7 SECURITY ISSUES IN HARDWARE

Chapter Objectives

After reading this chapter, you will understand :

- Safety issues in data storage and downloadable devices
- Physical security of IT assets
- Physical access control
- CCTV and Intrusion Detection System (physical)
- Backup security measures

7.1 INTRODUCTION

Hardware includes :

(1) Hardware in computer, for example, ASICS (chips), FPGA (programmable), Firmware (kind of programmable in low level) and TPM (Trusted Platform Modules).

(2) Hardware which can be carried around, for example, Smart cards, SIM cards, Chip and Pin cards (credit cards/debit cards), Physical Uncloneable Functions (PUFs), Token (RSA), Laptops etc.

The various security issues in hardware are :

[I] Supply Chain Security

If we don't have control of supply chain, we are vulnerable to malware. When we buy a product, it may already contain malware. Thus, the concept of supply chain security is important.

- Memory may be pre-infected with malware.
- It is a big problem in hard drive, digital picture frames, memory sticks, GPS units, etc.
- Even major manufactures have experienced supply chain security problem.
- Recently security breaches have been reported in credit card terminals also.

[II] Trusted Platform Modules (TPMs)

- TPM is a chip in our computer. It is useful to store cryptographic keys.

Scanned by CamScanner

- It gives a chance to enable secure boot.
  - As software stack boots : (BIOS→ bootloader→ OS), (Apps) TPM takes "measurements" of values in registers, etc.
  - After boot, it signs the final state.
  - OS checks this state and traces signature back to Intel. Part of the TPM stores a cryptographic key. This key is signed by the manufacturer and used for signing the final state of the system.
  - Also supports remote "attestation" (checking). If somebody works for a company and access remotely, they will save the final state and while connecting ask to send the final state saved in TPM to check if it is the final secure state we logged in. There is a problem for this approach :
  - ***Privacy concern*** - tracking TPM signing key is unique. Each person have unique TPM and each TPM has unique key. It is possible to keep track of person with the unique key used by TPM.
  - To solve privacy concern, we use Crypto protocol—DAA (Direct Anonymous Attestation). It just proves that the final state is signed with valid key but don't show the value of the key or whose key is it.
  - Also allows storage of keys.
  - ***Full disk encryption*** : TPM gives a chance to stick key in a secure place. If it doesn't stick there, it has to be somewhere. It is shown that if the key goes to RAM to read it, there is a possibility to read by freezing the RAM. Freezing the RAM will make the content to be there for around 10 minutes. Thus, there is enough time to read it.
  - ***Disadvantage of TPMs*** : Does not protect against run-time attacks (Cl, BO, ROP). After secure boot, all the run-time attack may happen. However, malware cannot permanently stay in computer.

[III] Smart Cards

There are two kinds of smart cards :

(1) Active (have power)

(2) Passive (no power): *e.g.,* RFID which are more common. They are powered by the card reader.

There are five attack methods for smart cards :

(1) Recover functionality via Black-box testing

- Guess output based on inputs and check against card
- Reverse-engineering (for week crypto)—break it
- Protection is possible by using known crypto standards

Some smart cards have their secret cryptography algorithm and circuit. To find out the circuit, person may try to guess the circuit and test the input and output of the guessed circuit and the smart card circuit. Therefore, the secret algorithm will be revealed. Here the goal is not to find out the key or content, the goal is recovering the encryption algorithm.

Scanned by CamScanner

Recover functionality via imaging

- Peel off layers of chip chemically.
- Expose circuit, photograph it and train a computer vision algorithm to recognize 2-NAND, 3-NAND, NOT, etc gates.
- Reverse-engineering : If the crypto is weak then attack it.
  - Mitigation can be done by using known crypto standards

(3) Disrupt functionality with selected dropping

- Protocols would fail open. So if there is no response, then it will permit action. So it is easy to disrupt. For example, TV cable/satellite providers; stream all channels. Some card that deny access to certain channels are fail open. These cards are example of active cards.
  - Such attacks can be prevented by never fail open cards.

