# Unit-6
# Responding to Security Incidents and Breaches

# Introduction

Security provides a safe and danger free environment, wherein people can conduct their daily chores and businesses. In a rapidly changing social and technological environment, understanding of security aspects, actions and use of modern equipment is of great relevance for improving security. However there is no concept of an ideal security. Security set up of any organization is subject to threat, vulnerability and risks and incidents of various nature, generally termed as security/safety incidents or breaches. These incidents takes place because of various reasons such as human error, technological and equipment errors.

The Security Incident Management is the process of managing security incidents of any type. It enables security personnel to create and manage incident records so that an accurate and detailed record of individual security incidents is maintained. Incident is recorded on specific incident types and specific locations defined at building, floor and even room level, so that relevant officers, supervisors, safety officers and others are always informed. Ideally all incidents should be investigated so that it can help us to analyse the weakness in the current system determine economic losses, improve upon the standards and systems, recommend action to prevent a recurrence. Security Managers can also generate detailed reports by any combination of search parameters including incident category, incident type, crime/non-crime, etc.

The aim of this Unit is to provide you with the knowledge and skills to understand the need and importance of incident management. Incident management is practiced basically to establish what happened, identify measures to prevent its recurrence, data gathering, trend analysis, and to determine immediate and underlying causes of the incident.

# Session-1
# Incident Management

## Relevant Knowledge

An incident is an alert to the possibility that a breach of security/safety may be taking or may have taken place. It is an event which is not part of the standard operation and which causes or may cause disruption in the work or business.

## Categories of an Incident

Incidents can be categorized into security incidents and safety incidents

### Examples of Security Incident

Theft is a case of breach of security of material. A thief's intention is to steal the belongings of someone. Since prevention of theft is the responsibility of security personnel, any theft occurring or likely to occur assumes the status of a security incident. Thefts can be major and minor in nature and require formal investigation for ascertaining the cause and subsequent punitive actions.

**Intentional Damage** is an act that causes damage to the identity, reputation or physical assets with a malafide intention. The effects may not be immediate but may surface later. Here it becomes difficult to pinpoint responsibility as the beneficiary may be operating 'behind the scene'. However, since the intention itself becomes malicious, the act is serious and requires to be investigated.

### Examples of Safety Incident

**Slips, Trips, and Falls Constitute** the majority of general industry accidents. Second only to motor vehicle accidents; slips, trips and falls are the most frequent accidents leading to personal injury. Slips trips and falls can result in head injuries, back injuries, broken bones, cuts and sprained muscles. There are many situations that may cause slips, trips, and falls, such as ice, wet spots, grease, polished floors, loose flooring or carpeting, uneven walking surfaces, clutter, electrical cords, open desk drawers and filing cabinets.

Loose, irregular surfaces such as gravel, shifting floor tiles, and uneven sidewalks, can make it difficult to maintain your footing. Most slip, trip and fall incidents are preventable with general precautions and safety measures.

An electric shock can occur upon contact of a human body with any source of voltage high enough to cause sufficient current flow through the muscles or nerves. The minimum detectable current in humans is thought to be about 1 mA. The current may cause tissue damage or heart, if it is sufficiently high.

## Incident Management

The process and procedures followed to manage an incident, identify the root cause from the time it occurs till restoration takes place. The objective of incident management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.

## Root Cause Analysis

Root cause analysis (RCA) structured approach to identifying the factors that resulted in the nature, the magnitude, the location, and the timing of the harmful consequences of one or more past events in order to identify what behaviours, actions, inactions, or conditions need to be changed to prevent recurrence of similar harmful outcomes.

Root cause analysis can help to transform a reactive culture into a forward-looking culture that solves problems before they occur or escalate.

More importantly, it reduces the frequency of problems occurring over time within the environment where the RCA process is used.

## Factors Causing Incidents

There are two types of factors causing incidents, active failure, an action that has immediate effects and has the likely hood to cause an incident/accident. The second is dormant or delayed action, as these events can take years to have an effect; they usually combine with triggering events and then cause the incident/accident.

