MODULE 3

CHAPTER 3

Ethical Issues and Privacy

University Prescribed Syllabus

Information Security, Threat to IS, and Security Controls.

3.1 ETHICAL ISSUES

- **Ethics mean the guidelines that decide whether a behavior is right or wrong. A code of ethics is** a collection of principles that aim to help in ethical decision making.
- Most of the modern organizations have developed their own codes of ethics also commonly called as **business ethics** to guide themselves as well as employees towards a good conduct at the workplace and at the same time protecting their employees' moral rights.

3.1.1 Ethical Frameworks

- Although there are many more, the four broadly used ethical standards are **the utilitarian approach, the rights approach, the fairness approach, and the common good approach.**
- According to the utilitarian approach, the act that does the most good or least harm to someone is ethical.
- The rights approach considers those actions as ethical that protect and respect the moral rights of someone to the greatest.
- The fairness approach states that treat all human beings equally or atleast fairly.
- Lastly, the common good approach emphasizes on social relationship where reverence and consideration for all beings is considered to be ethical.
- By combining these four standards, we can build up a general framework for ethical decision making. The framework can be summarized into five steps as follows:
  - Identify the ethical issue and how it is affecting an individual or a group of individuals.
  - Collect the relevant facts from the concerned people so that you are able to make a right decision.
  - Assess all possible actions that can be taken based on any of the above approaches such as utilitarian, rights, fairness or common good approach.
  - Take up a decision to select the best possible approach that solves the issue and also check its consequences or impact.
  - Carry out the appropriate action.
- To understand the ethical framework we can consider this example. As per our belief an ethical action would be the one where an individual who does more of physical hard work should be paid more and one who does less work should be paid less.
- But in practicality, a construction labour that does maximum physical hardwork is not paid higher or even equally to the Vice President (VP) of a company who does comparatively less physical hardwork. So, is it really unethical act to pay a VP more and labour less?
- But if we analyze the scenario and collect the facts we see that the person who is paid more as VP has done a lot of hardwork initially and taken lot of efforts to reach that position and a labour worker could not pursue a good qualification due to some reasons and as a result has to do a lot of physical hardwork to earn a living.

- The VP is a person who is actually controlling the entire organization and its decisions. The job may involve less physical work but more of logical decision making as well as responsibility. Therefore paying a VP more and construction worker less is ideally ethical.
- Thus, we can see that we can apply the above framework to analyze a situation and decide whether an action is ethical or not.
- Consider another example where Government taking a decision to demolish an illegally constructed building. Although it is correct by law but it might seem unethical to destroy homes of so many people living in that building and making them homeless. So, any decision that is unethical need not be illegal.
- The fundamental code of ethics includes **responsibility, accountability and liability.**
- **Responsibility** means that an individual is answerable for the consequences of decisions/actions taken.
- **Accountability** means to find out who is responsible for decisions/actions taken.
- **Liability** means a person has the right to legally recover the harm or loss caused due to the decision/action.

3.1.2 Ethics and Information Technology

UQ. Explain the Ethical issues and threats of information security? **MU - Q. 1(c), Dec. 19, 5 Marks**

UQ. Describe the categories of ethical issues related to information technology. **MU - Q. 2(e), Jan 21, 5 Marks**

- Once we have understood the concepts of ethics and ethical framework in general, let us go ahead with ethics related to Information Technology.
- **Computer ethics** involve appropriate use of computers. Examples of unethical use of computers include excessive usage of office internet for personal use by employees, a firm selling its customer information databases to other companies, monitoring of employees activities by employer when at work etc.
- There should be some rules and principles within an industry that will guide to what is ethical and what is not.
- The vast growth of IT applications has generated a variety of **ethical issues** that fall into four categories. They are:
  1. **Privacy issues** involve issues related to accumulating and protecting information about individuals. E.g. what information about someone can be revealed or what should be kept private, to what extent surveillance should be carried on an employee within an organization etc.
  2. **Accuracy issues** involve issues related to ensuring the preciseness and correctness of information about individuals. E.g. how to ensure that the information about customers in company databases like their addresses, contact numbers is all updated and correct.

3. **Property issues** involve issues related to ownership of information. E.g. who has the copyrights for a particular intellectual property and what is the fair and just means to access it, say by paying some amount of access fees.
4. **Accessibility issues** involve issues related to rights of an individual to use particular information and to what extent and at what price. E.g. who has the right to accesss confidential information within an organization, under what restrictions and to what extent?

3.2 PRIVACY

- Privacy is the right of an individual to not be disturbed or observed by anyone whereas Information privacy is the right of an individual to decide how much information about oneself can be revealed and/or collected by others.
- Information technology is becoming so advanced that collecting information of people is becoming very easy and rapid.
- This is leading to many questions on privacy issues related to individuals. Few examples of the same are discussed below.

