DON BOSCO INSTITUTE OF TECHNOLOGY, MUMBAI - 400 070
Department of Computer Engg. & Info. Technology
(Academic Year ODD Semester 2021 – 2022)

Course Code and Name: ILO 7016 - Cyber Security and Laws(BE Sem VII)

Name:Hayden Cordeiro **Branch: COMPS** **Roll no: 05**

ASSIGNMENT NO. 6

Assignment Questions:

1. **Define information and explain the contemporary definition for information security. What are the protection goals of information security?**

Information

- Information, in a general sense, is processed, organised and structured data. It provides context for data and enables decision making. For example, a single customer's sale at a restaurant is data – this becomes information when the business is able to identify the most popular or least popular dish.
- More technically, information can be thought of as the resolution of uncertainty; it answers the question of "What an entity is" and thus defines both its essence and the nature of its characteristics.

Information Security

- Information security, sometimes abbreviated to infosec, is a set of practices intended to keep data secure from unauthorized access or alterations, both when it's being stored and when it's being transmitted from one machine or physical location to another. You might sometimes see it referred to as data security. As knowledge has become one of the 21st century's most important assets, efforts to keep information secure have correspondingly become increasingly important.

Information Security Goals in an Organization

There are three main objectives protected by information security, collectively known as CIA:

- Confidentiality—prevents unauthorized users from accessing information to protect the privacy of information content. Confidentiality is maintained through access restrictions. Breaches of confidentiality can occur due to human error, intentional sharing, or malicious entry.
- Integrity—ensures the authenticity and accuracy of information. Integrity is maintained by restricting permissions for editing or the ability to modify information. Loss of integrity can occur when analog information is not protected from environmental conditions, digital information is not transferred properly, or when users make unapproved changes.
- Availability—ensures that authorized users can reliably access information. Availability is maintained through continuity of access procedures, backup or duplication of information and maintenance of hardware and network connections. Loss of availability can occur when networks are attacked due to natural disasters, or when client devices fail.

2. **What is an information security management system (ISMS)? Why is an ISMS important? What are the advantages of an ISMS?**

- An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.
- An ISMS typically addresses employee behavior and processes as well as data and technology. It can be targeted towards a particular type of data, such as customer data, or it can be implemented in a comprehensive way that becomes part of the company's culture.
- ISO27001 is a specification for creating an ISMS. It does not mandate specific actions, but includes suggestions for documentation, internal audits, continual improvement, and corrective and preventive action.

Importance

- Secures your information in all forms

An ISMS helps protect all forms of information, including digital, paper-based, intellectual property, company secrets, data on devices and in the Cloud, hard copies and personal information.

- Increase your attack resilience

Implementing and maintaining an ISMS will significantly increase your organisation’s resilience to cyber attacks.

- Reduce information security costs

Thanks to the risk assessment and analysis approach of an ISMS, organisations can reduce costs spent on indiscriminately adding layers of defensive technology that might not work.

- Respond to evolving security threats

Constantly adapting to changes both in the environment and inside the organisation, an ISMS reduces the threat of continually evolving risks.

- Improve company culture

The Standard’s holistic approach covers the whole organisation, not just IT, and encompasses people, processes and technology. This enables employees to readily understand risks and embrace security controls as part of their everyday working practices.

- Offers organisation-wide protection

An ISMS protects your entire organisation from technology-based risks and other, more common threats, such as poorly informed staff or ineffective procedures.

- Provides a central framework

An ISMS provides a framework for keeping your organisation’s information safe and managing it all in one place.

- Protects confidentiality of data

An ISMS offers a set of policies, procedures, technical and physical controls to protect the confidentiality, availability and integrity of information.

3. **What are the objectives of ISO 17799?**

The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

- security policy
- organization of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development and maintenance
- information security incident management
- business continuity management

- compliance.

The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment.

4. Briefly discuss the ISO 17799/BS7799. Also mention their drawbacks. ISO 17799/BS 7799

- One of the most widely referenced and often discussed security models is the Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- In 2000, this Code of Practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799.

