UNIT -V: Cybercrimes and Cyber security:

1. Why Do We Need Cyber laws: The Indian Context.
2. The Indian IT Act.
3. Challenges to Indian Law and Cybercrime Scenario in India.
4. Consequences of Not Addressing the Weakness in Information Technology Act.
5. Digital Signatures and the Indian IT Act.
6. Information Security Planning and Governance.
7. Information Security Policy Standards and Practices.
8. The information Security Blueprint.
9. Security education, Training and awareness program.
10. Continuing Strategies.

RGAN-CSE

1. Cybercrime and Cyber security: Why Do We Need Cyberlaws: The Indian Context

- Cyberlaw is a framework created to give legal recognition to all risks arising out of the usage of computers and computer networks.
- Under the preview of cyberlaw, there are several aspects, such as, *intellectual property*, *data protection and privacy*, *freedom of expression* and *crimes committed using computers*.
- The Indian Parliament passed its first cyberlaw, the ITA 2000, aimed at providing the legal infrastructure for E-Commerce in India.
- ITA 2000 received the assent of the President of India and it has now become the law of the land in India.
- The Government of India felt the need to enact relevant cyberlaws to regulate Internet-based computer related transactions in India.
- It manages all aspects, issues, legal consequences and conflict in the world of cyberspace, Internet or WWW.
- In the Preamble to the Indian ITA 2000, it is mentioned that it is an act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as *electronic commerce*.
- The reasons for enactment of cyberlaws in India are summarized below:

1. Although India possesses a very well-defined legal system, covering all possible situations and cases that have occurred or might take place in future, the country lacks in many aspects when it comes to newly developed Internet technology. It is essential to address this gap through a suitable law given the increasing use of Internet and other computer technologies in India.

2. There is a need to have some legal recognition to the Internet as it is one of the most dominating sources of carrying out business in today's world.

3. With the growth of the Internet, a new concept called *cyberterrorism* came into existence.

- Cyberterrorism includes the use of disruptive activities with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives in the world of cyberspace. It actually is about committing an old off ense but in an innovative way.
- Keeping all these factors into consideration, Indian Parliament passed the Information Technology Bill on 17 May 2000, known as the ITA 2000.
- It talks about cyberlaws and forms the legal framework for electronic records and other activities done by electronic means.

RGAN.CSE

www.Jntufastupdates.com

2. The Indian IT Act

- As mentioned above, this Act was published in the year 2000 with the purpose of providing legal recognition for transactions carried out by means of electronic data interchange, commonly referred to as *electronic commerce*.
- Electronic communications involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies.
- Another purpose of the Indian IT Act was to amend the Indian Penal Code (IPC), the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891, the Reserve Bank of India Act 1934 and matters connected therewith or incidental thereto.
- The Reserve Bank of India Act has got Section 58B about Penalties. Subsequently, the Indian IT Act underwent some important changes to accommodate the current cybercrime scenario; a summary of those changes is presented in Table 6.7 – note specially the changes to Section 66 and the corresponding punishments for cyber offenses.
- The scope and coverage of the Indian IT Act is briefly described in Section 27.4, Ref. #6, Books, Further Reading.
- The structure of the Indian ITA 2000 is provided in Table 6.6 for readers' immediate reference.
- The sections mentioned in bold italics are relevant in the discussion of cybercrime and information security.

ITA Sections are as follows:

1. Section 65: Tampering with computer source documents
2. Section 66: Computer-related offences
3. Section 67: Punishment for publishing or transmitting obscene material in electronic form
4. Section 71: Penalty for misrepresentation
5. Section 72: Penalty for breach of confidentiality and privacy
6. Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars
7. Section 74: Publication for fraudulent purpose

Positive Aspects of the ITA 2000

- The Indian ITA 2000, though heavily criticized for not being specific on cybercrimes, in our opinion, does have a few good points.
  1. Prior to the enactment of the ITA 2000 even an E-Mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the ITA 2000 changed this scenario by legal recognition of the electronic format. Indeed, the ITA 2000 is a step forward.
  2. From the perspective of the corporate sector, companies are able to carry out E-Commerce using the legal infrastructure provided by the ITA 2000. Till the coming into effect of the Indian cyberlaw, the growth of E-Commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.
  3. Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the ITA 2000.
  4. In today's scenario, information is stored by the companies on their respective computer system, apart from maintaining a backup. Under the ITA 2000, it became possible for corporate to have a statutory remedy if anyone breaks into their computer

www.Jntufastupdates.com

RGAN-CSE

systems or networks and causes damages or copies data. The remedy provided by the ITA 2000 is in the form of monetary damages, by the way of compensation, not exceeding ` 10,000,000.

