6 March Afternoon

06 March 2020 16:10

Cognizant (Data Security)

Mr. Vijay Bhaskar
Mr. Harish

Info sec - 5Ws: What, Why, Who, When, Where
- Who is responsible
- When : What is the right time to address info sec
- Where should it be applied

CIA - Confidentiality, Integrity, Availability

Top Down Approach
- Business Owner / Stakeholder / Senior management who has interest in company
  - Accountable for info sec
- Business Unit Leaders
  - Guys who make money out of business
  - Making money is primary objective, protecting the info is secondary
  - Responsible for InfoSec
- Employees
  - Responsible for InfoSec
- Third Parties
  - Contractors and vendors who have access and must protect the business. These requirements should be included in the contractual agreement

Data Management
- Data Classification
- Information Lifecycle Management (ILM)
  - A tool for categorization of data to enable/ help organizations to effectively answer the following
    - What data types
    - Where are certain data located
    - Access levels
    - What protection level, adhere to compliance regulations

Types of Data
- Sensitive Data
  - Example: Personally Identifiable Information, Medical records
- Confidential Data
  - Medical records stored with the govt should be considered confidential
- Proprietary Data
- Public Data

Data Classification
- Regulatory requirements
- Strategic/Proprietary worth
- Organization Specific Policies
- ethical and Privacy considerations
- Contract Agreements

Laws and Regulations
- Act: set of rules that get passed through legislations
- Law: System of rules which the country/org recognizes as regulating the actio
- Policy: A course or principle of action adopted or proposed by the organizatio individual
- Standard: Level of quality

Some Laws
- Sarbanes-Oxley Act (SOX)
  - Stock Market Data Security (By Security and Exchanges Commission of US)

SSAE 16 - SOC (Data Center Security)
- Payment Card Industry Data Security Standard (PCI DSS)
- Gramm-Leach-Bliley (GLB) Act
  - Financial Institutions
  - Personal Financial Data
  - 3 Rules
    - Financial Privacy Rule
      - Give privacy notices to customers etc. (Read from other sources)
    - Safeguard Rule
    - Pretexting Provisions
      - Prevent customers from getting their data by using false pretences
- FISMA (Federal Information Security Management Act)
  - Procedures for detecting, reporting and responding to security incidents
- NIST (National Institute of Standards and Technology)
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
  - (See sub areas for each)

CIS - Center for Internet Security
- Non profit org
- Mission to identify, develop, promote and sustain best practices
- See List of Standards online

ISO 27000 Series
- Implementation
- Auditing

Controls of ISO27000

Case Study - I
- Organization Internally
  - InfoSec, Segregation Duty
- Mobile Usage and remote working
- Termination and change of employment
- Memory and Media Handling
  - Management if removable media
  - Disposal of media
  - Physical Media transfer
- Exclude - Protection from Malware
- Communication Security