## Direct Causes

These failures are unsafe acts (errors and violations) committed by those at the end of the system or process (the actual operators of machinery, supervisors of tasks/process). It is the people at the human-system interface whose actions can, and sometimes do, have immediate adverse consequences.

## Indirect Causes

They are created as the result of decisions taken at different levels of an organisation. There damaging consequences may lie dormant for a long time; only becoming evident when they combine with local triggering factors. For example, the planning, scheduling, forecasting, designing and policy making, can have a slow burning effect. The actual unsafe act that commits or triggers an accident can be traced back through the organisation and the subsequent failures will be exposed, and discover the accumulation of latent failures within the system as a whole that led to the incident/accident becoming more likely and ultimately happening.

## Components of Incident Management

The components of incident management are prevention, detection, investigation and reporting-corrective and preventive action.

### Prevention

As the popular saying goes “prevention is better than cure”. The same principle apply to the incident management process. All efforts should be made to make sure that an incident does not take place by following all the Standard operating procedures (SOPs) diligently. One of the key elements in the incident prevention is creating awareness by conducting training and development programmes.

### Detection

Detection is the act of detecting actions or events that attempt to compromise the security, safety, confidentiality, integrity or availability of a resource. For example, detection of a bomb or bomb like object, detection of a breached wall in the perimeter. Incident detection can be done in two ways; direct observation or technological aids. Direct observations are physical inspections or checks carried out, for example, while patrolling checking for a broken lock or a damaged window. Technological aids are devices used to ward off or detect an incident, for example, use of a fire detector, infra-red ray based intrusion alarm, perimeter sensor, and motion detecting cameras.

### Investigation

Investigation is a process of carrying out systematic scrutiny, checking and analysing to ascertain the cause and effect of a breach of security/safety. It also scrutinises, checks and analyses the defaulter.

The steps or process flow for investigations would generally be the following:

1. **Receipt of Complaint/Incident:** It may be verbal, written, through telephone or electronic mail.

2. **Assessment of Complaint/Incident:** To ascertain whether complaint is of minor or serious nature.

3. **Incident Spot Visit:** This is undertaken immediately to avoid loss of time and tampering of evidence.

4. **Incident Spot Study:** This requires action by specialised persons to understand the physical conditions, the environmental conditions, the evidences, gathering of information through interrogation/questioning and relating these facts to the incident.

5. **Collection of Evidence:** All types of evidences, for example, photographs, documents, any item/weapon, witnesses and circumstantial evidence needs to be collected, collated and interpreted to arrive at least for solving the case.

6. **Examination of Witnesses:** Eye witnesses and others will be thoroughly examined to corroborate evidence.

7. **Analysis:** Investigation analysis will be drawn out based on complaint, evidence and statement of witnesses to arrive at the final cause and effect by which accountability could be fixed.

8. **Conclusion and Reporting:** The incident will be reported giving details as analysed.

## Incident Reporting

Incident report is a written document describing inadvertent situation, errors or omissions or untoward events happening to people, equipment or the process. Such a report should be filed, soon after the event. However, in some cases it may not be possible.

In security and safety operations, the generally accepted practice is to give the first informal message orally or written followed by a formal detailed report within 24 to 48 hours of the incident.

Incident report comprises of information on affected staff, customers, data, process and property. The report must be authenticated by an authorized person like the head of the department or supervisor. At times some of the security incident reports are confidential and should be handled according to the policy and procedure of the organisation.

## Corrective and Preventive Action

Corrective action is an action initiated to arrest the problem or incident immediately and on the spot, whereas preventive action is an action taken to ensure that such problem or incident does not occur again.

## Incident Reporting Format

It may be noted that different organization follow different formats for incident reporting, however, the generally accepted format is given in table 1.

