1. introduction to MoIS
2. Planning for security
3. Planning for contingencies
4. Information Security Policy
5. Developing the security program
   1. Security in s. org.
   2. In medium
   3. In large
   4. Components of security program
   5. Roles and titles
   6. SETA programs
   7. Developing security awareness components
6. Security Management Models
   1. Blueprints, frameworks, and security models
   2. Access control models
   3. Data classification models
   4. Trusted computing base
   5. Common criteria
7. Security Management Practices
   1. Benchmarking
   2. Due Care/Due Diligence
   3. Baselining
   4. Support for benchmark and baseline
   5. Risk Management Framework
8. Introduction to Risk Management
   1. Overview
   2. Definitions
   3. Important terms
   4. General risk management model
   5. Daily risk management model
9. Risk Management in Public Sector
   1. Purpose risk management in arahan keslematan and MyMIS
   2. Gov. direction
   3. SIRIM’s risk assessment method
10. Protection Mechanism
    1. Various access control approaches
    2. Various types of firewall
    3. Dial-up and protection
    4. IDPS
    5. Cryptography
11. Personnel and Security

Security issues in small, medium, and large organization

* Small and medium size organization:

**1)   Unprecedented Attacks**

The amount of valuable information that resides on multiple data sources has grown exponentially from the early days of a single computer. So, Business owners must make security plans with this attack surface in mind, and not think only about their business computers and mobile devices.

**2)   Cyber Espionage**

 It’s important for business owners to be aware of cloud technology best practices and regulations surrounding sensitive data. Setting the cloud up securely is important, and monitoring it is key.

**3)   Data Theft**

Many criminals target these businesses as “gateways” into larger ones, as small businesses usually don’t have the large and robust security protocols in place that prevent theft.

* Large size organization:

**1)   Cyber attack**

**2)   Data breach**

**3)   Unplanned IT and telecom outages**

**4)   Interruption to utility supply**

**5)   Adverse weather**

Security education, training, and awareness

Security education: Teaching the fundamental concept of security

Security Training: Practical approach on real situation

Security Awareness Program: Awareness of the security on daily operations, the consequences on every action towards the system security and the contemporary security issues

Data classification

***Data Classification-***is the process of categorizing data assets based on nominal values according to its sensitivity. For example, data might be classified as: public, internal, confidential (or highly confidential), restricted, regulatory, or top secret.

NIST security model

Blueprints, frameworks, and security models

Blueprints: describes existing controls and identifies other security controls

Framework: the outline of the more through blueprint

Security model: a generic blueprint offered by a service organization

Benchmarking

***Benchmarking*** **is a methodology of setting goals at specific levels with reference to an outside performance standard, such as best practices/performance of another department / enterprise**.

For example, a benchmark might be best-in-class customer service level for any enterprise in an industry or a competitor with best customer service level. ***Benchmarking* is a process of learning, measuring and adapting best practices and processes from any organization to improve performance.**

Security Performance measurement

**Information security performance measurement:**

is a tool that may be used by the management to support their decisions.Furthermore, a performance measure seeks to design, implement and manage the utilization of the data collected. The data collected is referred to as measures. The performance measure aims at determining the efficiency of the whole security program.

**Indicators of effective performance measurement might include:**

* The time it takes to detect and report security-related incidents.
* Benchmarking comparable organizations for costs and effectiveness.
* The ability to determine the effectiveness/efficiency of controls.
* The absence of unexpected security events.
* Knowledge of impending threats.

IDPS

An **intrusion detection system** (IDS) is software that automates the **intrusion detection** process. An **intrusion prevention system** (IPS) is software that has all the capabilities of an **intrusion detection system** and can also attempt to stop possible incidents.

Firewalls

**Packet Filtering Routers:** Routers are configured to control access by monitoring the protocol and address information of each packet. It is also known as Static Filtering.

**Screened Host Firewalls:** This includes Packet Filtering along with a dedicated firewall which examines HTTP Protocol(Application Layer Protocol). This particular host is called as Bastion Host.

**Dual-Homed Host Firewalls:** This is a dual homed host firewall with more than one NIC(Network Interface Cards). The main objective of this firewall is to make all traffic physically pass through the firewall.

**Screened Subnet Firewalls:** This architecture provides a Demilitarized Zone consisting of two or more internal bastion hosts. Each individual bastion hosts are trusted to be protected.

Access Control

* **I*dentification:****is a mechanism that gives info concerning associate degree unproved entity that wishes to access to a well-known entity*

* ***Authentication:****is the method of verifying the alleged identity of a provider.*

* ***Authorization:****is a security mechanism wont to verify user privileges or access levels associated with system resources.*

* ***Accountability:****ensures that all system actions can be attributed to an authentic identity.*

Encryption

**Symmetric Encryption:** The key used by the sender for encryption and receiver for decryption is same and shared.

**Asymmetric Encryption:**uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys.

\* Two keys are used in this encryption, **Private Key** and **Public Key**.

**- Public Key** is used for encryption at the sender's end.

**- Private Key** is used for decryption at the receiver's end.

Authentication

**Knowledge:** It is something the user knows and remembers. For example, remembering an ATM PIN (or) Google Account Password.

**Possession:** It is something the user should have to authenticate him . For Example, OTP while making a transaction.

**Inherence:** It is a unique characteristic of only one user and none of the other users has the same. For example, Fingerprint, Voice/Face Recognitoin, etc..

**Location:** It is about where the user is. For example, detecting user's location with IP Address.

Info sec certificates

* Certified Information Systems Security Professional (CISSP)
* Systems Security Certified Practitioner (SSCP)
* Certified Secure Software Lifecycle Professional (CSSLP)
* Certified Information Security Manager (CISM)
* Certified Information Security Auditor (CISA)
* Certified in the Governance of IT (CGEIT)
* Certified in Risk and Information Systems Control (CRISC)

Infosec positions

* Chief Information Security Officer (CISO)
* Security manager
* Security Technician