5. ITA 2000 defined various cybercrimes. Prior to the coming into effect of the Indian Cyberlaw, the corporate were helpless as there was no legal redress for such issues. However, with the ITA 2000 instituted, the scenario changed altogether.

Weak Areas of the ITA 2000

As mentioned before, there are limitations too in the IT Act; those are mainly due to the following gray areas:

1. The ITA 2000 is likely to cause a conflict of jurisdiction.

2. E-Commerce is based on the system of domain names. The ITA 2000 does not even touch the issues relating to domain names.

3. The ITA 2000 does not deal with issues concerning the protection of Intellectual Property Rights (IPR)

4. As the cyberlaw is evolving, so are the new forms and manifestations of cybercrimes. The offenses defined in the ITA 2000 are by no means exhaustive.

5. The ITA 2000 has not tackled issues related to E-Commerce like privacy and content regulations.

RGAN-CSE

www.Jntufastupdates.com

3. Challenges to Indian Law and Cybercrime Scenario in India

- The offenses covered under the Indian ITA 2000 include:

1. Tampering with the computer source code or computer source documents;
2. un-authorized access to computer ("hacking" is one such type of act);
3. publishing, transmitting or causing to be published any information in the electronic form which is lascivious or which appeals to the prurient interest;
4. failure to decrypt information if the same is necessary in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign state, public order or for preventing incitement to the commission of any cognizable off ense;
5. securing access or attempting to secure access to a protected system;
6. misrepresentation while obtaining, any license to act as a Certifying Authority (CA) or a digital signature certificate;
7. breach of confidentiality and privacy;
8. publication of digital signature certificates which are false in certain particulars;
9. publication of digital signature certificates for fraudulent purposes.

- There are legal drawbacks with regard to cybercrimes addressed in India – there is a need to improve the legal scenario.
- These drawbacks prevent cybercrimes from being addressed in India.
- **First**, the difficulties/ drawbacks with most Indians not to report cybercrimes to the law enforcement agencies because they fear it might invite a lot of harassment.
- **Second**, their awareness on cybercrime is relatively on the lower side.
- Another factor that contributes to the difficulty of cybercrime resolution is that the law enforcement agencies in the country are neither well equipped nor knowledgeable enough about cybercrime.
- There is a tremendous need for training the law enforcement agencies in India. Not all cities have cybercrime cells.
- Most investigating officers with the Police force may be well equipped to fight cybercrime We need dedicated, continuous and updated training of the law enforcement agencies.

4. Consequences of Not Addressing the Weakness in Information Technology Act

- In light of the discussion so far, we can see that there are many challenges in the Indian scenario for fight with cybercrime.
- Cyberlaws of the country are yet to reach the level of sufficiency and adequate security to serve as a strong platform to support India's E-Commerce industry for which they were meant. India has lagged behind in keeping pace with the world in this regard.
- The consequences of this are visible – India's outsourcing sector may get impacted.
- There are many news about overseas customer worrying about data breaches and data leakages in India.
- This can result in breaking India's IT business leadership in international outsourcing market.
- Outsourcing is on the rise; if India wishes to maintain its strong position in the global outsourcing market, there should be quick and intelligent steps taken to address the current weaknesses in the Information Technology Act.
- If this is not addressed in the near future, then the dream of India ruling the world's outsourcing market may not come true.

www.Jntufastupdates.com

RGAN-CSE

5. Digital Signatures and the Indian IT Act

- A few technical concepts regarding Digital Signature.

5.1. Public-Key Certificate

- A public-key certificate is a digitally signed statement from one entity, saying that the public key of another entity has some specific value.
- A digital signature is a type of electronic signature that is used to guarantee the integrity of the data.
- When linked to the identity of the signer – using a security token such as X.509 Certificates – Which is a digital signature.
- An X.509 Certificate contains information about the certificate subject and the certificate issuer (the CA that issued the certificate).
- The role of a certificate is to associate an identity with a public-key value.
- A certificate includes:

1. X.509 version information;
2. a **serial number** that uniquely identifies the certificate;
3. a **common name** that identifies the subject;
4. the **public key** associated with the common name;
5. the **name of the user** who created the certificate, known as the subject name;
6. information about the **certificate issuer**;
7. signature of the issuer;
8. information about the **algorithm** used to sign the certificate;
9. some optional **X.509 version 3 extensions**.

