UNIT 03 Data Security and Management

Structure

3.0 INTRODUCTION

The tremendous and intensive use of information for several different tasks makes data security, trustworthiness and privacy increasingly critical for these functionalities' in day-to-day living. The protection of data from unauthorised access, use, change, disclosure and destruction by using methods to ensure network security, physical security and file security based on a collection of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure is known as data security. Data security can be applied through various techniques and technologies including administrative controls, organizational standards, etc. and other safeguarding techniques that limit or preclude access to unauthorized or malicious users or processes.

The fundamental question which emerges from this extensive use of data is that why is it important to secure this data and how is this object to be achieved.

Different organizations create, collect, store, receive or transmit data within an organization as well as between organizations/associations and individuals or from one organization to an organization. It doesn't matter what device, technology or process is employed to manage, store, collect or distribute data, but it must be protected as data breaches may result in litigation and huge penalties alongside damage to an organization's reputation. Therefore, the importance of protecting data from security threats is more important today than ever before.

Threats to database are often numerous which can either be accidental or intentional and in either case security of the database and the entire system, including the network, operating system, the physical area where the database resides and the personnel access all have to be considered and protected accordingly.(**Sie Learning, Sydney, 2020, p.1**)

A data security plan which includes procedures both physical and virtual through extensive use of data management software is required to be put in place.(**Michael Buckee, 2020, p.1**)

3.1 OBJECTIVES

After studying this unit, you will be able to:

- Explain what is data security
- Explain data management
- Explain security requirements
- Explain security threats and attacks
- Security measures and usability
- Security management

3.2 Data security and Data Management

Database security is necessary in the following situations:

- Theft and fraud
- Loss of availability of data
- Loss of confidentiality
- Loss of data privacy
- Loss of data integrity

The situations given above are the most likely to be exposed to date security threats and are required to be protected so that the chances of losses in this regard can be significantly reduced.(**The National Academics Press, 1991, ch. 4, p. 49-73)**

It is noteworthy that these situations often cause cumulative losses due to inter dependencies and hence a loss due to one situation can affect multiple areas in the same organisation.

The purpose of data protection (also known as information privacy and data privacy) is to define when and under what circumstances data can be safely put to use

Data management

The main aim of data management helps people and organizations for data to be used within the boundaries of policies and regulations for the maximum benefit of these organizations and businesses and therefore is very valuable as an intangible asset. Data management can be achieved by the practise of collection, keeping and usage of data in a secure, efficient and cost-efficient manner.

Therefore, efficient ways and means are sought by various organizations for data management. The management of data is done through various platforms and include databases, data analysis and more such tools like Microsoft SQL server, Google cloud, Amazon web services, etc.

1. Data management is the responsible stewardship of data throughout its lifecycle. There are five components to data management:

- **Acquisition**
- **Utilization**
- **Maintenance**
- **Access**

- **Protection**

  Effective data management requires appropriate acquisition, utilization, maintenance, access, and protection of data. Data management depends on information confidentiality and criticality.

3.3 SECURITY REQUIREMENTS (CIA)

Data is being used by a vast majority of individuals, entities, businesses and organizations. One such example are the banking giants which deal with massive volumes of private and financial data to the one-man business storing the contact details of his customers on a mobile phone, data is at play in companies both large and small**.(Michael Buckbee, 2020, p.1**)

Since individuals, entities, businesses and organizations deal with data on an everyday basis, this data accumulated over time needs to be protected from outsiders with an intention to misuse such data. Therefore, data security is the primary aim for protection of such data.

Data security is necessary and importantin today's world for all devices or processes which deal with collection, management and storage of data as data breaches may occur anytime and can not only lead to litigation but also damage to the brand and reputation.

The core elements of data security are *confidentiality, integrity and availability*. Also known as the **CIA triad**, this is a security model and guide for organizations to keep their sensitive data protected from unauthorized access.(**Michael Buckbee, 2020, p.1**)

The three governing principles are as follows:

- **Confidentiality**
  Confidentiality or privacy refers to measures taken to ensure that data- particularly sensitive data- is protected from unauthorised access. Keeping in mind the age of ultra-modern technology, privacy is required to be a basic design consideration. The extent of level of confidentiality can vary based on the data type and/or regulation.