## Table 1: Security Incident Reporting Format

| | | | |
|---|---|---|---|
| Incident Report | | | |
| Department Affected | | Incident Date | |
| Location | | Incident Time | |
| Incident Description | | | |
| Incident Reported by | | | |
| Employee Name | | Department | |
| Designation | | Signature | |
| | | | |
| Incident Management | | | |
| Incident Registration Number | | | |
| Incident Category | Security Incident | Safety Incident | |
| Incident Analysis | | | |
| Corrective Action | | | |
| Preventive Action | | | |
| Incident Reported by | | | |
| Employee Name | | Department | |
| Designation | | Signature | |

## Responsibility of Security Personnel in the Investigation Process

Security personnel have important role and responsibilities in the investigation process. Since security personnel get involved with the incident, their contributions towards information gathering, collection and protection of evidence, incident reporting and examining witnesses becomes extremely vital. The following are some of the points:

- Prepare Detailed Incident Report
- Collect and Preserve Evidence Relating to the Case
- Prepare Detailed Examination Report of Witnesses
- Maintain Contact Details of Witnesses
- Prepare Detailed Log Report on Incident
- Identify and Record Contact Details of Eyewitnesses, if Any
- Give Updates to the Investigating Authority
- Assist Investigating Authorities as and When Required.

## Incident Manager

Incident Manager is a person who manages the incident. The Incident Manager is a functional role and not a position. He/she is a focal point for leadership and plays a key role during an incident/event by ensuring adherence to follow-up on commitments and adequate information flow.

## Exercise

### Assignment

Suppose you are an employee of the XYZ Bank and you have been asked by your Branch Manager to prepare an incident report based on a given narration. Prepare the incident report in the format:

---

### Impostor Tricks People after seeking ATM Card Details on Phone

An impostor posing as a Bank Manager has called people and after seeking their personal information about Credit Cards duped them of lakhs of rupees. The accused has been making calls to people posing as manager of the XYZ bank. More than a dozen people have already been duped in the past few days in the capital city by the fraudster forcing the cyber crime sleuths to issue an advisory. After getting the pin details the accused made fraudulent transactions.

In all the incidents, the complainants have received calls and the person who introduced them as bank manager has asked for card details assuring them issue of fresh cards. Later, using the card details, the unidentified accused shopped online, including buying prepaid mobile vouchers or buying credits through different sites and later transferring it into his account.

------------------------------------------------------------------------------------------

## Assessment

### A. Short Answer Questions

1. Explain the term ‘incident’.

------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------

2. List the categories of incident.

------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------

3. List four examples one each of security and safety incident.

------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------

4. List the components of incident management.

-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------

5. List the steps/process of investigation.

-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------

6. List the responsibilities of security personnel in the investigation process.

-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------

## Checklist For Assessment Activity

Use the following checklist to see if you have met all the requirements for assessment activity.

**Part A**

(a) Differentiated between Direct and Indirect Causes of Incidents

(b) Differentiated between Prevention and Detection of Incidents

(c) Differentiated between Corrective and Preventive Action

**Part B**

Discussed in class the following:

(a) What are various categories of incidents?

(b) What are the role and responsibilities of an incident manager?

(c) What are the components of incident management?

(d) What are the steps involved in investigation?

(e) What are the responsibilities of security persons in investigation?

**Part C**

**Performance Standards**

The Performance Standards may include, but not limited to:

| **Performance Standards** | **Yes** | **No** |
|---|---|---|
| Identify the type of incident | | |
| List the steps/process involved in investigation | | |
| Fill the incident reporting form | | |

# Session-2
# Dealing with Bombs and IED Threat

## Relevant Knowledge

Security provides a safe and danger free environment, wherein people can conduct their daily chores and businesses. However, there is no concept of an ideal security. Security set up of any organization is subject to threat, vulnerability and risks and incidents of various nature, generally termed as security/ safety incidents or breaches. These incidents take place because of various reasons, such as human, technology and equipment errors.