(4) Recover key

- Cat and mouse: probing
- Slow down the clock cycle, reboot
  - Protection is possible by smaller circuits and tamper protecting them

Suppose we know the crypto algorithm. The key is set in the card and we want to get the value of the key. Flip flops stores the keys. Knowing the circuit does not give us the value of the key, it just says it is stored in these flip flops. Using the small probes and stick it to the flip flops we can examine the voltage to know if it is one or zero. This technique is called "cat and mouse" because designers make small size circuits and then attacker comes up with better probes to stick to that flip flops and then designer tries to make smaller flip flops and it goes back and forth. Now-a-days, this attack is not applicable because circuits are too small to probe. To augment the attack, he can slow down the clock cycle. So, it will get better chance to have reliable measurement because data will not go fast. In addition to slowing down, if the attacker missed a value, he can reboot and have it repeat the values.

(5) Recover key via power analysis :

- Read key value based on power consumption of the device; it needs to know the cryptographic algorithm and the exact time in algorithm that it uses key to encrypt the message.
- It appears that having the shadow circuit in reverse of the crypto circuit will hide the key value. But, because of manufacturing differences, the circuit will not have exactly reverse result. So it is not applicable to use shadow inverse circuit. Another solution is crypto trick. In brief, we can multiply our message by random number. We basically blind it. We sign the blinded value. This crypto trick will resolve the issue.

[IV] Chip and PIN

- Bank cards have a chip that stores the PIN. PIN is saved on the chip on the card and not in the bank. When the PIN is entered in terminal, it is checked on the card. The idea behind the chip and PIN is "what you know and what you have"

Scanned by CamScanner

which means that if our card is stolen, there won't be any problem as the attacker doesn't know the PIN. The attack below shows how the stolen card is used without PIN.

- Chip and PIN protocol is very complex and has hundreds of pages of specification. The attacker uses a computational device that will stay between card and terminal. Attacker enters the stolen card along with the computational device into the terminal. It is asked for PIN. Attacker enters a wrong PIN likene r 0000. Computational device tell the card "PIN is not required" and also send OK for PIN to the terminal. Card is signed the final state appears as "successful". The problem is that it doesn't say what is successful. If the card signs the message that says "it is successful because no PIN is required", terminal can find out the problem. To solve this problem the final state must be more verbal and say "*what is successful.*"

7.2 DATA STORAGE AND DOWNLOADABLE DEVICES

- *Database security* deals with the entire array of protection mechanism pertaining to safeguard the integrity of database content, the owners and the legitimate users. Any willful unauthorized access attempt to database and unauthorized access by malicious codes or users is prevented.
- *Database access control* will check the privilege levels of a user or program to ascertain the information access permission in a database. The information can be specific like record kinds, particular record, data structures, queries or utilizing path to the aforesaid. The controls are put in place by database owners who are in charge of dedicated DBMS security interfaces.
- *Data security* deals with protection of particular data from physical corruption, alteration or damage. An audit will confirm that any kind of security breach has not taken place and the kind of measures to be implemented if data trails reveal unauthorized intrusion to the system.

Data Storage

We have already discussed the various issues regarding data storage in chapter 3. Here we discuss the issues related to physical conditions that should be provided for storing data. The aspects of physical security are discussed in next article.

Areas and rooms designated for storage of digital or non-digital data should be suitable for the purpose for which they are being used. Data should be well-organised, clearly labelled, easily located and physically accessible. The storage rooms should be structurally sound and free from the risk of flood and as far as possible from the risk of fire.The conditions under which data are stored significantly affect their longevity.

Optical media are vulnerable to poor handling, changes in temperature, changes in relative humidity, air quality and lighting conditions. Magnetic media, like hard drives, are equally sensitive to their physical environment. A personal computer is more likely to suffer from a fatal crash in a very hot office than in a temperature-controlled environment.

Printed materials and photographs are subject to degradation from sunlight and

Scanned by CamScanner

id, e.g. from sweat on skin. High quality media should be used for preparing paper-based materials for storage, or for copies of originals. Examples are using acid-free paper, folders and boxes and non-rust paperclips rather than staples.