- **Integrity**
  Integrity pertains to safeguarding the accuracy of data as it travels through workflows. There should be measures taken to protectdata from unauthorized deletion or modificationand to quickly reverse the damage in the event of a breach. (**ShyamOza, 2019, p.1**)
- **Availability**
  Availabilitymeans providing seamless and continuous access to users through robust servers and network infrastructure with high availability mechanisms built into system design (**ShyamOza, 2019, p.1**).

Some practices for implementation of CIA Triad of confidentiality, integrity and availability are as follows:

i) Putting confidentiality into practice

- Categorization of data and assets being handled by individuals in an organization based on their privacy requirements.
- Requirement of all data encryption and two-factor authentication to be basic security hygiene as a fundamental practice in all organizations dealing with sensitive information.

- Ensure that access control lists and file permissions are monitored and updated regularly by professionals from the IT department in an organization.

ii) Scoping integrity

- Review all data processing, transfer and storage mechanisms and run diagnostic tests to ensure there is no unauthorised access.
- Understand organization's compliance and regulatory requirements by keeping in check with the rules and regulations updated.
- Invest in dependable backup and recovery solution; one that assures business continuity and quick data recovery in the event of a security or data breach.

iii) Ensuring availability

- Build preventive measures into system designs, make security audits routine, auto-update or stay alert of system, network and application updates.
- Utilize detection tools such as network/server monitoring software and anti-virus solutions and regular check-up through timely runs.

Check your progress1 *Spend 3 Min*

What is availability and integrity?

3.4 SECURITY THREATS AND ATTACKS

In today's day and age there is a host of new and evolving cyber security threats that has the information security industry on high alert. There is an increasingly more sophisticated cyber-attacks involving malware, phishing, cryptocurrency. Therefore, the data and assets of the corporations, governments and individuals are at constant risk.

The information technology industry suffers from a severe shortage of cyber security professionals and due to the ever-evolving new technology being introduced periodically, there has been an exponential rise in cybercrime.

The following cyber security threats are constantly growing and creating issues related to data privacy:

i) **Phishing attacks**- These are carefully targeted digital messages transmitted to fool people into clicking on a link that can then install malware or expose sensitive data. Nowadays everyone is aware of the risks of email phishing or of clicking on suspicious-looking links, leading to hackers upping their ante by distributing fake messages with the hope that the recipients will unwittingly compromise their network system. Such attacks enable hackers to steal user logins, credit card credentials and other types of personal financial information, as well as gain access to private databases.

ii) **Ransomware attacks-** Hackers deploy technologies that enable them to literally kidnap an individual or organization's databases and hold all of the information for ransom. These types of attacks are believed to cost victims billions of dollars every year.

iii) **Cyber-physical attacks**- The technology that has enabled to modernize and computerize critical infrastructure also brings risk. There is an ongoing threat of hacks targeting electrical grids, transportation systems, etc., which represent a major vulnerability.

iv) **State-sponsored attacks-** Hackers look to make profit through stealing individual and corporate data. Now even nation states use cyber skills to infiltrate other governments and perform attacks on critical infrastructure. Cyber crime today is a major threat not only to the private sector and individuals but also towards the governments and nations as a whole.
Many such attacks target government-run systems and infrastructure, but private sector organizations are also at risk.

Please answer the following Self-Assessment Question.

Check your progress2 *Spend 3 Min*

What are the various types of cyber threats?

3.5 COMPUTER, MOBILE AND INTERNET

The computer is the foundation of the entire virtual world and is now extensively used both personally and professionally in all walks of life. As the technology related to computers is constantly developing, the methods to secure data within the computers is not necessarily progressing a same pace. The computer inturn has given rise of many other forms of communication which includes the mobile.

The mobile from its name itself denotes communication on the move. This has actually made many conventional systems of interaction obsolete. However due to its ease of use certain issues of data security have surfaced from time to time.

The Internet is an international network of computer systems that has evolved over the last decade. Currently, the Internet interconnects several thousand individual networks that connect over a million computers. The Internet today has become the electronic backbone for computer research, development and user communities. Similar issues of data security which affect the computer and mobile also affect the Internet.