3.2.1 Digital Dossiers

- **Digital Dossier** is nothing but creation of electronic profiles of people who use the internet. People visiting shopping websites, social networking sites, querying search engines, leave behind their digital footprints and reveal alot about themselves.
- This information can be collected together from various places to generate a digital dossier of the person which is depicted in Fig. 3.2.1.
- Not only this but enough data about someone can be captured through surveillance systems such as CCTV cameras on traffic signals and toll roads, over telephone calls, through government records etc. The process of forming a digital dossier is also called as **profiling.**

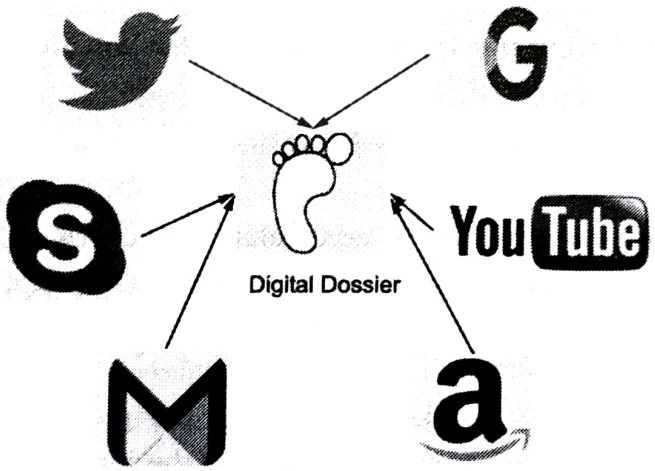

Fig. 3.2.1: Digital dossier

3.2.2 Electronic Surveillance

- Another major privacy related concern is Electronic Surveillance. According to law carrying out electronic surveillance is considered legal.
- Therefore, there is almost no restriction on employers conducting surveillance on their employees or by the government on the citizens.
- Employers can monitor and track the employees' e-mails, softwares and documents stored on the employees' computer and also trace their internet usage pattern.
- If needed employees may incorporate url filtering to restrict access to inappropriate content on the internet and also to avoid wastage of employee time and increase their productivity.
- The Government also keeps a track of vehicles passing through toll roads and traffic signals through CCTV surveillance.
- The technologies used to conduct this surveillance are becoming easily achievable and affordable at very cheaper costs.
- Devices such as digital cameras, sensors, data collection and storage technologies have become quiet inexpensive.
- That is the reason for rapid growth in usage of these technologies by various organizations and government agencies.

3.2.3 Personal Information in Databases

- Many Organizations collect and store information about individuals in their organizational databases.
- Banks maintain their customer databases, hospitals have their patient databases, and schools have their student databases. How appropriately is this information being used by organizations? And do they ensure that integrity of this information is maintained?
- Do the organizations guarantee that this information will not be misused or propogated to some other organizations for profit making without the consent of the individual? Maintaining an appropriate balance between data collection and personal privacy is very important.

3.2.4 Information on Internet Bulletin Boards, Newsgroup and Social Networking Sites

- In our daily lives we are making extensive use of newsgroups, chatrooms, weblogs and social networking sites.
- The bulletin boards and blogs are regularly updated and also contain personal opinions and views.
- Do these groups ensure that the information they reflect about someone is completely true, authentic and not offending anyone?
- Anonymous and offensive information on such websites about individuals can defame them and can have a negative impact on their image. It is a major ethical issue to maintain a right balance between freedom of speech and privacy.

3.2.5 Privacy Policies

- **Privacy policies** are rules framed by an organization to guide them as to which information about their customers and employees can be revealed and which should be kept private.
- Many organizations give their customers the choice to decide what kind of information and to how much extent can that information be collected from them in the form of opt-in and opt-out models, cookies, private browsing methods etc.

(i) Privacy Policy Guidelines

The Privacy policy guidelines emphasize on three major aspects.

- **Data Collection :** Data about individuals should be collected only with their consent. Secondly, only that much data should be collected that will suffice the business needs. Say, if a company wants to take feedback about their product from the customer, then only sufficient data to get reviews from the customer should be collected. No other hidden means should be used to track additional information about the customer without his consent.
- **Data Accuracy :** Very personal and essential information collected about individuals should be properly validated by the individuals themselves before storing them into company databases for future references. Changes to this stored data must be checked and updated regularly with the latest copy of it, so that all authorized users have access to the updated version of the information.
- **Data Confidentiality :** Proper security mechanisms to protect data from unauthorized access should be applied. Anyone other than the authorized user should take proper permissions to access the information.

(ii) Data Protection Laws

- The Data Protection Laws implement the above guidelines to streamline the ways an individual's personal data is collected, stored and disseminated.
- These laws help in protecting the privacy and integrity of data about individuals which is possessed by business organisations.
- In India today we have minimal laws that administer data protection and privacy.
- The Law in India that deals with data protection and privacy is the **Information Technology Act, 2000 and the (Indian) Contract Act, 1872.**
- The Government has also advised the Information Technology Rules, 2011. The Rules only deal with protection of very confidential and personal information such as passwords, bank details, credit/debit card information, medical records, mental conditions, sexual orientation etc.