Data Storage and Downloadable Devices

We commonly come across various data storage devices like compact disks, DVDs, memory cards, pen-drives, flash drives etc. These devices are used to store information by downloading the data. They can then be removed from the system. These devices are small in size and easy to hide. Also, these devices are vulnerable to theft and destruction. These can also be used by attacker to download data and be the medium of stolen data transfer. Specific security measures have to be put in place to prevent information being damaged, stolen or corrupted by internal and external threats to such devices.

The main threat in storage devices is that being small in size, they can be easily hidden after theft. Also, the original device can be destroyed, thereby resulting in loss of crucial data. An unauthorized person can also alter or delete the data so that it is no longer available to authenticated users. There is also a possibility that an intrudes may introduce certain kind of malware to breach the security measures.

While planning for the physical security, all these issues have to be taken care of by specific protection measures. The most important aspect in these measures is people's awareness through education and training. When people are aware about the security issues involved in these devices, the security of the system is strengthened. The help of advanced surveillance and monitoring technology can also be utilized for the security of these devices.

7.3 PHYSICAL SECURITY OF IT ASSETS

Physical security describes both measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media, and guidance on how to design structures to resist various hostile acts. It can be as simple as a locked door or as elaborate as multiple layers of armed security guards and guardhouse placement. Hence, it is different from information security where the issues are about unauthorized access through a port, modem or wireless access point.

Physical security deals with hardware as a physical asset and with the protection of these physical assets from harm or theft. The traditional tools of physical security such as locks and keys are applied which, restrict access to and interaction with the hardware components of an information system. Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible. If the system itself is not physically secure, nothing else about the system can be considered secure. With physical access to a machine, an intruder can halt the machine, bring it back up in privileged mode, replace or alter the disk, plant Trojan Horse programs, or take any number of other undesirable actions.

Scanned by CamScanner

7.3-1 LAYERED PHYSICAL SECURITY

[I] Site and Facility (Environmental) Design

The initial layer of physical security for a building, office, campus or a physical space uses the principle of "*crime prevention through environmental design.*" The aim is to make it difficult for a criminal to hide, gain access or escape. It is done by unobstructed areas, creative lighting and functional landscaping.

Three basic strategies are employed :

(1) ***Natural access control*** : It is done by :

- Restricting movement
- Differentiating between public, semi-private and private areas
- Target hardening through
  - Window and door locks
  - Alarms
  - Photo ID requirements
  - Sign in/sign out procedures

(2) ***Natural surveillance*** : Make intruder activity more observable and easily detectable by :

- Windows overlooking streets and parking areas.
- Landscaping to eliminate hidden areas.
- Open railings on stairs.
- Numerous low-intensity lighting fixtures to eliminate shadows and reduce blind spots.

(3) ***Territorial reinforcement*** : This is done by creating a sense of pride and ownership among employees and people involved.

- Regular and timely maintenance : pick up trash, fix broken bulbs, etc.
- Assigning responsibility to individuals
- Adding amenities like benches, water fountains etc.

[II] Personnel Identification

ID cards and badges aid in identifying people as known versus unknown people. ID cards are frequently used alongwith electronic access control systems. ID card is typically concealed whereas the ID badge is visible.

ID cards utilize biometrics (facial recognition, finger prints etc). However, they should not be the only control as they can be easily duplicated, stolen or modified. When unauthorized individuals follow authorized users through the control, it is called *gatecrashing* or *tailgating*

[III] Mechanical, Electronic and Procedural Access Control

The next layer is *mechanical* and includes gates, doors, and locks. Key control of the locks becomes a problem with large user populations and any user turnover. Keys quickly become unmanageable forcing the adoption of electronic access control.

Scanned by CamScanner

Electronic access control easily manages large user populations, controlling for user lifecycles times, dates, and individual access points. For example a user's access rights could allow access from 0900 to 1700 Monday through Friday and expires in 90 days.