COMPUTER

A computer in layman terms is essentially a machine that was primarily used for calculations. Over the years, the use of a computer has grown two-fold; it not only helps in storing work related information but also has the capacity to transfer communication from one system to another with the help of the Internet.

Computers today have reduced complicated jobs into much simpler tasks. For example, one can write a letter in a word document, edit it, spell check, print copied and also send it to someone across the world in a mere matter of seconds. These activities of simply even writing a letter would have taken someone days, to do before the advent of computers.

In other words, a computer simply is an information processor in a way that it takes whatever raw information or data which is fed by a human and stores that information, then proceeds to decrypt the information entered and consequently provide the result in the form of an output.

The work of a computer is nothing without a computer program. We can see various computer programmes on a computer we rely on like Microsoft Word, Excel, etc. used for carrying out day to day activities at all spheres of life.

MOBILE

The world of digital technology has led to the evolution of various devices that are used for day to day purposes. A computer system is one that cannot be carried by an individual to every place. Therefore, foreasy use of electronic devices and to avail benefits of a computer system a mobile was invented.

A mobile device in essence is a general term used for a handheld computer or a smartphone. The mobile devices invented not only has functions of making calls, receiving calls, sending and receiving text messages, but all contains functions of obtaining emails and carries out functions of a computer system at a smaller level.

A mobile as per defined by digital technology refers to a cell phone usually one with computing ability, or a portable, wireless computing device used while held in the hand, as in mobile tablet, mobile, mobile app, etc.

The success of a mobile's technology has risen in today's world due to possession of a smartphone which has access to Internet and can be used to connect to multiple users wherever and whenever required.

Characteristics of a mobile device (Priya Viswanathan, 2019, p.1):

- Wi-Fi or cellular access to the Internet
- A battery that powers the device for several hours
- A physical or onscreen keyboard for entering information
- Touch-screen interface
- Ability to download data from the Internet

Different meanings of mobile

In different contexts, mobiles are also defined as "mobile development", "mobile-friendly", etc. The term "mobile development" usually refers to creating apps for smartphones, but does not include laptops. "Mobile friendly" on the other hand refers to websites that are easy to use by any user owning a smart phone.

INTERNET

Merriam-Webster's dictionary defines Internet as *an electronic communications network that connects computer networks and organizational computer facilities around the world*.(**Merriam-Webster Dictionary, 2020, p.1**)

There are various devices that help facilitate connections with people around the world with the help of a network. These multiple interconnected networks form the Internet.

How does a user access the Internet?

The answer is simple. A single device that is assigned with an address when it connects to the Internet known as the Internet protocol (IP) address and this address helps in differentiating between devices in the network form all other devices.

Almost every connection to be made with the Internet requires a device which includes an address for sending/receiving messages in the form of emails. Mobile phones too, operate within a network based on services that are provided by service providers. They convert our voice into electronic signals which are then transmitted through radio waves. The same then get converted back into a sound once it reaches another mobile phone.

The use of Wi-Fi has grown two-fold due to connection to the Internet wirelessly. The concept of free Wi-Fi is now commonly available in public places such as airports, cafes, etc.

3.5.1 LIMITATIONS

Like every technology that has advanced every day, the risks too increase. Even a mobile phone/device and a computer having an Internet technology has its limitations. Some of them are mentioned below:

- Speed- Speed of the Internet is very essential for complete usage of a mobile device. If the speed of an Internet connection is slow, it results in lagging or slows down of the device and crashes which then renders the mobile device unusable.
- Accessibility- Websites though easily accessible on laptops may not be easily accessible on a mobile device as the website may not have implemented mobile versions. Therefore, a mobile phone may not always get the desired website to be accessed by a user.
- Incompatibility- Mobile web browsers are not the same as a laptop or a computer web browser works. Therefore, some web browsers may be incompatible with mobile operating systems.
- Leakage of data- Mobile apps often provide free apps in the form of advertisements, which usually do not undergo malware tests to ensure safety of the app. Therefore, users downloading such mobile apps make themselves liable to unintentional data leakages relating to personal data.
- Use of unsecured Wi-Fi- Users of internet want to preserve their cellular data for the long run or to not receive hefty phone bills and therefore rely on free Wi-Fi networks. At time such free Wi-Fi network are unsecured and leads to compromise of data security which is liable to be hacked by technology users.
- SMishing- This type of scam is similar to the phishing scam wherein cybercriminals ask users to download malware by clicking on malicious links. The method of SMishing scam is done through text messages instead of email like in the case of phishing scams.