(iii) International Aspects of Privacy

- With the rapid growth and excessive use of the Internet, governments all over the world have enacted a large number of inconsistent privacy and security laws.

- Approximately fifty countries have some form of data-protection laws. Many of these laws conflict with those of other countries, or there are countries that have no privacy laws at all.
- The absence of consistent or uniform standards for privacy and security obstructs the flow of information among countries, a problem we refer to as *transborder data flows.*
- For example, since many countries are outsourcing their work into India, data protection has become a critical political issue.
- Lack of data protection laws in India does not generally affect India's ability to handle personal information from the United States but the growing market of outsourcing from EU countries is placing greater pressure for India to abide by their rules and regulations.
- So, the same country India has to follow different laws and to what extent it can actually fulfil the data protection restrictions is still questionable. And problems like these will become more complicated over a period of time where online businesses are increasing rapidly.
- Governments must make an effort to develop laws and standards to cope with rapidly changing information technologies in order to solve some of these concerns.

3.3 INFORMATION SECURITY

3.3.1 Introduction to Information Security

- **Information security** specifies the various rules designed to safeguard an organization's information and information systems (IS) from access and misuse by unscrupulous users.
- The security measures are applied to overcome the threats posed on the safety of these information resources.
- A **threat** is nothing but any risk or danger to which a system may be exposed. Whereas **vulnerability** refers to the weaknesses of the information systems that increase the chances of systems being affected by some form of threat.

The root causes to these vulnerabilities can be explained as below:

(A) Today's Interconnected, Interdependent, Wirelessly Networked Business Environment
(B) Smaller, faster, cheaper computers and storage devices
(C) Decreasing skills necessary to be a computer hacker
(D) International organized crime taking over cybercrime
(E) Lack of management support

(A) Today's Interconnected, Interdependent, Wirelessly Networked Business Environment

- With the advent of Internet, the computer systems can be connected anywhere over the globe and information can be easily shared anywhere and anytime.

- And as a result alongwith trusted networks within the organization, untrusted networks which are external to the organization can also easily get access to the organizational resources.
- To add to it, the upcoming use of wireless technologies is making it even more dangerous to secure private information.

(B) Smaller, faster, cheaper computers and storage devices

- Modern technologies and computing equipments such as laptops, palmtops, pendrives, smart phones used for information storing, processing and sharing are becoming quiet smaller, cheaper and easily portable.
- Because of which they can be easily lost or stolen and as a result important information stored in them can easily be achieved by unauthorized users.

(C) Decreasing skills necessary to be a computer hacker

- The Internet has become a huge source of information of any type.
- Due to which any person with minimal technical knowledge can easily learn the tricks to hack sensitive information from any computerized system.
- They can easily understand the code and scripts that can be used to invade information systems.

(D) International organized crime taking over cybercrime

- Lot of cybercrimes are happening for money making purposes .Although they might not be that brutal but they may lead to losses of thousands of dollars to the victim.
- Computer-based crimes cause huge damage to businesses in terms of cost of loss of business as well as recovery costs.

(E) Lack of management support

- Lastly, the support of top level management for incorporating security policies within the organizations for safeguarding their information resources is very important.
- The lower level managers and executives who are responsible for the day-to-day activities of the other employees must monitor and keep a track that those policies are being strictly implemented.

3.3.2 Principles of Information Security

Any information security measure implemented should follow the following principles.

- **Confidentiality :** Confidentiality refers to personal information about an individual that generally cannot be revealed to third parties without his consent. Very often the terms "confidentiality" and "privacy" are used interchangeably.
- **Integrity :** Integrity refers to ensuring that the data has not been corrupted or changed and is accurate and consistent.
- **Availability :** Availability refers to timely, reliable and continual accessibility of data.

- **Non repudiation :** Non repudiation refers to non denial by an individual of being responsible for a particular action.
- **Authenticity :** Authenticity refers to proving that the information is legitimate and reliable.
- **Accountability :** Accountability means taking responsibility for what you do with personal data and how you comply with the other principles.

3.3.3 Security Threats

UQ. Explain the Ethical issues and threats of information security ? **MU - Q. 1(c), Dec. 19, 5 Marks**

UQ. What are major security threats to the information system? Discuss the measures taken to control information security. **MU - Q. 4(b), Dec. 19, 10 Marks**

Information systems within organizations are susceptible to various types of threats. These threats can be classified into two major types :

(a) Unintentional Threats (b) Deliberate Threats

We will discuss both the types in detail in the further section and the same has been shown in the Fig. 3.3.3.