Another form of access control (*procedural*) includes the use of policies, processes and procedures to manage the ingress into the restricted area. An example of this is the deployment of security personnel conducting checks for authorized entry at predetermined points of entry. This form of access control is usually supplemented by the earlier forms of access control (*i.e.*, mechanical and electronic access control), or simple devices such as physical passes.

An additional sub-layer of mechanical/electronic access control protection is reached by integrating a *key management system* to manage the possession and usage of mechanical keys to locks or property within a building or campus.

[IV] Video Monitoring

The fourth layer is *video monitoring* systems. Security cameras can be a deterrent in many cases, but their real power comes from incident verification and historical analysis. For example, if alarms are being generated and there is a camera in place, the camera could be viewed to verify the alarms. In instances when an attack has already occurred and a camera is in place at the point of attack, the recorded video can be reviewed. Although the term closed-circuit television (CCTV) is common, it is quickly becoming outdated as more video systems lose the closed circuit for signal transmission and are instead transmitting on computer networks. Advances in information technology are transforming video monitoring into video analysis. For instance, once an image is digitized it can become data that sophisticated algorithms can act upon. As the speed and accuracy of automated analysis increases, the video system could move from a monitoring system to an intrusion detection system or access control system. It is now possible to imagine a video camera inputting data to a processor that outputs to a door lock. Instead of using some kind of key, whether mechanical or electrical, a person's visage is the key. When actual design and implementation is considered, there are numerous types of security cameras that can be used for many different applications. We must analyze their needs and choose accordingly.

[V] Intrusion Detection

The last layer is *intrusion detection* systems or alarms. Intrusion detection monitors for attacks. It is less a preventative measure and more of a response measure, although some people would argue that it is a deterrent. Intrusion detection has a high incidence of false alarms. In many jurisdictions law enforcement will not respond to alarms from intrusion detection systems.

Other Physical Security tools

People play a significant role in all these layers. In the first layer guards patrol and act at check points. In the second layers guards have a role by questioning, reporting and detaining suspicious people. In the third layer, they have to administer electronic

Scanned by CamScanner

access control. In the fourth they have to monitor and analyze video. In the fifth layer, they are expected to respond to alarms. The response force must arrive on site in less time than it is expected that the attacker will require to breach the barriers.

In recent times, new developments in *information and communications technology*, as well as new demands on security managers have widened the scope of physical security apparatus.

Fire alarm systems are increasingly becoming based on *Internet Protocol*, thus leading to them being accessible via local and wide area networks within organisations. Emergency notification is now a new standard in many industries, as well as physical security information management (PSIM). A PSIM application integrates all physical security systems in a facility, and provides a single and comprehensive means of managing all of these resources. It consequently saves on time and cost in the effectual management of physical security.

Many installations, serving many different purposes have physical obstacles in place to deter intrusion. This can be high walls, barbed wire, glass mounted on top of walls, etc.

The presence of PIR-based motion detectors are common in many places, as a means of noting intrusion into a physical installation. Moreover, VSS/CCTV cameras are becoming increasingly common, as a means of identifying persons who intrude into physical locations.

Businesses use a variety of options for physical security, including security guards, electric security fencing, cameras, motion detectors, and light beams.

ATMs (cash dispensers) are protected, not by making them invulnerable, but by spoiling the money inside when they are attacked. Money tainted with a dye could act as a flag to the money's unlawful acquisition.

7.4 THREATS TO PHYSICAL SECURITY

A *disaster* is a natural or man-made hazard that results in significant physical damage or destruction, loss of life or dramatic change to the environment. A disaster occurs when hazards meets vulnerability. A natural disaster is the effect of a natural hazard, for example, flood, earthquakes, volcanic eruption, hurricane, tornados etc.

The physical security of information system resources is threatened by :

(1) *Fire* : Burning caused by fire affects IS through heat, smoke etc. Fire need three elements to take place— burning material (fuel), heat which ignites it and oxygen (for continuity). In case of fire, saving lives is always the top priority.

Control of fire is possible through :

(i) Installing smoke detectors.

(ii) Keeping fire extinguishers near equipments.

(iii) Training of employees in fire evacuation exercises and using fire extinguishers properly.