3.6 SECURITY MEASURES AND SOLUTIONS

As discussed on 3.3 which deal with security requirements, it has been stated that the concept of CIA is very important. Further, security threats are inventive according to the new information technology launched. These security threats constantly evolve and are harmful to an organization as they steal, harm or corrupt information stored in an organization's system. An organization should arm themselves with resources to safeguard themselves from the ever-growing security threats. Therefore, the CIA triad though being a security model and guide for organizations to protect their sensitive data there are a few other data security considerations that one should be aware of:

- **Access security**- By restricting access of users who have been granted access to information, thereby results in monitoring who all have access to a particular data. Therefore, in cases of data theft, sifting through the timelines of access granted to users can be easier to track down the culprit.

- **Data encryption**- Data when kept unencrypted leads to misuse of personal data by cybercriminals. Therefore, data has to be encrypted by usage of unique encryption codes, so as to avoid leakage of vital information stored in databases. When data has been encrypted and only the user has access to such a data has the decryption code, results in prevention of data theft.

- **Email security**-It is a form of procedure to protect an email account and the contents on an email account from unauthorised access. Therefore, measures like strong email passwords, end-to-end encryption of emails or messages that are sent from one person to another result in prevention of misuse of data, as emails are a popular forum for hackers to spread malware, spam and phishing attacks. For example- end-to-end encryption used by WhatsApp.

- **Risk-assessment analysis**- Organizations have to take a proactive approach while dealing with information security concerns. The main of conducting a risk assessment is to identify the risks pertaining to information stored in an organizations system. By conducting risk assessment analysis, an organization can understand and assess internal and external risks to their security, confidentiality and personal information stored in various storage media like laptops and portable devices.

- **Monitor effectiveness**- It is critical for an organization to verify security programs established and to establish if such security programs manage cyber security measures implemented for safeguarding an organization's information or data. This is done through regular tests and monitoring of information security programs annually or quarterly helps to assess the number of attacks made to an organizations data.

- **Third party issues**- Website's play a major role while showcasing an organization's success. Therefore, they implement third party tools to make their websites' more interactive and user-friendly and offer smooth connectivity for user interaction. These third-party tools help in generating revenue for an organization's website. Therefore, an organization has to undertake to ensure that all reasonable steps have been taken prior to giving access to third party service providers and that such third-party service providers apply the stringiest security measures.

- **Strong firewall**- Firewall of a system is part of such system's cyber security measure. A firewall enables to protect a system from internet traffic and services it is exposed to. These services are accessed by everyone who uses an internet. Therefore, firewalls enable to control who gains access to an organization's system like insider attacks which may originate from within a network used by an organization. Antiviruses are for files and firewalls are needed to protect from unauthorised access or usage of network. A firewall simply helps to control Internet traffic that is generated by using a network for work.

- **Antivirus protection**- An antivirus protection can be gained in the form of antivirus software. This software is a program designed to avoid, detect and deal with cyber

security threats that an organization may face. The process of an antivirus is to run background scans on a system to detect and restrict unauthorised access in the forms of malware and to protect a system from vulnerabilities it may face. These solutions are extremely important for data security and must be installed on computer systems. These antivirus protections are available not only for laptops and computers but also for mobile devices and help to fight unwanted threats to files and data.

- **Back-up regularly-** A data security is meant for protecting information stored on a system from unauthorised access, destruction of such information and includes network security. Therefore, to avoid loss of data, data should be regularly be stored and kept somewhere safe where it cannot be accessed or violated by anyone. Further, the securing of such data helps in preventing accidental modification to data, theft of data, breach of confidentiality agreements and avoid release of data prior to its verification and authentication.

Check your progress3 *Spend 3 Min*

Describe in brief the various security measures.

3.7 SECURITY POLICY

In 2013, the Government of India took the primary formalized step towards cyber security vide Ministry of Communication and Information Technology, Department of Electronics and Information Technology's National Cyber Security Policy, 2013.

