Cloud Compliance Concepts

4.2 Compare and Contrast Aspects of Compliance and Regulation

Description

- In this episode, we will explore many of the terms and concepts that are relevant to the world of compliance and regulation

Resources

- https://gdpr-info.eu/
- https://www.govinfo.gov/content/pkg/PLAW-107publ204/html/PLAW-107publ204.htm
- https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

Learning Objectives

- List and define common terms and concepts related to compliance and regulation

Notes

- Data Sovereignty
    - The idea that different jurisdictions have the right to impose authority and govern data within said jurisdiction
        - Some require that the data is generated within a jurisdiction
            - And that data is processed and stored within that border
            - Ramifications for data-flows that cross borders
- Data Ownership
    - Similar to Sovereignty
    - Ownership focuses on PERSONAL owership and control
        - Sovereignty focuses on GOVERNMENTAL control
- Data Locality
    - Residency
        - Where the data is stored PHYSICALLY
            - Data stored closer to clients increases performance
            - May increase storage and access charges due to necessarily storing data in multiple locations
    - Localization
        - Requiring certain data to be stored and processed within a specific jurisditional border
            - Data sensitive to national security interests
            - Regulatory compliance
- Data Classification
    - What kind of data is this?
        - Sensitivity level with regards the Confidentiality and Integrity (sometimes Availability)
            - Types
                - Content-Based
                    - The CONTENT in the documents is what defines its sensitivity/classification
                - Context-Based
                    - The CONTEXT around the data is what defines its sensitivity/classification
                - User-Based
                    - The sensitivity/classification is set by the user at the user's discretion

- The user relies on their intimate knowledge of the data for final judgement
- Common Classifications
    - Public
    - Internal
    - Restricted
    - Confidential
    - Sensitive
    - Confidential
    - Secret
    - Top Secret

- Data Retention
    - Legal Hold
        - Triggering Event
            - A legal event is about to happen
                - Litigation
                - Gov Investigation
                - Audit
        - Scope
            - The data relevant to the case
        - Notification
            - Relevant persons are notified of the hold and instructed how to proceed and proctect data
        - Data Preservation
            - Making sure that the relevant data is not destroyed/corrupted
                - Secure Backups
        - Monitoring
            - Ensures that the relevant parties are compliant with legal hold instructions
        - Release
            - Control of data is returned to original party
        - Exchange PowerShell M365 - `Set-Mailbox <username> -LitigationHoldEnabled $true`
    - Contractual
    - Regulatory
        - FISMA - 3 years
        - ISO 27001 - 3 years
        - SOX - 7 years
        - HIPAA - 6 years