(2) *Environmental failure* : This is a type of disaster that includes any

Scanned by CamScanner

interruption in the supply of controlled environmental support provided to the operating area.

Environmental controls include :

(i) Clean air

(ii) Air-conditioning (temperature is maintained between 20-25°C)

(iii) Humidity and water control (humidity should be controlled to 40%-60% in computer rooms)

(3) *Earthquake* : Earthquake is a violent ground motion that results from stresses and movement of the earth's surface. Buildings may collapse or become unsafe.

The control lies in keeping computer systems away from glass and elevated surface, and in high risk areas.

(4) *Liquid Leakage* : In spite of best care taken, small accident can happen in the hand of individual working at office premises and data centre. Liquids can harm computers and can electrocute people.

Control is possible by keeping liquid proof cover over the equipments when not in use.

(5) *Lightening* : An electrical charge of air can cause either direct lightening strike to the facilities or through transformers and substations.

There is a need to install surge suppressions, and test uninterruptible power supply. System to prevent damage by lightening.

7.5 PHYSICALLY SECURE FACILITY

A secure facility is a physical location that has been engineered with controls designed to minimize the risk of attacks from physical threat. A secure facility can use the natural terrain; traffic flow, urban development, and can complement these features with protection mechanisms such as fences, gates, walls, guards, and alarms.

Controls for Protecting the Secure Facility

- Walls, fencing, and gates
- Guards
- Dogs, ID cards, and badges
- Locks and keys
- Mantraps
- Electronic monitoring
- Alarms and alarm systems

Controls used in a Secure Facility

[I] ID Cards and Badges

- Ties physical security to information access with identification cards (ID) and/or name badges
  - ID card is typically concealed whereas name badge is visible

Scanned by CamScanner

- These devices are actually bio-metrics (facial recognition). Should not be the only control as they can be easily duplicated, stolen, and modified.

[II] Locks and Keys

- There are two types of locks—mechanical and electro-mechanical
- Locks can also be divided into four categories—manual, programmable, electronic, and biometric

Locks can fail and facilities need alternative procedures for access.

[III] Electronic Monitoring

- Records events where other types of physical controls are not practical
- May use cameras with video recorders
- Drawbacks are :

(i) Do not prevent access or prohibited activity *i.e.*, they are reactive only.

(ii) Recordings are often not monitored in real time and must be reviewed to have any value.

[IV] Alarms and Alarm Systems

- Alarm systems notify when an event occurs.
- Used for fire, intrusion, environmental disturbance, or an interruption in services.
- These systems rely on sensors that detect the event: motion detectors, smoke detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors.

Computer Rooms and Wiring Closets

- Computer rooms and wiring and communications closets require special attention.
- Logical controls are easily defeated, if an attacker gains physical access to the computing equipment.
- Custodial staff are often the least scrutinized of those who have access to offices and are given the greatest degree of unsupervised access.

Interior Walls and Doors

- The walls in a facility are typically either standard walls or fire-resistant walls.
- All high-security areas must have firewall grade walls to provide physical security from potential intruders and improves the facility's resistance to fire.
- Doors that allow access into secured rooms should also be evaluated. They should be strong enough to resist forcible entry.
- Emergency exits should be clearly labeled and should be able to unlock from inside.
- Computer rooms and wiring closets can have push or crash bars installed to meet building codes and provide much higher levels of security than the standard door pull handle.

Scanned by CamScanner

Fire Safety

- The most serious threat to the safety of the people who work in the organization is the possibility of fire.
- Fires account for more property damage, personal injury, and death than any other threat.
- It is necessary that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards.
- ***Fire suppression systems*** are devices installed and maintained to detect and respond to a fire.
- They work to deny an environment of one of the three requirements for a fire to burn: heat, fuel, and oxygen.
  - Water and water mist systems reduce the temperature and saturate some fuels to prevent ignition.
  - Carbon dioxide systems rob fire of its oxygen.
  - Soda acid systems deny fire its fuel, preventing spreading.
  - Gas-based systems disrupt the fire's chemical reaction but leave enough oxygen for people to survive for a short time.