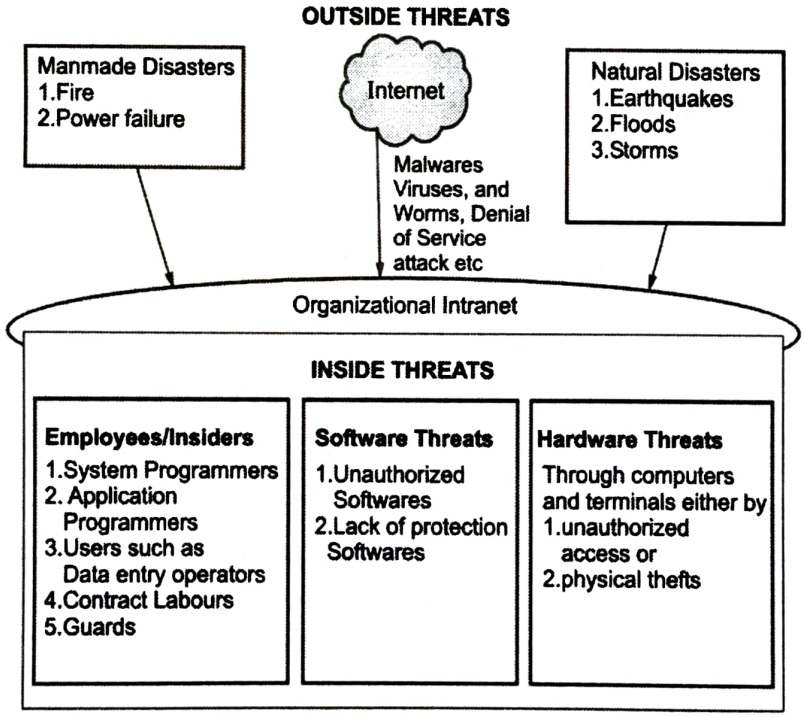

Fig. 3.3.3 : Security Threats

Let us have a look at Unintentional Threats.

(a) Unintentional Threats

These type of threats are unintended and unplanned threats but if caused impose serious problems to information security.The main class of threats under this type are threats that are caused due to **Human errors.**

1) Human Errors

- Mistakes caused by employees within an organisation could pose severe issues to information security.
- Who are the people who could be a major cause of such problems? First and foremost the higher level employees who have access to the entire organizational data.
- Secondly, the human resource people who deal with the personal data of all the employees and the software people who control the entire information systems within the organization.
- The information security employees have all the privileges to access, create, store, and modify critical data within the organization. A small mistake by these people could lead to disastrous impact on the information security.
- Other than these, employees like contract labours and guards could also be indirectly responsible for information leakage because contract labours are also temporarily hired and cannot be completely relied upon.
- Security guards could also be appointed on contract basis and many a times they are the ones who are working when the entire office staff has left. Any kind of negligence from such employees also could be a risk factor.
- Other types of human errors which could lead to loss of information could be due to carelessness and laziness of individuals like forgetting to logout from personal machines, setting weak passwords, misplacing personal devices like laptops, disposing off old equipments without erasing personal data etc.

2) Social Engineering

- The second class of unintentional threats is **Social Engineering.**
- It is a type of attack caused by social interactions. The employees within the organization are fooled by attackers by pyshcologically manipulating them to reveal confidential information. Examples of social engineering attacks include **Impersonation, Exterminator, Tailgating, Shoulder Surfing.**
- **Impersonation :** Such type of attacks include fraud calls impersonating some senior official of the company, pretending to have forgotten some important password and tries to convince the junior employee to reveal the same.

- **Exterminator :** Somebody who pretends to be a Computer technician or an AC repair person and gets an entry into the organization. He then uses his tricks to gain information from employees through social skills.
- **Tailgating :** Also known as piggybacking, is a physical **security** breach in which an unauthorized person follows an authorized employee to enter a secured premise.
- **Shoulder Surfing :** An attack where the suspect watches over the employees shoulder to gather some secret information. May be a visitor in the company just tries to watch the computer screen standing behind the employee.

  Also in public places like airports or public transport where the employee is doing his office work on personal laptop and somebody tries to spy the activities of the employee without his knowledge to gain some confidential information.

▶ **(b) Deliberate Threats**

Such attacks are caused on purpose to pose serious problems to information security. The various types of deliberate threats are discussed below.

- **Espionage :** Espionage is like trespassing, where an unauthorized person tries to gain access to organizational information through illegal means.
- **Information Extortion :** Information extortion is where an attacker steals or threatens to steal confidential information from the organization. The attacker may force the organization to pay a ransom for not misusing that information.
- **Sabotage or Vandalism :** Sabotage or vandalism involves defaming the image of the organization by giving negative reviews or false tweets about the company and its products and services. This leads to a catastrophic impact on the customer loyalty and the company might lose its customers.
- **Theft of Equipment or Information :** All the computing devices used these days such as laptops, PDASs, smartphones etc. are getting smaller in sizes but larger in their computing and storage capability. They are also easily portable and as a result chances of them getting lost or being stolen is increasing. And once stolen attackers could easily try to retrieve the information from these devices.
- **Identity Theft :** Identity theft is an intentional attempt to steal some ones identity to misuse it. Usually it is done to get access to the person's financial information such as bank account details, credit card information etc. This can be done through impersonation, stealing the mails or searching through disposed off items like old files and folders, pendrives etc. (also called as dumpster diving).
- **Compromises to Intellectual Property :** Intellectual property rights are the rights given to persons or organizations for creation of their original work and usually for a particular duration of time. Four types of intellectual properties are *Copyrights, Patents, Trademarks, and Trade Secrets.*Protecting such intellectual properties is a very critical issue for people who make their livelihood in knowledge fields.