A bomb threat is an effective means of disrupting business. The problems are intensified when the incident involves an actual explosive or incendiary device. Although there is no fool proof means of securing a premises against a bomb threat (or bomb attack), a good security plan correctly executed, will enable a business to deal with an incident properly. Bombs and the threat of their use has become the primary weapon of the terrorist. They are also used as a means of retaliation by employees with real or fancied grievances, as well as by criminal extortionists.

The aim of this unit is to provide learners with the knowledge on general guidelines that can be used in responding to bombing incidents.

## Explosives and Bombs

Explosives are chemical compounds which flare up and burst with a loud sound. It is a material capable of getting rapidly converted into gas under extremely high temperature and pressure, creating an instantaneous chain of events. A bomb is an explosive device which has a casing in which explosives are packed. The explosive device is fused to explode under specific conditions time, pressure, vibration, photosensitivity, remote control, etc., resulting in an extremely sudden and violent release of explosion.

## Detonator

A detonator is a device used to trigger an explosive device/bomb. Detonators can be chemically, mechanically or electrically initiated; the latter two being the most common.

## Categories and Types of Explosives

**Explosives are classified into two categories:** Low Explosive and High Explosives.

**Low Explosives** burns or deflagrates. Low explosives burn very fast, but do not explode. They are generally mixed with high explosives to trigger an explosion. However, at times, a low explosive also explodes.

**High Explosives** detonate or explode. A high explosive bursts and explodes very fast. People use high explosives in mining or destroying old buildings. Military weapons use high explosives. High explosives produce more pressure than low explosives.

**Types of Explosives:** TNT (Tri Nitro Toluene), semtex, nitro-glycerine, ammonium nitrate, gun powder, RDX are some of the explosives used in making bombs.

## IED Triggering Mechanism and Means of Concealing

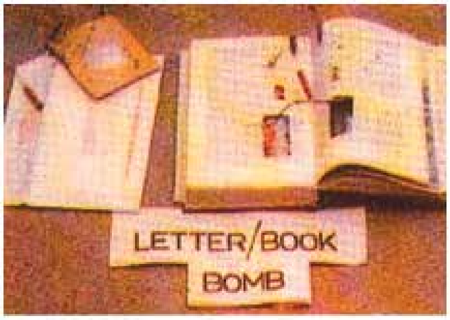
**Improvised Explosive Devices (IED):** It is an explosive device placed or fabricated in an improvised manner. IEDs are ‘home-made’ devices made to injure, maim or kill. They are typically thrown or laid on the sides of roads or on the road itself (unseen by a passing vehicle occupant). IEDs can be set off by a timer, a timed fuse, a cell phone, pressure, tilt, vibration or a remote control. They are designed to destroy, incapacitate, harass or distract.

## IEDs fall into three categories

- Package Type IED
- Vehicle Borne IED
- Suicide Bomb IED

Following are the types of triggering device for IEDs which are commonly used.

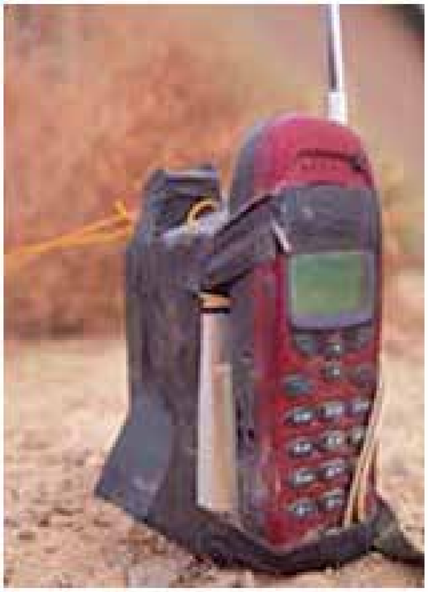
- Time Control
- Light Control
- Speed Control
- Apply Pressure
- Release Pressure
- Anti Open
- Anti Lift
- Anti Roll
- Remote Controlled



There are many ways in which an IED can be concealed. However the most commonly practised means of concealing explosives/IEDs are mentioned hereunder.