7.6 PHYSICAL ACCESS CONTROL

- Access to information system resource must always be provided only on a "*need-to-know*" basis.
- The physical measure may be complemented by procedural and personnel measure such as :
  (i) Education and training programs.
  (ii) A personnel security system that ensures appropriate approval.
- The number of physical access point at facilities that store or handle information facilities should be commensurate with safety aspect and work function at the site.

Access point should have physical security control such as :

(1) *Fences* : Double doors should be used at critical access points such that unauthorized persons end up trapped between the doors.

(2) *Security guards* : Guards can not be replaced by technology because they have discernment, visibility and serve multiple functions. However, the disadvantages are unpredictability, imperfections and the cost involved associated with human beings.

(3) *Locks* : All facilities in information systems should be locked and controlled. Three types of locks can be employed for physical access controls.

(i) *Preset type* : This is the most common type of lock which requires a particular key to open.

(ii) *Programmable* : They can be mechanical with a dial combination or electronic (cipher lock or keypad).

Scanned by CamScanner

(iii) *Electronic* : These are like the modern car locks.

(4) ***Security badges*** : Photo ID, smart cards or proximity cards can be used as security badges. Photo ID must always be examined by a guard. Biometric access controls require finger scan, retina pattern, voice recognition etc and are very effective in controlling unauthorized access.

7.7 CCTV

Close Circuit TV systems are generally installed in premises for monitoring of assets or organization product quality and surveillance from distant location. This is also used for recording the activities which may be useful for further analysis of any particular event, which went unnoticed or reference of which is felt necessary for analyzing. Similarly, it is found to be very good tool for surveillance of remote but otherwise sensitive areas, to check theft and intrusion. These are also coming alongwith night viewing features and infrared lamps, motion detectors etc. This make them suitable for surveillance with lesser manpower. Following are the main parts of CCTV systems :

(1) ***Camera*** : This is normally CCD type and sends continuous signal from its angle of view to control room.

(2) ***Zoom lens*** : This is put in front of camera and generally motorised type. This consists of a set of lenses. Changing of focal length is from remote (*i.e.*, control room) for zooming in/out and improving focusing/clarity of seen object.

(3) ***Pan-tilt unit*** : For viewing different objects, camera movement in horizontal and vertical direction is required. This is achieved through Pan-tilt unit. The unit comprises of two motors—one each for horizontal and vertical movement. The motor control is through control room. Limit switches are provided to restrict movement in both directions to avoid winding-up of connecting cables.

(4) ***Telemetry receiver*** : This is installed near camera to separate and feed various signals to desired instruments *i.e.*, camera movement (Pan-tilt), zoom lens movement, video signal etc.

(5) ***Cables*** : Cables are required to feed power to various CCTV equipments and carry signals between camera and control room. Coaxial cable (RG-11) is used for this communication. In some configurations, telemetry signals are carried on separate twin twisted cable instead of on co-axial cable, in combination with video signal.

(6) ***Control station*** : This is located in control room and generally consists of multiplexer, controller, monitor, recorder etc. Multiplexer receives and transmits signals to more than one cameras and establishes interface with controller. Controller selects and controls various cameras movement/focusing, selection of cameras on monitor etc. Monitor is usually a TV. High resolution TVs are used to improve clarity of seen objects.

Scanned by CamScanner

7.8 PHYSICAL INTRUSION DETECTION

Intrusion detection system (IDS) are designed to detect actual or attempted unauthorized entry, identify its location and signal a response with an alarm. IDS can :

(i) Provide continuous surveillance over secure area.

(ii) Extend coverage into area not usually accessible to guard.

When the surveillance system is used to monitor or record live events, they are detective. However, if the camera is visible or by putting boards saying "you are under CCTV surveillance" we can use them as a deterrent control.

Intrusion detection systems (physical) can be of following types :

(1) *Photoelectric sensors* which use a grid of visible or IR light.

(2) *Dry contact switches* and *metallic tape* which sound alarm when door is opened or tape is broken.

(3) *Motion detectors* which analyze wave pattern, capacitance or audio signals to signal an alarm.