- A **trademark** is a type of intellectual property consisting of a recognizable sign, design, or expression which identifies products or services of a particular source from those of others.
- A **trade secret** is an intellectual work, such as a business plan, that is a company secret and is not based on public information. An example is the Coca-Cola formula.
- A **patent** is an official document that grants the holder exclusive rights on an invention or a process for a specified period of time.
- **Copyright** is a statutory grant that provides the creators or owners of intellectual property with ownership of the property for a designated period.Owners are entitled to collect fees from anyone who wants to copy their creations. Copyright laws protect expression of ideas rather than the ideas themselves. Under section 13 of the Copyright Act 1957, copyright protection is conferred on literary works, dramatic works, musical works, artistic works, cinematograph films and sound recording.

– **Software Attacks**

Since the computers and the internet have evolved, software attacks have taken pace. Cybercrimes are increasing, attackers are using malicious softwares to infect as many computers all over the world with the intent of money making or personal rivalries. Few of the software attacks include:

- **Virus :** A small code or script that attaches to another computer program to cause malicious actions.
- **Worm :** A small computer code or script that not just performs malicious actions but also replicates and spreads by itself.
- **Phishing Attack :** Phishing attacks use some fraudulent technique to gain access to confidential information by impersonating some official looking emails or messages.
- **Denial-of-Service Attack :** Attacker sends so many requests to a computer system which it is unable to handle and as a result crashes.

– **Alien Softwares**

- **Alien softwares** are like undercover programs that are installed on your computer through deceitful methods.
- These softwares are not that harmful but could be annoying like the adware softwares that keep flashing some pop up ads on the screen or small pieces of code like the cookies that can track the behaviour and surfing patterns of an individual on the Web.

– **Supervisory Control and Data Acquisition(SCADA)Attacks**

- SCADA systems are distributed control systems used to control chemical, physical, and transport processes used in oil refineries, water and sewage treatment plants, electrical generators, and nuclear power plants.
- They make use of sensors that are connected in a network and if attackers get access to the network, they can cause severe damage to the operations of the oil refineries or nuclear plants.

- **Cyberterrorism and Cyberwarfare**
  - **Cyberterrorism** and **cyberwarfare** include making use of computer systems connected over a network to perform some kind of harm to other computer systems with the intent of destroying or damaging the systems or revealing some sensitive information.
  - Such actions are usually carried out for money or to oppose a political agenda.

3.3.4 Information Security Controls

UQ. Identify the three major types of controls that organizations can use to protect their information resources, and provide an example of each one? **MU - Q. 2(f), Jan. 21, 5 Marks**

UQ. What are major security threats to the information system? Discuss the measures taken to control information security. **MU - Q. 4(b), Dec. 19, 10 Marks**

- To safeguard the critical information within the organization many security controls are being implemented.
- All the aspects of an information system including hardware, software, data and networks need to be protected using various countermeasures.

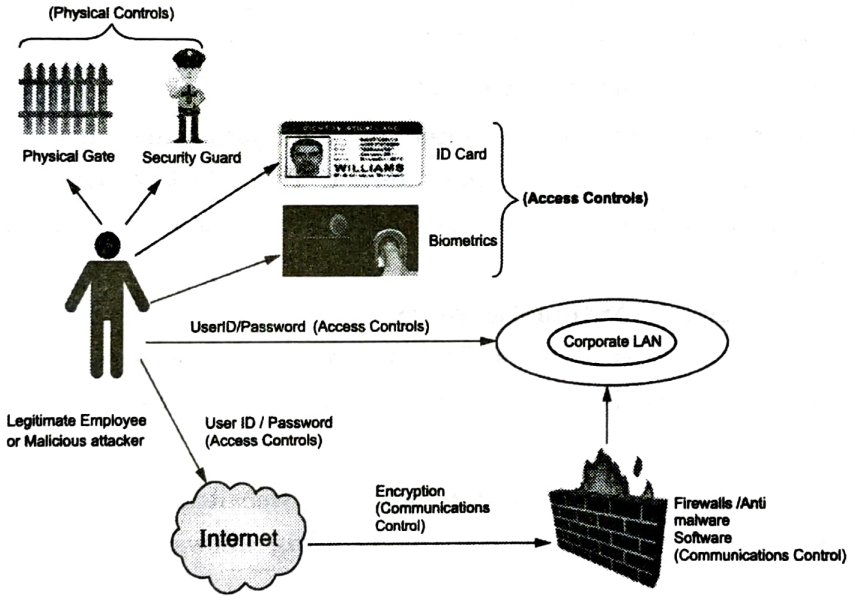

Fig. 3.3.4 : Types of Security Controls

- The three major types of controls include **physical controls, access controls, and communications controls.** Fig. 3.3.4 illustrates these controls.