The purpose of the policy is to create a safe and resilient cyber space for individuals, organizations and the government. The mission is to secure cyberspace data and framework, develop capacity to avert and react to cyber-attacks and mitigate harm through collaboration of institutional systems, individuals, procedures and technology.

Some of the strategies adopted by the policy include (Government Initiatives, 2013):

- Creating an assertion structure;
- Encouraging open standards;
- Strengthening the administrative structure combined with intermittent audits, synchronization with global guidelines and spreading awareness about the legitimate system;
- Securing e-administration by executing worldwide accepted procedures and more extensive utilization of Public Key Infrastructure.

In India, the government recently implemented some essential tools to resolve cyber security issues as mentioned below:-

1. USB Pratirodh was launched by the government to monitor unauthorized use of removable USB storage media devices.
2. Samvid permits just pre-approved set of executable documents for execution and shields work areas from suspicious applications from running.
3. M-Kavach gives insurance against issues identified with malware that take individual data and accreditations, abuse Wi-Fi and Bluetooth assets, misplaced or stolen versatile gadget and undesirable/spontaneous approaching calls.

Browser JSGuard is a device which fills in as a program augmentation which distinguishes and protects malicious HTML and JavaScript attacks. It warns the user while visiting malicious web pages and provides a comprehensive threat analysis report of the web page.

3.8 SECURITY MANAGEMENT

Security management means minimizing the interruption of business activities and reducing the vulnerability to various attacks. Security bargains with distinctive trust aspects of information.

Data security includes engineering where an incorporated permutation of appliances, arrangements and resolutions, software, surveillance, and vulnerability scans work together.

Security is not just restricted to computer systems; it applies to all perspectives of securing data or information, in whatever structure. Security is accomplished utilizing a few methodologies at the same time or utilized in blend with one another.

There are six principles of security management:-

1. Availability- The continuous accessibility of systems tends to procedures, policies and controls which are used to ensure prompt access to data for authorized customers. This purpose secures against deliberate or inadvertent endeavours to refute legitimate costumers' access to data.

2. Integrity of data or systems- System and data integrity is linked to the procedures, policies and controls which are used to guarantee that data has not been modified in an unconstitutional way and that systems are liberated from illicit manipulation that would compromise precision, comprehensiveness and consistency.

3. Confidentiality of data or systems- Confidentiality covers the procedures, policies and controls which are utilized to secure data of customers and the organization against illicit access or use.

4. Accountability- Accountability incorporates the procedures, policies and controls essential to follow activities to their source. Accountability specifically underpins non-repudiation, anticipation, infringement, deterrence, security checking, recuperation and legitimate tolerability of records.

5. Assurance- Assurance addresses the procedures, strategies and controls which are used to create certainty that specialized and equipped security measures are working as anticipated.

6. Privacy- It centres on the constitutional rights of people, the motivation behind data assortment and processing, security predilection and the manner in which organizations administer individual's data. It focuses on how to gather, process, offer, document and erase the information/data as per the law.

3.9 SECURITY AUDIT

Security auditing is a vital part to assess the security strength of data frameworks and systems for any organization and in this way the determination of the foremost suitable

security auditor could be an important choice. Due to its exceptionally particular and specialized nature, security examination is often outsourced.

Considering the inclusion of sensitive, critical and private organizational information, it is imperative that security evaluator should be competent and reliable. Security inspecting assignments can take numerous diverse shapes depending upon the sort and measure of auditee organization. It is recommended that audit contracts be settled only upon discussion with auditee's officially authorized/contractual specialists and after consultation with the auditor. Security auditing under the risk management plan may be conducted as a separate task or as part of the risk assessment process.

Security audits give a reasonable and computable way to scrutinize how secure a site really is. This assessment is designed to:-

- Create a security benchmark for your organization;
- Identify the qualities and shortcomings of current security rehearses;
- Prioritize the exposures that present the most serious hazard;

Provide hazard alleviation proposals reliable with consistence guidelines, security industry best practices, customer industry best practices and customer business targets. The information picked up from data security audits enables customers to make more informed resolution about how to allot budgets and assets so as to most viably oversee hazard.

Check your progress4 *Spend 3 Min*

Describe security audit?

3.10 SECURITY AND USABILITY

Reliance on information technology in the society has been increasing by leaps and bounds with the resulting ability of organizations, individuals to conduct attacks on computer systems, networks, mobiles, etc.