Alarms used for IDS should have separate circuitry and a backup power source. Also there should be provision to detect attempts to tamper with alarm systems. Alarms are of five types :

(1) *Local system*

- Sounds audible alarm
- Requires *local response capability*—someone to call the police/fire dept.

(2) *Central station system*

- Operated and monitored by private security organizations.
- Connected directly to the protected site via leased or dial-up lines.

(3) *Proprietary System*

- Like central station systems but operated and monitored directly on the premises

(4) *Auxiliary station systems*

- Contact police or fire departments directly
- Require prior authorization
- Typically used along with central station systems

(5) *Remote station system*

- Calls police or fire and plays a recorded message

7.9 BACKUP SECURITY MEASURES

- Contingency Planning (CP) comprises a set of plans designed to ensure the effective reaction and recovery from an attack and the subsequent restoration to normal modes of business operations.

The following points outline the various evaluation tasks that should be evaluated to develop a contingency plan :

Scanned by CamScanner

(1) Evaluate the organization's security policies and controls to accommodate any opportunities found for minimizing vulnerabilities. The evaluation should address the organization's current emergency plan and procedures, and their integration into the contingency plan.

(2) Evaluate current emergency response procedures and their effect on the continuous operation of business.

(3) Develop planned responses to attacks and integrate them into the contingency plan, noting the extent to which they are adequate to limit damage and minimize the attack's impact on data processing operations.

(4) Evaluate backup procedures, including the most recent documentation and disaster recovery tests, to assess their adequacy, and include them in the contingency plan.

(5) Evaluate disaster recovery plans to determine their adequacy in providing a temporary or longer term operating environment. Disaster recovery plans should include testing the required levels of security so that security personnel can see if they continue to enforce security throughout the process of recovery, temporary operations, and the organization's move back to its original processing site or to a new processing site.

Draw up a detailed document outlining the various findings in the above tasks. The document should list :

(1) Any scenarios to test the contingency plan.

(2) The impact that any dependencies, planned-for assistance from outside the organization, and difficulties in obtaining essential resources will have on the plan.

(3) A list of priorities observed in the recovery operations and the rationale in establishing those priorities.

- Organizations need to develop disaster recovery plans, incident response plans, and business continuity plans as subsets of an overall CP as shown in fig. (1).

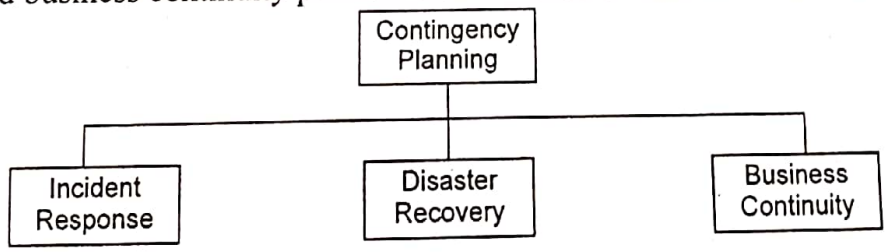

Fig. (1) Components of contingency planning

- An *incident response plan (IRP)* deals with the identification, classification, response, and recovery from an incident, but if the attack is disastrous(*e.g.*, fire, flood, earthquake) the process moves on to disaster recovery plan and BCP.
- A *disaster recovery plan (DRP)* deals with the preparation for and recovery from a disaster, whether natural or man-made and it is closely associated with BCP. It is used to restore normal business operations within a definite period after the disaster.

Scanned by CamScanner

- A Business continuity plan (BCP) ensures that critical business functions continue, if a catastrophic incident or disaster occurs. BCP occurs concurrently with DRP when the damage is major or long term, requiring more than simple restoration of information and information resources.

There are six steps to contingency planning. They are :

(1) Identifying the mission or business-critical functions,
(2) Identifying the resources that support the critical functions,
(3) Anticipating potential contingencies or disasters,
(4) Selecting contingency planning strategies,
(5) Implementing the contingencies strategies,
(6) Testing and revising the strategy

Scanned by CamScanner