Assignment-2

Name : Nitesh Kumar Verma **Reg-No :21MCA10060**

Q1) Ans:

Both general management and IT management are responsible for implementing information security to protect the ability of the organization to function. Decision-makers in organizations must set policy and operate their organization in a manner that complies with the complex, shifting political legislation on the use of technology. Management is responsible for informed policy choices and the enforcement of decisions that affect applications and the IT infrastructures that support them. Management can also implement an effective information security program to protect the integrity and value of the organization's data.

Q2) Ans:

Data is important in the organization because without it an organization will lose its record of transactions and/or its ability to deliver value to its customers. Since any business, educational institution, or government agency that functions within the modern social context of connected and responsive service relies on information systems to support these services, protecting data in motion and data at rest are both critical. Other assets that require protection include the ability of the organization to function, the safe operation of applications, and technology assets.

Q3) Ans:

Employees are the greatest threats since they are the closest to the organizational data and will have access by nature of their assignments. They are the ones who use it in everyday activities, and employee mistakes represent a very serious threat to the confidentiality, integrity, and availability of data.

Employee mistakes can easily lead to the revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information.

Common types of malwares are viruses, worms, Trojan horses, logic bombs, and back doors.

Computer viruses are segments of code that induce other programs to perform actions. Worms are malicious programs that replicate themselves constantly without requiring another program to provide a safe environment for replication.

Once a trusting user executes a Trojan horse program it will unleash viruses or worms to the local workstation and the network as a whole.

Viruses and worms both cause damage and copy themselves rapidly. The main difference is how they self-replicate, with viruses requiring the help of a host and worms acting independently. Unlike viruses, worms can replicate and spread without any human activation.

Q4) Ans:

In more recent worm attacks such as the much-talked-about. Blaster Worm., the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely. A Trojan horse is not a virus. It is a destructive program that looks as a genuine application.

A buffer overflow occurs when a program tries to write too much data in a fixed length block of memory (a buffer). Buffer overflows can be used by attackers to crash a web-server or execute malicious code.

If your web-server is vulnerable to buffer overflow attacks, it is only a matter of time until a hacker injects code and takes control of your system.

Q5) Ans:

The major differences between law and ethics are mentioned below:

1. The law is defined as the systematic body of rules that governs the whole society and the actions of its individual members. Ethics means the science of a standard human conduct.
2. The law consists of a set of rules and regulations, whereas Ethics comprises of guidelines and principles that inform people about how to live or how to behave in a particular situation.
3. The law is created by the Government, which may be local, regional, national or international. On the other hand, ethics are governed by an individual, legal or professional norm, i.e., workplace ethics, environmental ethics and so on.
4. The law is expressed in the constitution in a written form. As opposed to ethics, it cannot be found in writing form.
5. The breach of law may result in punishment or penalty, or both which is not in the case of breach of ethics.
6. The objective of the law is to maintain social order and peace within the nation and protection to all the citizens. Unlike, ethics that are the code of conduct that helps a person to decide what is right or wrong and how to act.
7. The law creates a legal binding, but ethics has no such binding on the people.

Civil law comprises a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people.

Policy is the outlines of what a government is going to do and what it can achieve for the society as a whole. “Policy” also means what a government does not intend to do. It also evolves the principles that are needed for achieving the goal. Policies are only documents and not law, but these policies can lead to new laws.

Q6) Ans:

The ISO/IEC 27001 family of standards, also known as the ISO 27000 series, is a series of best practices for improving an organization’s information security policies and procedures, giving it a framework to address risks and capitalise on opportunities as it moves into the future.

The ISO 27000 family of information security management standards is a series of mutually supporting information security standards that can be combined to provide a globally recognised framework for best practice information security management.

The ISO 27000 series is the most widely referenced security models in the information technology-code of practice for information security management. Since Oct 2005, the ISO has published six of this these standards. ISO 27001: for creating information security management systems (ISMS). ISO 27002: this is a code of practices governing information security. ISO 27003: this focuses on the PDCA (Plan-do check-act) problem solving method for ISMS. it has been proposed but not yet published. ISO 27004: This standard guides the development and assessment of ISMS, in alignment with the ISO 27002. ISO 27005: It discusses information security risk management. ISO 27006: This regulates the accreditation of organization that certify and register ISMS.