CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-1-policies_plans_and_procedures
Title: Policies, Plans, and Procedures
Subtitle: CompTIA Security+ (SY0-501)

5.1 Policies, Plans, and Procedures

- 5.1 Explain the importance of policies, plans and procedures related to organizational security.
    - Standard operating procedure
    - Agreement types
        - BPA
            - Sets the terms and conditions for the partnership
            - Establishes the responsibilities of each business partners
            - Can define
                - Duration of the partnership
                - Decision-making process
                - Liability
        - SLA
            - Contract between a service provider and an end user or business
            - Defines what the acceptable level of performance is
            - Can define
                - Quality of service
                - Availability
                - Responsibilities
                - Usage statistics
                - Plans for addressing downtime
                    - Outages
                    - Service Credits
                    - Compensation
        - ISA
            - NIST SP 800-47
                - Defines technical and security requirements (VPN, authentication mechanisms, encryption) for establishing, operating and maintaining a connection between two organizations
        - MOU/MOA
            - Defines responsibilities of two parties or what the parties will contribute to a partnership. It defines the details of cooperation between two companies that have a common goal.
            - Not legal binding
    - Personnel management
        - Mandatory vacations
            - Seek to uncover malicious activities of employees
            - Five consecutive workdays
        - Job rotation
            - Gives employees a larger skill set
            - Helps with cross-training
            - Ensures that not a single employee retains
        - Separation of duties
            - Having more than one person to complete a task
            - Restricting the power a single person has
        - Clean desk
            - A clean desk policy can be an import tool to ensure that all sensitive/confidential materials removed from an end user workspace and locked away
            - http://bit.ly/2oYBqFi
        - Background checks
            - Part of the employment screening process
            - Often performed when the candidate is seeking a position of trust or high degree of security
        - Exit interviews
            - These are performed as an employee is leaving an organization
            - Gives the organization a chance to understand the reasons (constructive feedback)
            - Allows the employee the change to leave on a good note
        - Role-based awareness training
            - Data owner
                - Defining the information
                - Assigning value to the data
                - Defining the level of protection
                - Deciding who should have access
            - System administrator
                - Understanding secure system configuration
                - Protection of information
                - Understanding of industry-standards

  - System owner
    - Best practices
  - User
    - Computer security basics
    - Policies and Procedures
  - Privileged user
  - Executive user
    - Management
    - Compliance
    - Development of policies
    - Risk-factors
- NDA
- Onboarding
- Continuing education
  - Reduces the number of security breachs as it promotes awareness
  - Security training needs to adapt new technologies and trends
  - Promotes continued participation
  - SETA (Security, Education, Training and Awareness)
  - Helps to promote employee awareness and competency
- Acceptable use policy/rules of behavior
- Adverse actions
  - General security policies
  - Social media networks/applications
  - Personal email