3. System Analisis and Design

Munawar, PhD

Information Security (Definition)

- Preservation of confidentiality, integrity and availability of information.
- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability).
- Information Security is the process of protecting the intellectual property of an organization
- Information security is a risk management discipline, whose job is to manage the cost of information risk to the business

Basic Prinsiples of Information Security

- Integrity : maintaining and assuring the accuracy and consistency of data over its entire life-cycle. It means data cannot be modified in an unauthorized or undetected manner.
- Availability: the information must be available when it is needed at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.
- Authenticity: the data, transactions, communications or documents (electronic or physical) are genuine.
- Non-repudiation: one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction

Risk Management

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization. (CISA, 2006)

Risk Management Process

- Identification of assets and estimating their value.
- Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, and malicious acts originating from inside or outside the organization.
- Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
- Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
- Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
- Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.

Information Security Classification

- In the business sector, labels such as: Public, Sensitive, Private, and Confidential.
- In the government sector, labels such as: Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret, Top Secret and their non-English equivalents.
- In cross-sectoral formations, the Traffic Light Protocol, this consists of: White, Green, Amber, and Red.

Security Governance

- An enterprise-wide issue
- Leaders are accountable
- Viewed as a business requirement
- Risk-based
- Roles, responsibilities, and segregation of duties defined
- Addressed and enforced in policy
- Adequate resources committed
- Staff aware and trained
- A development life cycle requirement
- Planned, managed, measurable, and measured
- Reviewed and audited

System Testing

- Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements.
- to detect any inconsistencies between the software units that are integrated together (called assemblages) or between any of the assemblages and the hardware.

Testing the Whole System

- Functional Requirement Specification(s) (FRS)
- System Requirement Specification (SRS).

System Testing

- GUI testing → meets its written specification
- Usability Testing → testing it on users
- Software Performance Testing → responsiveness & stability
- Compatibility Testing → compatibility with the computing environment
- Load Testing →to determine a system‘s behavior under both normal and anticipated peak load conditions.
- Volume Testing →testing the software application with a certain amount of data to test the application's performance on it.

System Testing (cont'd)

- Stress Testing →thorough testing used to determine the stability of a given system or entity.
- Security testing →to reveal flaws in the security mechanisms of an information system that protect data and maintain functionality as intended. It may include specific elements of confidentiality, integrity, authentication, availability, authorization and non-repudiation.
- Scalability testing →to test user load, concurrent connections, transactions, and throughput of many internet services.
- Sanity Testing → to quickly evaluate whether a claim or the result of a calculation can possibly be true.

Error Correction

- Automatic repeat request (ARQ). This is an error control technique whereby an error detection scheme is combined with requests for retransmission of erroneous data.
- Forward error correction (FEC): The sender encodes the data using an error-correcting code (ECC) prior to transmission.
- ARQ and FEC may be combined, such that minor errors are corrected without retransmission, and major errors are corrected via a request for retransmission: this is called hybrid automatic repeat request (HARQ).

Thank You !

Munawar, PhD