5.2. Representation of Digital Signatures in the ITA 2000

- ITA 2000 had prescribed digital signatures based on Asymmetric cryptosystem and Hash system as the only acceptable form of authentication of electronic documents recognized as equivalent to “signatures” in paper form.
- When the ITA 2000 was drafted, there was a slip-up in the drafting of Section 35, subsection (3), which made it mandatory for an applicant of a digital signature certificate to enclose a *Certification Practice Statement* along with his application.
- One of the major deficiencies in the bill, which could hinder implementation, is the provisions regarding the role and function of the CAs as well as the process of issuing digital certificates.

5.3. Impact of Oversights in ITA 2000 Regarding Digital Signatures

- The Ministry of Information and Technology had to urgently establish a task force to assist them in the drafting of the rules.
- The task force consisted of experts in the field.
- It is said that now this blunder has been accompanied by more avoidable confusions.
- The Information Technology Amendment Bill 2006 was drafted on the basis of the recommendations of an “Expert Committee.”
- The Committee took into consideration a recommendation from technical community that
    - (a) the PKI-based system made the law dependent on a single authentication technology and
    - (b) there was a need to make the law *Technology Neutral*

www.Jntufastupdates.com

6. Information Security Planning and Governance

- Strategic planning sets the long-term direction to be taken by the organization and each of its component parts.
- Strategic planning should guide organizational efforts and focus resources toward specific, clearly defined goals.
- After an organization develops a general strategy, it generates an overall strategic plan by extending that general strategy into plans for major divisions.
- Each level of each division then translates those plan objectives into more specific objectives for the level below.
- To execute this broad strategy, the executive team must first define individual responsibilities.
- The executive team is sometimes called the organization's C-level, as in CEO, COO, CFO, CIO, and so on.

Planning Levels

a. **Operational plan:** The documented product of operational planning; a plan for the organization's intended operational efforts on a day-to-day basis for the next several months.

b. **Operational planning**: The actions taken by management to specify the short-term goals and objectives of the organization in order to obtain specified tactical goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.

c. **Tactical plan:** The documented product of tactical planning; a plan for the organization's intended tactical efforts over the next few years.

d. **Tactical planning**: The actions taken by management to specify the intermediate goals and objectives of the organization in order to obtain specified strategic goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.

Information Security Governance

a. **Corporate Governance**: Executive management's responsibility to provide strategic direction, ensure the accomplishment of objectives, oversee that risks are appropriately managed, and validate responsible resource use.

b. **Governance:** "The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."

c. **Information security governance:** The application of the principles of corporate governance to the information security function.

According to the Information Technology Governance Institute (ITGI), information security governance includes all of the accountabilities and methods undertaken by the board of directors and executive management to provide:

- Strategic direction
- Establishment of objectives
- Measurement of progress toward those objectives
- Verification that risk management practices are appropriate
- Validation that the organization's assets are used properly