Computer security in layman terms is defined by the attributes of the CIA triad.

The term usability can be taken in narrow terms of quality of a system's interface, but the concept applies more broadly to how a system supports the requirements of the user. Usability though dealing with quality of a system's interface also includes the term "user experience". This refers to the ease with which a user can access or use a product or a website.

The official ISO 9241-11 definition of usability is: *"the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."* **(Interaction Design Foundation, 2020, p.1)**

Thus, usability deals with the following outcomes:

- A website or product should be easy for a user, so that they can navigate such websites without unnecessary hindrances and work with efficiency;
- A user can achieve their objectives through using a particular website by way of easy and detailed navigation. For example: the process of booking a movie ticked, if a good design is in place, it will guide the user through the easiest process to purchase movie tickets;

– A user upon subsequent visit to a website or a product page can easily recall and use such website or product page.

Usability though dealing with quality of a system's interface also includes the term "user experience". This refers to the ease with which a user can access or use a product or a website.

Many advances have been made towards security but it often remains complex and has to be managed effectively or conveniently by individuals or enterprises. Security is hard to understand and thereby often results in use of operating systems in an unsecured manner. Therefore, security technologies have been developed in such a manner wherein system administrators have primary responsibility of maintaining security protection.

Though security protections have been enhanced in various ways to protect a data system from malicious attacks, at times such security protections tend to be clumsy and awkward, resulting in obstacles to get work done resulting in security protections being disabled or bypassed by users. This leads to end users often engaging in actions, knowingly or unknowingly compromising the security of computer systems or contribute to attacks by hackers. Therefore, security and usability are attributes that trade off against each other. Usability decides if protection of a system is strong or not.

3.11 SUMMARY

The protection of data from unauthorised access, use, change, disclosure and destruction by using methods to ensure network security, physical security and file security based on a collection of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure is known as data security. Data security can be applied through various techniques and technologies including administrative controls, organizational standards, etc. and other safeguarding techniques that limit or preclude access to unauthorized or malicious users or processes.

Database security is necessary for the following situations:

- Theft and fraud
- Loss of confidentiality or secrecy
- Loss of data privacy
- Loss of data integrity
- Loss of availability of data

In some conditions, these areas are directly related such that an activity that results in a loss in one area can also cause a loss in another since all of the data within an organization are interconnected.

Data management is the practice of collecting, keeping and using data securely, efficiently, and cost-effectively. The goal of data management is to assist people, organizations and connected things optimize the use of data within the bounds of policy and regulation in order that they will make decisions and take actions that maximize the benefit of the organization.**(Oracle, 2020, p.1)**

The main objective of data security is to protect the data which an organization directly owns or that which belongs to third party while this data is being received, collected, stored created or shared, as the case maybe.

There is no difference as to which device, technology or process is utilized to manage, store or collect data, and it must be protected. Data breaches may result in litigation cases and huge

fines, but it may also lead to damage an organization's reputation. The importance of shielding organizations, individuals and business' data from security threats is more important today that it's ever been.

The core elements of data security are *confidentiality, integrity and availability*. Also known as the **CIA triad**, this is a security model and guide for organizations to keep their sensitive data protected from unauthorized access and data exfiltration. (**Michael Buckbee, 2020, p.1**)

The information technology industry continues to suffer from a severe shortage of cyber security professionals and experts constantly warn that the stakes are higher than ever. The rise in cybercrime epidemic even risks shaking the public faith in such cherished ideals as democracy, capitalism and personal privacy.

The following cyber security threats are on the rise and posing a risk to data privacy:

i) Phishing attacks
ii) Ransomware attack
iii) Cyber-physical attack
iv) State-sponsored attack

The CIA triad though being a security model and guide for organizations to protect their sensitive data there are a few other data security considerations that one should be aware of:

- Access security
- Data encryption
- Email security
- Risk-assessment analysis
- Monitor effectiveness
- Third party issues
- Strong firewall
- Antivirus protection
- Back-up regularly

Security management means minimizing the interruption of business activities and reducing the vulnerability to various attacks. Security bargains with distinctive trust aspects of information.

Data security includes engineering where an incorporated permutation of appliances, arrangements and resolutions, software, surveillance, and vulnerability scans work together.

