SOS POLITICAL SCIENCE AND PUBLIC ADMINISTRATION
JIWAJI UNIVERSITY, GWALIOR

MBA FA IV SEM

PAPER- FA 402

SUBJECT NAME: E-BUSINESS AND CYBER LAW

TOPIC NAME: DATA SECURITY

- Data is any type of stored digital information
- Every company needs places to store institutional knowledge and data.

- Frequently that data contains proprietary information
  - Personally Identifiable Data
  - Employee HR Data
  - Financial Data

- The security and confidentiality of this data is of critical importance.

AVAILABILITY

- Data needs to be available at all necessary times
- Data needs to be available to only the appropriate users
- Need to be able to track who has access to and who has accessed what data

- Security is about the protection of assets.
- Prevention: measures taken to protect your assets from being damaged.
- Detection: measures taken to allow you to detect when an asset has been damaged, how it was damaged and who damaged it.
- Reaction: measures that allow you to recover your assets.

Security Policy

- . A security policy is a comprehensive document that defines a companies' methods for prevention, detection, reaction, classification, accountability of data security practices and enforcement methods.
- It generally follows industry best practices as defined by ISO 17799,27001-02, PCI, ITIL, SAS-70, HIPPA , SOX or a mix of them.

- The security policy is the key document in effective security practices.

- Once it has been defined it must be implemented and modified and include any exceptions that may need to be in place for business continuity.

- All users need to be trained on these best practices with continuing education at regular intervals.

TOOLS TO SECURE DATA

- Data needs to be classified in the security policy according to its sensitivity.
- Once this has taken place, the most sensitive data has extra measures in place to safeguard and ensure its integrity and availability.
- All access to this sensitive data must be logged.
- Secure data is usually isolated from other stored data.

- . Controlling physical access to the data center or area where the data is stored.

- Active or Open Directory is a centralized authentication management system that is available to companies to control and log access to any data on the system.

- Encryption of the sensitive data is critical before transmission across public networks

- The use of firewalls on all publicly facing WAN connections.
- Deploying VLANs’ and ACLs’ to isolate sensitive departments from the rest of the network.
- Shutting down unused switch ports.

- If wireless is deployed, use authentication servers to verify and log the identity of those logging on.

- Anti-Virus and malicious software protection on all systems.

SECURITY OVERVIEW

- . There are four key issues in the security of databases just as with all security systems

  - Availability
  - Authenticity
  - Integrity
  - Confidentiality

AVAILABILITY

- Data needs to be available at all necessary times

- Data needs to be available to only the appropriate users

- Need to be able to track who has access to and who has accessed what data

AUTHENTICITY

- . Need to ensure that the data has been edited by an authorized source
- Need to confirm that users accessing the system are who they say they are
- Need to verify that all report requests are from authorized users
- Need to verify that any outbound data is going to the expected receiver

INTEGRITY

- . Need to verify that any external data has the correct formatting and other metadata
- Need to verify that all input data is accurate and verifiable
- Need to ensure that data is following the correct work flow rules for your institution/corporation
- Need to be able to report on all data changes and who authored them to ensure compliance with corporate rules and privacy laws.

CONFIDENTIALITY

- . Need to ensure that confidential data is only available to correct people
- Need to ensure that entire database is security from external and internal system breaches
- Need to provide for reporting on who has accessed what data and what they have done with it
- Mission critical and Legal sensitive data must be highly security at the potential risk of lost business and litigation

THANK YOU