www.Jntufastupdates.com

RGAN-CSE

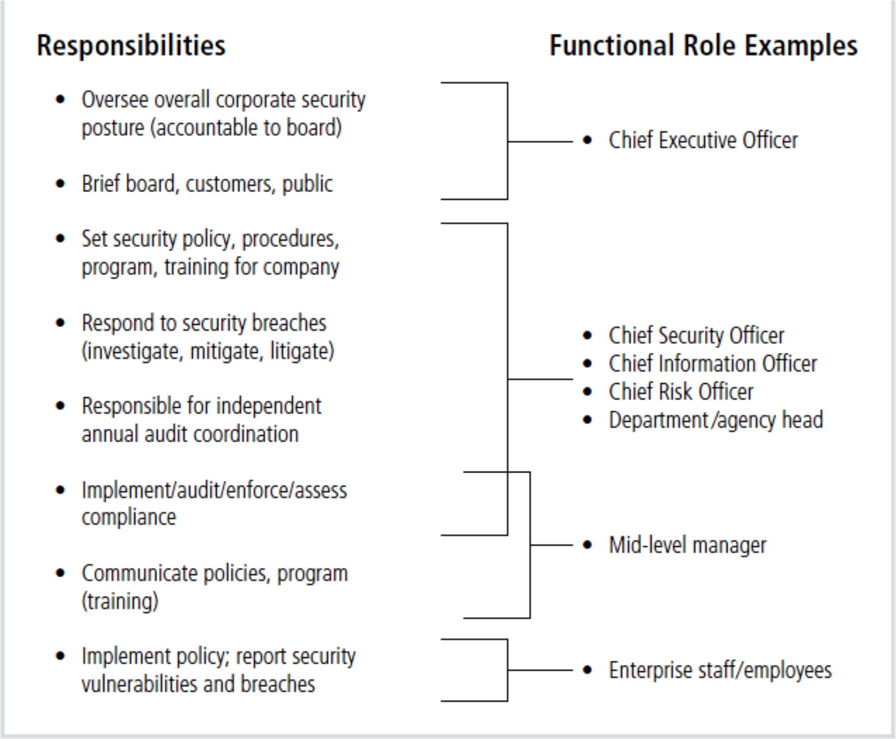

Responsibilities
Functional Role Examples
Oversee overall corporate security posture (accountable to board)
Brief board, customers, public
Chief Executive Officer
Set security policy, procedures, program, training for company
Respond to security breaches (investigate, mitigate, litigate)
Responsible for independent annual audit coordination
Chief Security Officer
Chief Information Officer
Chief Risk Officer
Department /agency head
Implement/audit/enforce/assess compliance
Communicate policies, program (training)
Mid-level manager
Implement policy; report security vulnerabilities and breaches
Enterprise staff/employees

Figure 4-1 Information security governance roles and responsibilities

RGAN

7. Information Security Policy, Standards, and Practices

- Management from all communities of interest, including general staff, information technology, and information security, must make policies the basis for all information security planning, design, and deployment.
- Policies direct how issues should be addressed and how technologies should be used.
- Policies do not specify the proper operation of equipment or software—this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation.
- In addition, policy should never contradict law;
- policy must be able to stand up in court, if challenged; and policy must be properly administered through documented acceptance. Otherwise, an organization leaves itself..

Policy as the Foundation for Planning

a. **de facto standard :** A standard that has been widely adopted or accepted by a public group rather than a formal standards organization. Contrast with a de jure standard.
b. **de jure standard** : A standard that has been formally evaluated, approved, and ratified by a formal standards organization. Contrast with a de facto standard.
c. **Guidelines**: Within the context of information security, a set of recommended actions to assist an organizational stakeholder in complying with policy.
d. **Information security policy:** A set of rules that protects an organization's information assets.
e. **Policy**: A set of principles or courses of action from an organization's senior management intended to guide decisions, actions, and duties of constituents.
f. **Practices**: Within the context of information security, exemplary actions that an organization identifies as ideal and seeks to emulate. These actions are typically employed by other organizations.

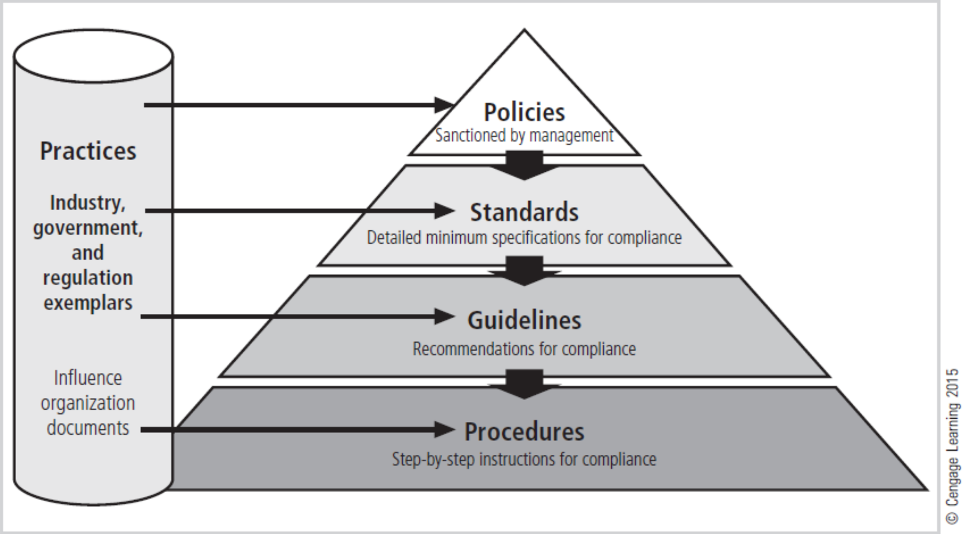

Practices
Industry, government, and regulation exemplars
Influence organization documents
Policies
Sanctioned by management
Standards
Detailed minimum specifications for compliance
Guidelines
Recommendations for compliance
Procedures
Step-by-step instructions for compliance
© Cengage Learning 2015