Drawbacks of ISO 17799/BS 7799

Several countries have not adopted 17799 claiming there are fundamental problems:

- The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
- 17799 lacks “the necessary measurement precision of a technical standard”
- There is no reason to believe that 17799 is more useful than any other approach currently available
- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

5. What is the Gramm-Leach-Bliley Act (GLBA)? Explain the security and encryption requirements for GLBA.

- The Gramm-Leach-Bliley Act (GLB Act or GLBA) is also known as the Financial Modernization Act of 1999.
- It is a United States federal law that requires financial institutions to explain how they share and protect their customers’ private information.
- To be GLBA compliant, financial institutions must communicate to their customers how they share the customers’ sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers’ private data in accordance with a written information security plan created by the institution.
- The primary data protection implications of the GLBA are outlined in its **Safeguards Rule**, with additional privacy and security requirements issued by the FTC’s **Financial Privacy Rule**, created under the GLBA to drive implementation of GLBA requirements.
- The GLBA is enforced by the FTC, the federal banking agencies, and other federal regulatory authorities, as well as state insurance oversight agencies.

Security and encryption requirements for GLBA

- Section 501 of the GLBA, “Protection of Nonpublic Personal Information,” requires financial institutions to establish appropriate standards related to the administrative, technical, and physical safeguards of customer records and information. The scope of these safeguards is defined in the GLBA Data Protection Rule, which states that financial institutions must:

➔ Ensure the security and confidentiality of customer data
➔ Protect against any reasonably anticipated threats or hazards to the security or integrity of such data

➔ Protect against unauthorized access to, or use of, such data that would result in substantial harm or inconvenience to any customer

- Many federal agencies oversee financial institutions, and the Federal Financial Institutions Examination Council (FFIEC) designs and supervises audits for the majority of them. The FFIEC publishes the IT Examination Handbook, which provides guidance for the IT security controls that can or should be used to protect nonpublic information under GLBA.
- According to the IT Examination Handbook, financial institutions should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit. Encryption implementations should include:

➔ Encryption strength sufficient to protect the information from disclosure until such time as disclosure poses no material risk
➔ Effective key management practices
➔ Robust reliability
➔ Appropriate protection of the encrypted communication's endpoints

6. State the differences between HIPAA, SOX, and GLBA regulatory compliance.

- The primary difference between each set of compliance regulations is that they are all focused on protecting a different type of data.
- HIPAA protects a patient's healthcare information, SOX protects financial information of public companies, and GLBA protects the data of financial institution customers.
- However, they all share a unified goal: keeping sensitive data secure.
- When you trust a secure file sharing solution to protect your data, you minimize the risk of noncompliance and can meet compliance regulations with a single solution.
- Instead of implementing all the needed security measures yourself, you can trust that your file sharing solution vendor has done the necessary work for you.
- You'll be confident that your data is protected, and you're in compliance with HIPAA, SOX, or GLBA

7. Write down the key IT requirement for the following:

a. NERC

Standard	Requirement	Level
CIP-005-5	R1.3: Enforce inbound and outbound access permissions	High, Medium
CIP-005-5	R1.5: Mechanisms to detect malicious communication	High, Medium (control centers)
CIP-005-5	R2.1: Remote interactive sessions direct to intermediate system	High, Medium (externally routable)
CIP-005-5	R2.2: Encrypt remote interactive traffic to intermediate system	High, Medium (externally routable)
CIP-005-5	R2.3: Multi-factor authentication for interactive sessions	High, Medium (externally routable)
CIP-003-7	p.30: LERC implements network access control on addresses and ports	Low

b. PCI

PCI DSS Requirements	
PCI DSS Objective 1	Build and Protect a Secure Network
PCI DSS Requirement 1	Install and maintain a firewall to protect your cardholder data
PCI DSS Requirement 2	Do not use the vendor's default values for device passwords and other security parameters
PCI DSS Objective 2	Protect Cardholder Data
PCI DSS Requirement 3	Protect stored cardholder data
PCI DSS Requirement 4	Encrypt the cardholder data transmission over public networks
PCI DSS Objective 3	Create a Vulnerability Management Program
PCI DSS Requirement 5	Use and update anti-virus software regularly
PCI DSS Requirement 6	Build and maintain secure applications and systems
PCI DSS Objective 4	Apply Strong Access Control Measures
PCI DSS Requirement 7	Limit access to cardholder data according to specified requirements

c. FISMA

- Information System Inventory
- Risk Categorization
- System Security Plan
- Security Controls
- Certification and Accreditation

d. HIPAA

- Network Encryption
- Control Access
- Authenticate ePHI
- Encrypt Devices
- Control Activity audits
- Enable Automatic logoff