- **Attorney:** Since computer forensics directly deal with investigation and to submit the case in the court, an attorney should be a part of this team.

First Responder (Incident Handlers)

The first responder and the function of the first responder are crucial for computer forensics and investigation. The first responder is the first person notified, and act to the security incident. The first responder toolkit will be discussed in the upcoming chapters, but at this stage, I will discuss the roles and responsibilities of the first responder.

The first responder is a role that could be assigned to anyone, including IT security engineers, network administrator and others. The person who is responsible to act as a first responder should have knowledge, skills and the toolkit of first responders.

The first responder should be ready to handle any situation and his/her action should be planned and well documented. Some core responsibilities are as follows:

- Figure out or understand the situation, event and problem.
- Gather and collect the information from the crime scene
- Discuss the collected information with the other team members
- Document each and everything

First responder or incident handlers should have the first-hand experience of Information security, different operating systems and their architectures.

1.11 Forensics Readiness

There are several reasons for this field 's growth; the most significant being that computers are everywhere. You'd be hard-pressed to find a household today without at least one computer. And it is not just computers that computer forensic examiners get involved with. Computer forensic examiners analyze all types of technical devices like cell phones, iPods, Tablets, PDAs, and text messaging. Computer forensic examiners analyze all of these electronic devices! Cyber forensics is a rapidly changing field. There are new technologies coming out daily that are becoming smaller, but storing more and more data. This leads to why cyber forensics is import. In computer- related crimes, such as identity fraud, it is becoming easier to hide data. With the proper analysis of digital evidence, better security can be made to protect computer users, but also catch those who are committing the crimes. Organizations have now realized the importance of being prepared to fight cybercriminals with their forensic readiness plan ready.

1.11.1 What is Forensics Readiness?

Forensic readiness is the ability of an organization to maximize its potential to use digital evidence whereas minimizing the costs of an investigation. Digital evidence can be in the form of log files, emails, back-up disks, portable computers, network traffic records, and telephone records etc.

CESG Good Practice Guide No. 18, *Forensic Readiness*, defines forensic readiness as: "The achievement of an appropriate level of capability by an organization in order for it to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or court of law.

Modern digital technologies not only present new opportunities to business organizations but also a different set of issues and challenges that need to be resolved. With the rising threats of cybercrimes, many organizations, as well as law enforcement agencies globally, are now establishing proactive measures as a way to increase their ability to respond to security

incidents as well as create a digital forensic ready environment.

Forensic readiness as defined by Mohay (2005) as the extent to which computer systems or computer networks record activities and data in such a manner that the records are sufficient in their extent for subsequent forensic purposes, and the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations.

1.11.2 Goals of Forensic Readiness

Some of the important goals of forensics readiness are:

- to gather admissible evidence legally and without interfering with business processes;
- to gather evidence targeting the potential crimes and disputes that may adversely impact an organisation;
- to allow an investigation to proceed at a cost in proportion to the incident;
- to minimise interruption to the business from any investigation; and
- to ensure that evidence makes a positive impact on the outcome of any legal action.

1.11.3 Benefits of Forensic Readiness

Forensic readiness can offer an organisation the following benefits:

- evidence can be gathered to act in an organisation's defence if subject to a lawsuit;
- comprehensive evidence gathering can be used as a deterrent to the insider threat (throwing away potential evidence is simply helping to cover the tracks of a cybercriminal);
- in the event of a major incident, an efficient and rapid investigation can be conducted and actions taken with minimal disruption to the business;
- a systematic approach to evidence storage can significantly reduce the costs and time of an internal investigation;
- a structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g. in response to a request under data protection legislation);
- forensic readiness can extend the scope of information security to the wider threat from cybercrime, such as intellectual property protection, fraud, extortion etc;
- it demonstrates due diligence and good corporate governance of the company's information assets;
- it can demonstrate that regulatory requirements have been met;
- it can improve and facilitate the interface to law enforcement if involved;
- it can improve the prospects for a successful legal action;
- it can provide evidence to resolve a commercial dispute; and
- it can support employee sanctions based on digital evidence (for example to prove a violation of acceptable use policy)

1.11.4 Steps for Forensic Readiness Planning

The following ten steps describe the key activities in forensic readiness planning:

1. Define the business scenarios that require digital evidence;
2. Identify available sources and different types of potential evidence;
3. Determine the evidence collection requirement;
4. Establish a capability for securely gathering legally admissible evidence to meet the