daCompTIA Security + 5.0 Risk Management

Filename: comptia-secplussy0501-5-6-disaster_recovery_and_business_continuity
Title: Disaster Recovery and Business Continuity
Subtitle: CompTIA Security+ (SY0-501)

5.6 Disaster Recovery and Business Continuity

- 5.6 Explain disaster recovery and continuity of operation concepts.
    - Recovery sites
        - Hot site
            - Fully functional replica site that can process and syncronize data between the two sites
            - Infrastructure is in place and functional
            - Site is preloaded with operating systems, applications, hardware
            - Expensive
                - Power/Utilities
                - Staffing
                - Management
                - Land Use
            - Downtime is minimalistic if even applicable
        - Warm site
            - Basic infrastructure is in place but site is not fully functional
            - Few critical systems may be provisioned
            - Operating system might only be installed on a handful of critical systems
            - Application may or may not be setup/installed on a few critical components
            - Warm sites might contain a backup of the organizations data in the event of site activation
            - Time to bring a warm site online can be a few hours to a few days
        - Cold site
            - These are used for long term outages on the primary
            - Basic infrastructure
                - HVAC
                - Network connectivity
            - Aquisition of hardware, building the systems, application installation, data restoration
            - Least expensive to maintain
            - Restore time is at minimum, measured in days but most likely weeks
            - Can be nothing more than a prospected site with a guarentee of access when needed (in the)
        - Hybrid(Optional)
    - Order of restoration
        - Restoration of systems needs to be done to meet the needs of the company
        - Critical Systems
        - Power >>> HVAC >> Server Room >> Hardware >>> Security >>> Connection to ISP >> Software applications >> Data Restoration
    - Backup concepts
        - Differential
        - Incremental
        - Snapshots
        - Full
        - Considerations
            - Scheduled
            - Performing
            - Validating
    - Geographic considerations
        - Off-site backup
            - Used in case of a disaster
            - Requires a different physical location
        - Distance
            - If a natural disaster happens is the DR site far enough away from the primary site to continue to function
            - Some say 1000 miles is the comfort zone others reduce that to 100 - 25 miles.
            - Distance can ensure a disaster does not affect both primary and secondary but may introduce latency
        - Location selection
            - Level of preparedness of the site
            - Cost
            - Distance to the primary site
            - Accessibility to the site
            - The Recovery Time Objective might influence the decision
            - **RTO** - *the ideal time that is needed to restore a function or service after an interruption*
            - **RTO** - *The maximum amount of time before an organization is negatively impacted by that interruption- how long can we go?*
            - **RPO** - *Focused on the amount of data loss is allowable*
            - **RPO** - *The maximum tolerable period in which data may be lost/backup frequency*
            - **RPO** - *Typically measured from the last successful backup*

        - **RPO** - *If the maximum allowed time is 5 hours or RPO of 5 hours, then backups need to be run every 5 hours at least*
    - Legal implications
        - Privacy becomes a challenge
        - Juristiction can change with different geographical location
        - Example
            - The exporting of European users PII and storing it on US-based servers is not allowed
            - This was controlled orignally by the US-EU Safe Harbor program
            - As of revelations by the Snowden leaks showing the NSA was spying on data held on US-based servers the program was invalidated by the EU
    - Data sovereignty
        - Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located.
        - important for cloud computing
        - Privacy and Compliance
        - SLAs are important
- Continuity of operation planning
    - Exercises/tabletop
        - Exercises
            - Testing out the BCP in a non threating emergency
            - Employee training and preparation
            - Good for:
                - Evaluation of affectiveness/preparedness
                - Identify deficiencies in the steps
                - Ensure clear understanding of roles and responsibilities
                - Improve coordination
                - Assess the capabilities of existing resources or need for additional resources
        - Tabletop
            - Discussion-based informal sessions between team members
            - Can be typically completed in 2 hours or so
            - Contrast to a Functional excercise which allow personnel to validate plans and readinessby performing their role repsonsibilities.
    - After-action reports
        - professional discussion of and event. focused on performance
        - Analytical retrospect of an event happening, why it happened, where it happened and who it happen to
    - Alternate processing location
        - Might reduce thte cost
        - Identify daata/telecommunication req.'s
        - Identiy environmeental req's.\
        - ID personel requirements
    - Alternate business practices