CompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-3-risk_management_processes_and_concepts
Title: Risk Management Processes and Concepts
Subtitle: CompTIA Security+ (SY0-501)

5.3 Risk Management Processes and Concepts

- 5.3 Explain risk management processes and concepts.
    - Threat assessment
        - Environmental
            - Climate Control
                - Humidity = High/Low
                - Temperature = High/Low
                - Water Leaks
                    - Rain/Flooding
                    - Plumbing
        - Manmade
            - Malware (all inclusive)
            - Cyber Attacks
            - Physical security attacks
            - Misconfiguration of systems, apps, ACls
            - Misuse of passwords, social media, email
        - Internal vs. external
            - Internal
                - Lack of training equates to user error
                - Malicious insider
                - Data Leaks (Unintentional/Intentional)
            - External
                - Hacktivist, nation states, competition, malicious insiders
                - Business data on company devices
                - Reputation-based attacks
                    - Social Media
                    - Websites
                - Mobile Exploitation
                    - Lack of encryption
                    - Malware
                    - Phishing
                    - Social Media
                    - Untrusted application sources
                    - Developer option(fun but not without risk >>damage >>> consequences)
    - Risk assessment
        - SLE
            - Single Loss Expectancy
            - (SLE) = Asset Value(AV) x Exposure Factor (EF)
            - (AV) Asset Value = What is the value of an asset to a company
            - (EF) Exposure Factor = % of damage to an asset
            - What is the maximum value the company will pay for the asset
        - ALE
            - Annual Loss Expectany
            - The expected monatary(cost) loss for an asset over time
            - ALE = SLE * ARO
        - ARO
            - Annual/Annualized Rate of Occurence
            - Probability of an annual risk event
            - Or the frequency in which the event happens
        - Risk register
            - List of identified risks. The identified risks are described in as much detail as is reasonable.
            - Risk Log
            - Contains:
                - Description of the risk
                - Impact of the event should it happen
            - List of planned or potential responses.
            - Use case scenario
                - Used in projects
                - Used in programs
                - Used in companies
        - Likelihood of occurrence
            - Probability of a risk event happening
            - This defines the probability of a specific threats to exploit a given vulnerability, based on a subjective analysis

        - Might be called Probability of Occurence
    - Supply chain assessment
    - Impact
        - Consequences including cost, time , performance , functionality
        - Potential effects on the company
    - Assessments
        - Reason
            - Determining what is valuable to the company through QUAL/QUAN Assessments
        - Types
            - Quantitative
                - Assigns cost or monetary value to assets, threats, processes
            - Qualitative
    - Testing
        - Penetration testing authorization
        - Vulnerability testing authorization
    - Risk response techniques(or strategies)
        - Accept Strategy
            - First in the list of objectives
            - Last in the list of response techniques
            - When no other strategy will work
            - Acceptance requires no immediate reaction
        - Transfer Strategy
            - Find another party that is willing to take on the risk, responsibility, management
            - Owned by a party that charges payment
            - Cosideration made on cost effectiveness
        - Avoid Strategy
            - remove the cause of the risk
            - not all risks can be avoided
        - Mitigate Strategy
            - Reducing risk to the lowest acceptable level
            - Reduces impact to acceptable levels
            - Minimalize risks/impact
- Change management