Physical Controls

- **Physical controls** are applied to prevent unauthorized access to a company's confidential information.
- Common physical controls include physical gates, security guards and alarm systems.

- Such type of controls also keeps a check that the employees log off their systems when they leave the office.

☞ **Access Controls**

- **Access controls** also avoid unauthorized access to organizational information .Common access controls include: **authentication and authorization**. **Authentication** is a process to check the identity of the person before giving him access to confidential data. Authentication methods involve IDs and passwords, biometrics etc.
- Biometric is a method of human identification based on his physical characteristics such as fingerprint recognition, face recognition, iris recognition etc.
- Once an individual is authenticated then is applied the process of authorization. **Authorization** decides what kind of privileges and access rights is given to the individual based on his identity.

☞ **Communications Controls**

Communications controls deal with various **network controls**. They deal with secure transfer of data over the network. Communications controls consists of firewalls, anti-malware systems, encryption, virtual private networks(VPNs), secure socket layer(SSL) / transport layer security(TLS), and employee monitoring systems.

- **Firewalls :** A **firewall** is a system that filters the information that should enter corporate LAN from untrusted outside world through the internet. The filtration depends upon specific rules defined within the firewall. It prevents unauthorized users to access company's private network over the internet.
- **Anti-malware Systems : Anti-malware systems** commonly known as *antivirus* software identify and remove viruses and worms. They are installed on corporate computer systems. Most widely used anti viruses include McAfee, Norton antivirus, Quick Heal etc
- **Whitelisting and Blacklisting**
  - **Whitelisting** allows only permitted softwares or websites to run on corporate systems i.e. those which are whitelisted whereas **Blacklisting** allows all the softwares and websites except those on the blacklist.
  - For example, a company might blacklist porn websites so that employees do not indulge into unfair activities or may restrict peer-to-peer file sharing on its systems.
- **Encryption**
  - It is the process of converting a plaintext (original message) into ciphertext (form which cannot be understood by anyone except the intended recipient). Encryption systems use keys which are used for encoding and decoding the messages.
  - Common type of encryption method used is **Public-key encryption** which is an asymmetric key encryption i.e it makes use of two sets of keys-public and private for encryption and decryption process. Usually public key is known to all whereas private key is kept secret.

- There are third party verification authorities also called as **Certification Authority (CA)** such as Verisign, which issue digital certificates to organizations.
- These digital certificates act as an identity proof for an organization and are valid for a particular period. Having a certificate from a CA ensures that the company is genuine and transactions carried out with such organizations are verified and safe.

– **Virtual Private Networking**

- A **virtual private network** is a private network but makes use of public network such as the Internet to connect users.
- VPNs use a process called **tunnelling** that encrypts each data packet that is to be sent and envelopes each encrypted packet inside another packet. In this manner, the packet can travel across the Internet with confidentiality, authenticity, and integrity.

– **Secure socket layer protocol**

- It is also called as Transport Layer Security (TLS).
- TLS encrypts and decrypts data between a Web server and a browser. Any website using TLS has the URL beginning with "https" rather than "http," and it often displays a small padlock icon in the browser's status bar. Padlock icon indicates secure connection.

– **Employee monitoring systems**

- They are a kind of surveillance systems that monitor the activities of employees like their usage of office computer systems, their e-mail activities, Internet surfing activities.
- These systems are implemented by corporates as a step to avoid unethical behaviour as well as avoiding and tracking employee mistakes.
- With the help of such systems, company authorities can easily identify employees who spend too much time surfing on the Internet for personal reasons or who visit questionable websites.

⏭ 3.4 MULTIPLE CHOICE QUESTIONS

Q.1 The purpose of a copyright is_____. **(Jan. 2021)**

(a) Closely safeguarded as a secret, or legal protections are lost

(b) Information that gives one company a competitive advantage over others

(c) Designed to protect the expression of ideas

(d) Designed to protect inventions, tangible objects, or ways to make them **✓Ans. : (c)**

Q.2 _____ is the method of translating an original message into a type that, except for the intended recipient, cannot be interpreted by anyone. **(Jan. 2021)**

(a) Virtual Private Network (VPN) (b) Firewall

(c) Secure Socket Layer (SSL) (d) Encryption **✓Ans. : (d)**

Q.3 The identity of the person who needs access is verified by a process called as ___

(a) Authentication (b) Authorization (c) Biometrics (d) Password ✓**Ans. : (a)**

(Jan. 2021)

Q.4 Which of the following statements does NOT provide an accurate description of ethics?

(a) Ethics is the code of moral principles that sets standards of "good" versus "bad" or "right" versus "wrong."

(b) Ethics provide principles to guide the behaviour of individuals and groups.

(c) Ethics is a set of principles that guide the organization's analysis of its external environment and the formulation of actions to respond to that environment.

(d) Ethics provides principles that help people in making moral choices among alternative courses of action.