- Transistor Bomb
- Pressure Cooker Bomb
- Doll Bomb
- Book Bomb
- Bicycle Bomb

- Human Bomb
- Vehicle Bomb
- Landmine IED
- Vehicle Borne IED
- Book Bomb IED
- Pepsi Can IED
- Mobile IED



## Effect of an Explosion

An explosion causes blast, shattering effect, heat and fire. This leads to injury, death and damage to the property.

## Procedures for Handling a Bomb Threat Call and Discovery of a Suspected Bomb

There are two types of bomb threat calls: Specific and non-specific. In specific threat call, the building, specific department, area and floor is mentioned or identified. The exact date and time is stated. If these specifications are not given, then the threat call is classified as non-specific. These threats cannot be neglected and a search of the building is to be carried out as per procedure. It may be noted that all bomb threat calls, whether hoax or genuine, has to be treated as a genuine call.

## Procedures for Premises Evacuation

Upon confirmation from the authorized person to evacuate the building, an announcement should be made over the public address system ordering the evacuation of people from the premises in an orderly and calm manner. The order/sequence of evacuation will depend on the time available, the type of threat (specific or non-specific) and bomb like object found.

## Exercise

**Case Study**

A powerful bomb exploded on Thursday near the office of a political party in the city, injuring at least 16 people, police said. The bomb was planted in a motorcycle parked about 20 yards from the office of the political party, as informed by the Director General of Police. The injured were being treated at nearby hospitals, where doctors said the condition of five people was serious. The blast was so powerful that nearby buildings shook and window panes were shattered. Three cars and several scooters were charred in the blaze that followed the blast. A police bus parked nearby was also badly damaged. On reaching the scene, the Police immediately cordoned off the area by placing the yellow tape around the scene and forensic experts gathered the evidence from the blast site. Sniffer dogs and bomb experts were deployed to collect the evidence from the scene. Investigations so far have confirmed that the explosive used to trigger the blast was an improvised explosive device (IED) in the form of a pipe (pipe bomb). Forensic experts found lithium and alkaline residues scattered around the site, an indication that the bomb was an Improvised Explosive Device (IED) in the form of a pipe bomb. The bomb was possibly attached to a motorbike to make it look like a component of the bike. The explosive material used was ammonium nitrate.

**Answer the following questions based on the above case study**

(i) Where was the bomb planted?

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

(ii) What is the action that the police took immediately to prevent from gathering at the scene?

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

(iii) Which device was used for explosion?

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

(iv) Which explosive material was used for the bomb?

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

## Assessment

1. Explain explosives and bombs.

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

2. Define a detonator.

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

3. List categories of explosives.

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

4. List types of explosives

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

5. Explain IED? Describe categories of IED.

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------------

6. List the types triggering device generally used for an IED.

---------------------------------------------------------------------------------------------

---------------------------------------------------------------------------------------------

---------------------------------------------------------------------------------------------

7. Describe the effects of an explosion.

---------------------------------------------------------------------------------------------

---------------------------------------------------------------------------------------------

---------------------------------------------------------------------------------------------

## Checklist For Assessment Activity

Use the following checklist to see if you have met all the requirements for assessment activity.

**Part A**

(a) Differentiate between Explosive and Detonator

(b) Differentiate between High Explosives and Low Explosives

(c) Differentiate between Different types of IEDs

**Part B**

Discussed in class the following:

(a) What are the different types of IEDs?

(b) How to deal with bomb/IED threats?

(c) What are the precautions to be taken during bomb threat evacuations?

**Part C**

**Performance Standards**

The Performance Standards may include, but not limited to:

| **Performance Standards** | **Yes** | **No** |
|---|---|---|
| Demonstrate the knowledge of the steps to be taken for dealing with bomb threat? | | |