Handling Model**

The main advantage of this model is that it restores the normal ICT operations in a short duration in case a security breach. This model tries to mitigate the security issues as quick as possible. However, in this model the processes for gathering information about the incident are not defined and hence the proper analysis about the incident is not possible. Another disadvantage of this model is that there is no scope for the stakeholders to implement their decision.
4.3.2 NIST Model

This model was proposed by National Institute of Standards and Technology in 2004 and consists of a four-stage process which is illustrated in Figure 4.3[51] [68].

1. Preparation Stage – During this phase, the organizational process are identified and adjusted to the general process of handling security incidents. The objective of this phase is to detect and to react to the security incidents properly.

2. Detection and Analysis Stage – This stage covers all methods concerning collection of information about the system operation, the process of detection of abuse and analysis of security incident occurrences.

3. Containment, Eradication, and Recovery Stage – The goal of this phase is to minimize the negative impact of security breaches and to restore normal operational status of the ICT system.

4. Post–Incident Phase- The goal of processes involved in this phase is to protect ICT environment from the reoccurrence of similar security attacks in the future.

![Figure 4.3: NIST Security Incident Handling Model](image)

The main advantage of this NIST model is that, it is a continuously improvising incident handling model. It collects the comprehensive information about the incident and hence, a
business impact analysis is done. However, this model does not predict the normalcy restoring time. Moreover, the role of stakeholders is not defined properly. This model does not describe the procedure for integrating and complying with the security standards.

### 4.3.3 CERT Model

CERT model was presented by Carnegie Mellon University Software Engineering Institute, USA in 2005. Its main objective was to foster the growth of global incident management capability [51]. This model consists of a five-stage process which is illustrated in Figure 4.4.

1. **Preparation Stage**– During this stage, incident management policies and the corresponding processes for implementations is defined in order to effectively handle security incidents.

2. **Detection Stage**- In this stage, security incident reports are prepared and analyzed.

3. **Triage Stage**- In this stage the incidents detected in the previous phase are categorized in order to standardize their further management. During this stage, the incidents are also prioritized and a team of competent employees are assigned to tackle the incidents.

4. **Response Stage**- The goal of this phase, is to ensure a proper incident handling. This stage consists of various sub stages, which ensure a proper security handling procedure. The sub stages are: Verification, Containment, Notification, Analysis, Eradication and Mitigation and Follow–up.

5. **Protection Stage**- During this stage, the internal and external parameters that control the security vulnerability are updated and adjusted based on the current threats that are detected.
Some of the disadvantages of SANS model and NIST model have been resolved by CERT framework. The main advantage of this CERT model over SANS model is that, it is a continuously improvising incident handling framework.

4.3.4 ISO Model

This model was proposed by International Standards of Organization in 2005. This model consists of a four-stage process which is illustrated in Figure 4.5 [51].

1. Planning and Preparation Stage– In this stage, all activities resulting in a development of a new process to detect and to react to security incidents, which offers effective control and all necessary safety mechanisms are prepared.

2. Use Stage– This stage uses actions focusing on detection and reaction to security incidents, conducted in accordance to a plan arranged and approved in the previous stage.

3. Review Stage– This stage reviews a number of measures taken after the incident is handled, in order to determine the background of incident in detail.

4. Improvements Stage – This stage is continuous strengthening phase. The goal is to enhance the general process of handling security incidents.
Figure 4.5: ISO Security Incident Handling Model

This model is based on the concept of Plan-Do-Check-Act (PDCA). It is the basis for defining ISO 9000 and ISO 14000 standards. The main advantage of ISO model is its integrity with other ISO standards. However, it does not describe the process of collecting information in case of a security incident. It also does not describe the process of risk management and eradication of security breaches.

4.3.5 RSP Model

M.Ryba, J.Sulwinski and A. Poniewierski had proposed this model in 2008. This model is based on the methodologies proposed by SANS, NIST, CERT and ISO model. The main objective of this model is to provide a systematic and coherent approach to the process of detection and reaction of security incidents [51]. This model consists of a four-stage process which is illustrated in Figure 4.6.

1. **Planning and Preparation Stage** – This stage constitutes the key phase of defining the process of detection and reaction to abuse in IT systems. The actions carried out are focused on the development of organizational infrastructure for IT incident handling in three following layers:
   - *Process Layer* – creating a strategy, policy and detailed procedures for detection and reacting to incidents
   - *Organization Layer* – assigning human resources necessary for incident
handling, deciding on organizational structure (distributed or centralized), appointing a team responsible for reaction to security incidents, creating a training program for team members and employees, etc.

- **Technology Layer** – the development and implementation of mechanisms for gathering information on events concerning security of all IT systems used in the organization and of tools supporting the process of detecting and reacting to abuse.

2. **Use Stage** – This stage constitutes the central part of the presented process of detection and reaction to IT systems abuse. In this phase, the following steps have been defined:

- **Detection and Reporting** - Detection and Reporting focuses on collecting events connected with IT environment security and reporting them to all people who may be involved.

- **Evaluation and Decision Making** - In this stage, the classification of abuse is conducted along with the assessment of its impact on the IT environment. Depending on the decision made, the course of action regarding the abuse event is indicated. During this step, the decisions concerning the seizure of evidence material and its analysis are made.

- **Reaction** - The following actions are taken based on the classified data on abuse during this stage:
  
  i. Publishing – contacts with environment for the purpose of acquiring or passing information on the detected abuse (e.g., informing the board, internal and external communication department);
  
  ii. Containment – all actions undertaken in order to minimize the negative influence of the abuse on the IT environment in the organization;
  
  iii. Eradication – measures connected with the elimination of factors which made the abuse possible; and
  
  iv. Recovery – activities carried out in order to restore normal operational status of the IT system.
3. **Review** - the following steps are conducted during the Review phase:
   - Analysis of evidence material located outside the IT system related to abuse
   - Preparation of enhancements for the IT environment connected with the identified abuse
   - Preparation of potential improvements to the process of detecting and reacting to abuse in case when deficiencies are discovered
   - Preparation of final report

4. **Improvements** - The Improvements stage focuses on the implementation of prevention, detection, and correction mechanisms in the IT environment of the organization. It also concentrates on implementing enhancements to the general process of detection and reaction to IT systems abuse in all layers (process layer, organization layer, and technology layer).
Though this model is based on PDCA concept and also flexible to adopt in an ISO standard environment but it does not describe the role of stakeholders to design in a security incident model. Disaster management plans are not enumerated. It does not provide the framework for recovery.

4.4 Conclusion

Responding to security incidents has always been an important part in the science of Information Security. With our heavy reliance on computers, networks and applications for nearly all sorts of daily operations a major concern arises: privacy. Formal methodologies for Incident Response such as SANS, NIST, CERT, ISO and RSP have been developed to maintain privacy by handling incidents effectively. The main goal of every methodology is to detect and react to incidents and to establish guidelines that can help potential security breaches to be managed properly. There are security concerns of the proposed methodologies which need to be taken into account while handling the incidents. Therefore, it is crucial to choose the one that best suits the organization’s needs, and to ensure its proper implementation and application.