✓**Ans. : (c)**

Q.5 _____ reflect(s) the code of moral principles that sets standards as to what is "good" versus "bad" or "right" versus "wrong" in people's conduct, and thereby guides their moral choices and behaviour.

(a) Group norms. (b) Legal behavior (c) Ethics (d) Civil law. ✓**Ans. : (c)**

Q.6 _____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.

(a) Network Security (b) Database Security

(c) Information Security (d) Physical Security ✓**Ans. : (c)**

Q.7 From the options below, which of them is not a vulnerability threat to information security?

(a) natural calamity like floods (b) without deleting data, disposal of storage media

(c) unchanged default password (d) latest patches and updates not done ✓**Ans. : (a)**

Q.8 A _____ is a computer program that can invade computer and perform a variety of functions ranging from annoying (e.g. popping up messages as a joke) to dangerous (e.g. deleting files)

(a) Computer Virus (b) Antivirus

(c) Ms Word (d) Ms Access ✓**Ans. : (a)**

Q.9 _____is the right to determine when and to what extent information about you can be gathered and/or communicated to others.

(a) Information Privacy (b) Information Integrity

(c) Information Right (d) Information Leakage ✓**Ans. : (a)**

Q.10 Which of the following is not a vulnerability factor to organizational information?

(a) Today's interconnected, interdependent, wirelessly networked business environment

(b) Smaller, faster, cheaper computers and storage devices;

(c) Decreasing skills necessary to be a computer hacker;

(d) Increasing use of firewalls.

✓**Ans. : (d)**

Q.11 Social Engineering threats include which of these

(i) Exterminator, (ii) Tailgating, (iii) Shoulder Surfing, (iv) natural disaster

(a) (iv) only (b) (i), (ii) and (iii)

(c) (iii) only (d) (ii) and (iv)

✓Ans. : (b)

Q.12 Which one of the following is not an internal threat?

(a) Hardware threats (b) Employee misconduct

(c) Data entry errors (d) Storms

✓Ans. : (d)

Q.13 _____ is a statutory grant that provides the creators or owners of intellectual property with ownership of the property for a designated period.

(a) Copyright (b) Research grant

(c) Apprenticeship (d) Proprietorship

✓Ans. : (a)

Q.14 Which of these is not a security control

(a) Physical controls (b) Access controls

(c) Communication controls (d) Patent control

✓Ans. : (d)

Q.15 A_____ is a collection of principles that aim to help in ethical decision making

(a) code of conduct (b) code of morals

(c) code of behavior (d) code of ethics

✓Ans. : (d)

Q.16 Which of these is not amongst the standard ethical approaches?

(a) the utilitarian approach (b) the rights approach

(c) the fairness approach (d) the moral approach.

✓Ans. : (d)

Q.17 The fundamental code of ethics include

(a) responsibility, accountability and liability (b) authencity, confidentiality, integrity

(c) responsibility, integrity, liability (d) none of above

✓Ans. : (a)

Q.18 Categories of Ethical issues include

(a) privacy, accuracy, property, accessibility (b) responsibility, accountability and liability

(c) authenticity, confidentiality, integrity (d) None of above

✓Ans. : (a)

Q.19 Privacy is

(a) the right of an individual to not be disturbed

(b) the right of an individual to not be observed by anyone

(c) to not reveal anything about oneself

(d) all of above

✓Ans. : (d)

Q.20 _____is the right of an individual to decide how much information about oneself can be revealed and/or collected by others.

(a) Information Security (b) Information Privacy

(c) Information Confidentiality (d) Information Integrity

✓Ans. : (b)

Q.21 The process of forming a digital dossier is also called as _____

(a) Dossiering (b) Footprinting

(c) Profiling (d) None of above

✓**Ans. : (c)**

Q.22 _____is the creation of electronic profiles of people who use the internet.

(a) Digital Profile (b) Digital Dossier (c) Digital Print (d) Digital trace

✓**Ans. : (b)**

Q.23 The Privacy policy guidelines emphasize on three major aspects of data:

(a) data collection, data accuracy, data confidentiality

(b) data privacy, data accuracy, data property

(c) data authencity, data confidentiality, data integrity

(d) data responsibility, data accountability, data liability

✓**Ans. : (a)**

Q.24 The Law in India that deals with data protection and privacy is the

(a) Information Technology Act, 2000 (b) Data Protection Act, 2000

(c) Information Privacy Act, 2000 (d) None of above

✓**Ans. : (a)**

Q.25 Transborder Data flow issues deal with

(a) The absence of uniform standards for privacy and security that obstructs the flow of information among cities

(b) The absence of uniform standards for privacy and security that obstructs the flow of information among countries

(c) The absence of uniform standards for privacy and security that obstructs the flow of information among states

(d) None of above

✓**Ans. : (b)**

Q.26 _____specifies the various rules designed to protect an organization's information and information systems (IS) from misuse.

(a) Information protection (b) Information privacy

(c) Information security (d) Information system protection

✓**Ans. : (c)**

Q.27 A _____ is any risk or danger to which a system may be exposed.