Figure 4-2 Policies, standards, guidelines, and procedures

Enterprise Information Security Policy

- Enterprise information security policy (EISP) is high-level security policy that is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts.

www.Jntufastupdates.com

- An enterprise information security policy (EISP) is also known as a general security policy, organizational security policy, IT security policy, or information security policy.
- The EISP is an executive-level document, usually drafted by or in cooperation with the organization's chief information officer.
- This policy is usually 2 to 10 pages long and shapes the philosophy of security in the IT environment.
- The EISP usually needs to be modified only when there is a change in the strategic direction of the organization.

Issue-Specific Security Policy

- Issue-specific security policy (ISSP) is Commonly referred to as a fair and responsible use policy;
- A policy designed to control constituents' use of a particular resource, asset, or activity, and provided to support the organization's goals and objectives.
- As an organization supports routine operations by executing various technologies and processes, it must instruct employees on their proper use.
- In general, the issue-specific security Statement of Purpose Answers the question "What is this policy for?" Provides a framework that helps the reader understand the intent of the document. "This document will:

- Identify the elements of a good security policy
- Explain the need for information security
- Specify the various categories of information security
- Identify the information security responsibilities and roles
- Identify appropriate levels of security through standards and guidelines

RGAN-CSE

8. The Information Security Blueprint

a. **Information security blueprint:** The basis for all security program elements; a scalable, upgradeable, comprehensive plan to meet the organization's current and future information security needs.

b. **Information security framework**: An outline or structure of the organization's overall information security strategy that is used as a road map for planned changes to its information security environment; often developed as an adaptation or adoption of a popular methodology,like NIST's security approach or the ISO 27000 series.

c. **Information security model**: An established information security framework, often popular among other organizations and backed by a recognized security agency, with exemplar details an organization may want to emulate in creating its own framework and blueprint.

- Once an organization has developed its information security policies and standards, the information security community can begin developing the blueprint for the information security program.
- If any policies, standards, or practices have not been completed, management must determine whether to proceed nonetheless with the development of the blueprint.
- After the information security team has inventoried the organization's information assets and then assessed and prioritized threats to those assets, it must conduct a series of risk assessments.
- These assessments, which include determining each asset's current protection level.
- This information security blueprint is the basis for the design, selection, and implementation of all security program elements.
- The security blueprint builds on top of the organization's information security policies.
- It is a detailed version of the information security framework.
- The blueprint specifies tasks and the order in which they are to be accomplished, just as an architect's blueprint serves as the design template for the construction of a building.

The ISO 27000 Series

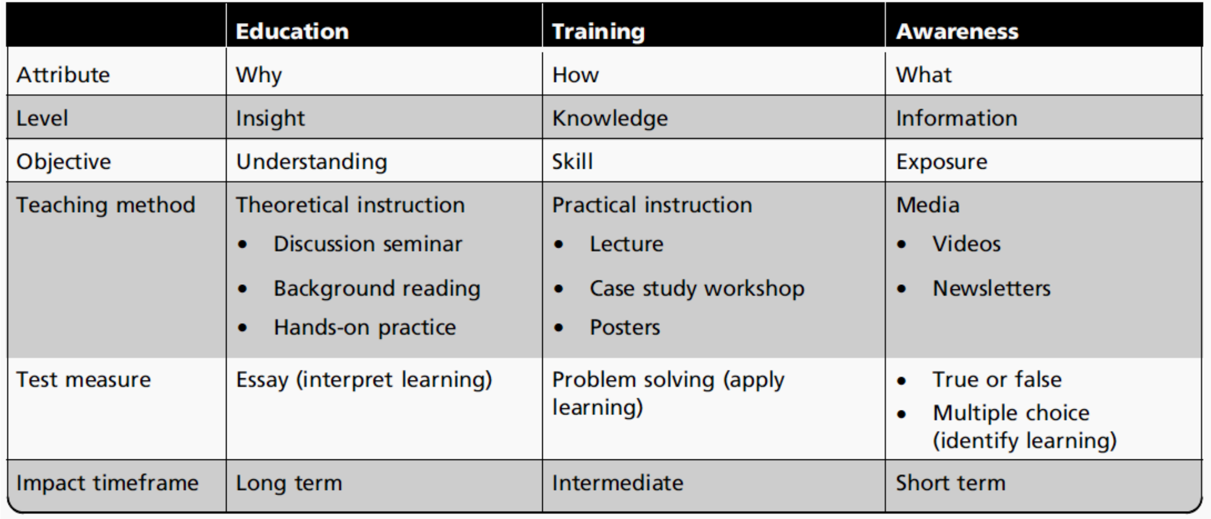
- One of the most widely referenced security models is the Information Technology—Code of Practice for Information Security Management, which was originally published as British Standard BS7799.
- In 2000, this code of practice was adopted as ISO/IEC 17799, an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- The document was revised in 2005 to become ISO 17799:2005