3.12 SOLUTIONS/ANSWERS

Check Your Progress

1. Integrity is the protection against proper modification or destruction of information includes non-repudiation and authenticity. Low integrity leads to concerns and information with high integrity is considered critical. Availability refers to the reliability, access to and use of information. Low availability of information may be considered supplementary whereas, high availability information is considered as critical and must be made accessible in order to prevent negative impact on an organization's activities.

2. The cyber crimes are:
   i) Phishing attacks which enable hackers to steal user logins, credentials and personal financial information to gain access to private databases;

ii) Ransomware attacks are used to kidnap an individual/organization's database for ransom purposes;
iii) Cyber-physical attacks are threats to electrical grids, transportation systems etc. to critical infrastructure;
iv) State sponsor attacks are used to infiltrate other governments and attack their critical information.

3. These are:
   i) Data encryption to ensure that personal data cannot be obtained illegally and be misused by cyber criminals;
   ii) Email security by end-to-end encryption so that only authorised individuals can access encrypted data;
   iii) Strong firewalls to protect from unauthorised access/usage of network;
   iv) Antivirus protection to protect data;
   v) Regular back-up to ensure that data is not lost or cannot be accessed by unauthorised individuals.

4. Security audit deals with regular inspection of security measures implemented to protect personal information. A security audit is conducted to give a reasonable way to scrutinize how secure a site is and/or the information stored is also properly protected. Security audit creates benchmarks for an organization to handle the shortcomings to security measures which have been implemented.

3.13 REFERENCES /FURTHER READINGS.

- Ashutosh Bhatt (2014). How Internet Works on Mobile Devices. p1-11; https://www.engineersgarage.com/how_to/how-internet-works-on-mobile-devices/
- Business Technology Standard. Security and data protection. p1-6; https://www.managebt.org/book/strategy-and-governance/security-and-data-protection/
- Circadence (2020). The future of finance cyber security in 2020. p1-3; https://www.circadence.com/blog/the-future-of-finance-cyber-security-in-2020/
- Denis Otieno (2020). Cyber security threats and trends for 2020. p1-14; https://just40days.com/detail_Cybersecurity-Threats-and-Trends-for-2020_37750
- Elisa Bertino (2016). Introduction to Data Security and Privacy, p1-6; https://link.springer.com/article/10.1007/s41019-016-0021-1
- Forcepoint. What is Data Security? Data security defined. explained and explored. p1-6; https://www.forcepoint.com/cyber-edu/data-security
- Government Initiatives (2013). https://baliyans.com/courses/disaster-management-and-internal-security/cyber-security/government-initiatives http://sielearning.tafensw.edu.au/toolboxes/Database_Administration/content/security/threats.htm
- Interaction Design Foundation (2020, p.1). https://www.interaction-design.org/literature/topics/usability
- Internet. https://www.merriam-webster.com/dictionary/Internet
- Makerere University. Data Security and Its Technologies. p1-3; https://answers.mak.ac.ug/security/data-security-and-its-technologies

- Michael Buckbee (2020). Data Security: Definition. Explanation and Guide. p1-12;.https://www.varonis.com/blog/data-security/
- Oracle India. What is data management?p1-10; https://www.oracle.com/in/database/what-is-data-management/
- Priya Vishwanatha (2019). What is a mobile device?. p1-11; https://www.lifewire.com/what-is-a-mobile-device-2373355
- Priya Viswanathan (2019. p.1). https://www.lifewire.com/what-is-a-mobile-device-2373355
- ShyamOza (2019, p1). CIA Triad: Best Practices for Securing Your Org.https://www.business2community.com/cybersecurity/cia-triad-best-practices-for-securing-your-org-02232416.
- ShyamOza (2019. p.1). https://spanning.com/blog/cia-triad-best-practices-securing-your-org/
- Sie Learning, Sydney (2020). Threats to the Database.
- The National Academics Press (1991). *Computers at Risk: Safe Computing in the Information Age*. Ch-4. 49-73; https://www.nap.edu/read/1581/chapter/4
- Unitag. What is mobile web?. P1-4. https://www.unitag.io/mobile-websites/
- W3Schools. Database Security. p1-2; https://www.w3schools.in/dbms/database-security/