(a) Threat (b) Vulnerability (c) Hazard (d) Menace

✓**Ans. : (a)**

Q.28 _____ refers to the weaknesses of the information systems that increase the chances of systems being affected by some form of threat.

(a) Threat (b) Vulnerabilty (c) Risk (d) Danger

✓**Ans. : (b)**

Q.29 Which of these is not a principle of Information security

(a) Confidentiality (b) Integrity (c) Non-repudiation (d) Testability

✓**Ans. : (d)**

Q.30 The two major categories of threats to information systems are

(a) intentional and deliberate (b) purposeful and unpurposeful

(c) unintentional and deliberate (d) None of above

✓**Ans. : (c)**

Q.31 Which of these are examples of unintentional threats?

(a) Human errors (b) Social engineering

(c) Impersonation (d) All of above **✓Ans. : (d)**

Q.32 _____ include fraud calls pretending to have forgotten some important information.

(a) Exterminator (b) Impersonation (c) Tailgating (d) Shoulder surfing **✓Ans. : (b)**

Q.33 Somebody who pretends to be a computer technician or fire marshal and gets an entry into the organization is which type of attack?

(a) Exterminator (b) Impersonation (c) Tailgating (d) Shoulder surfing **✓Ans. : (a)**

Q.34 It is a physical security breach in which an unauthorized person follows an authorized person to enter a secured premise.

(a) Exterminator (b) Impersonation (c) Tailgating (d) Shoulder surfing **✓Ans. : (c)**

Q.35 _____involves defaming the image of the organization by giving false negative reviews.

(a) Sabotage (b) Espionage (c) Tailgating (d) Impersonation **✓Ans. : (a)**

Q.36 Information extortion is where

(a) an unauthorized person tries to gain access to organizational information through illegal means

(b) an attacker steals or threatens to steal confidential information from the organization and asks for ransom for not misusing it.

(c) an attacker tries to defame the reputation of an organization.

(d) None of above **✓Ans. : (b)**

Q.37 _____is an intentional attempt to steal someones identity to misuse it.

(a) Identity theft (b) Identity breach

(c) Identity robbery (d) Identity burglary **✓Ans. : (a)**

Q.38 _____are the rights given to persons or organizations for creation of their original work and usually for a particular duration of time.

(a) Right to Identity (b) Authorization Rights

(c) Intellectual property rights (d) Access control rights **✓Ans. : (c)**

Q.39 A _____ is a type of intellectual property consisting of a recognizable sign, design, or expression which identifies products of an organization.

(a) Trademark (b) Patent (c) Copyright (d) Trade secret **✓Ans. : (a)**

Q.40 A small computer code or script that not just performs malicious actions but also replicates and spreads by itself.

(a) Worm (b) Virus (c) Bug (d) Germ **✓Ans. : (a)**

Q.41 A _____ is an official document that grants the holder exclusive rights on an invention or a process for a specified period of time.

(a) Trademark (b) Patent (c) Copyright (d) Trade secret **✓Ans. : (b)**

Q.42 Attacker sends too many requests to a computer system which it is unable to handle and as a result crashes. Which type of attack is it?

(a) Denial of service attack (b) Phishing attack

(c) Trojan horse attack (d) Alien attack

✓**Ans. : (a)**

Q.43 Which controls prevent unauthorized access to organizational information?

(a) Physical controls (b) Access controls

(c) Communication controls (d) Patent control

✓**Ans. : (b)**

Q.44 Access control involves

(a) authentication and authorization (b) verification and validation

(c) authentication only (d) verification only

✓**Ans. : (a)**

Q.45 _____ is a method of human identification based on his physical characteristics such as fingerprint,iris etc

(a) Physical metrics (b) Geometrics

(c) Biometrics (d) None of above

✓**Ans. : (c)**

Q.46 A _____is a system that filters information that should enter corporate LAN from untrusted outside world through the internet.

(a) Firewall (b) Virtual Private Network

(c) Secure Socket Layer (d) Transport Layer Security

✓**Ans. : (a)**

Q.47 Any website with URL beginning with "https" is using

(a) Firewall (b) Transport Layer Security

(c) Virtual Private Network (d) Tunneling

✓**Ans. : (b)**

Q.48 A _____is a private network but makes use of public network such as the Internet to connect users.

(a) Virtual Public Network (b) Virtual Private Network

(c) Bayesian Network (d) Neural Network

✓**Ans. : (b)**

Q.49 Public-key encryption makes use of

(a) asymmetric keys (b) symmetric keys

(c) public keys (d) private keys

✓**Ans. : (a)**

Q.50 Third party verification authorities also called as _____issue digital certificates to organizations.

(a) Certification Power (b) Certification Supremacy

(c) Certification Autonomy (d) Certification Authority

✓**Ans. : (d)**

Q.51 Which of these is not an Anti-malware system?

(a) CCleaner (b) Mcafee (c) Norton Antivirus (d) QuickHeal

✓**Ans. : (a)**

Chapter Ends...

❑❑❑