www.Jntufastupdates.com

RGAN-CSE

9. Security Education, Training, and Awareness Program

- Security Education, Training, and Awareness (SETA) is a managerial program designed to improve the security of information by providing targeted knowledge, skills, and guidance for organizations.
- Once your organization has defined the policies that will guide its security program by implementing a security education, training, and awareness (SETA) program.
- The SETA program is designed to reduce incidents of accidental security breaches by employees.
- Employee errors are among the top threats to information assets, so it is well worth developing programs to combat this threat.
- SETA programs are designed to supplement the general education and training programs that many organizations use to educate staff about information security.
- For example, if an organization detects that many employees are opening questionable e-mail attachments, those employees must be retrained.
- As a matter of good practice, systems development life cycles must include user training during the implementation phase.
- The SETA program consists of three elements: security education, security training, and security awareness.
- An organization may not be able or willing to undertake all three of these elements, and it may outsource elements to local educational institutions.
- The purpose of SETA is to enhance security by doing the following:
  - Improving awareness of the need to protect system resources
  - Developing skills and knowledge so computer users can perform their jobs more securely
  - Building in-depth knowledge as needed to design, implement, or operate security programs for organizations and system.
- Comparative Framework is as follows:



	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction • Discussion seminar • Background reading • Hands-on practice	Practical instruction • Lecture • Case study workshop • Posters	Media • Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

Table 4-6 Comparative Framework of SETA[26]

10. Continuity Strategies

- A key role for all managers is Contingency Planning (CP).

- Managers in the IT and information security communities are usually called on to provide strategic planning to assure the continuous availability of information systems.
- For managers, the probability that some form of attack will occur—from inside or outside, intentional or accidental, human or nonhuman, annoying or catastrophic—is very high.
- Thus, managers from each community of interest must be ready to act when a successful attack occurs.
- Various types of contingency plans are available to respond to events, including incident response plans, disaster recovery plans, and business continuity plans.
- In some organizations, these might be handled as a single integrated plan.
- In large, complex organizations, each of these plans may cover separate but related planning functions that differ in scope, applicability, and design.
- In a small organization, the security administrator or systems administrator may have one simple plan that consists of a straightforward set of media backup and recovery strategies and service agreements from the company's service providers.
- Plans for incident response, disaster recovery, and business continuity are components of contingency planning, as shown in the following Diagram.

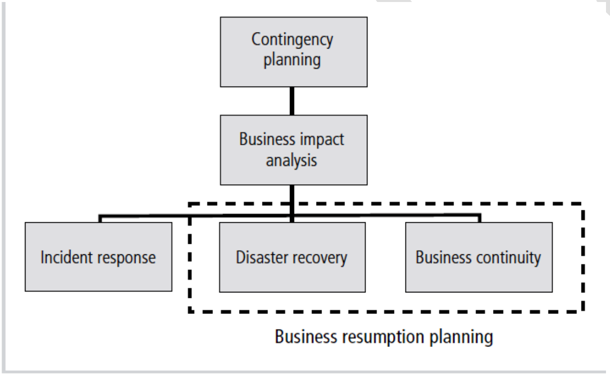


Figure 4-12 Components of contingency planning

- Contingency Planning (CP) includes incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP), in preparation for adverse events that become incidents or disasters.
- The primary functions of these three types of planning are as follows:
  a. **The incident response plan** (IR plan) focuses on immediate response.
  b. **The disaster recovery plan** (DR plan) typically focuses on restoring systems at the original site after disasters occur.
  c. **The business continuity plan** (BC plan) occurs concurrently with the DR plan when the damage is major or ongoing, and requires more than simple restoration of information.

www.Jntufastupdates.com