Overview of Best Practices for Protecting Sensitive Information - Summary

Jonathan R. Razo

July 17, 2012
Overview:

- This session will provide an overview of how organizations are being challenged implementing effective policies and security controls to protect their most sensitive and confidential information both internally and externally.

- Challenges such as classifying and restricting information appropriately, emergence of collaborative technology such as social networks, ineffective policies, among other factors, amplifies this problem.

- Lastly, this presentation will highlight best practices that organizations need to consider when implementing a framework for the identification of sensitive information, including management sponsorship and ownership, baselines, and security controls.
Protecting Sensitive Data - Business Case

- **Business Reason:**
  - Researchers need to work with sensitive data such as Protected Health Information (PHI).
  - Note: This information handling is regulated by the Health Insurance Portability and Accountability Act (HIPAA)

- **Goal:**
  - Provide a common solution for the division to handled the information security and in a controlled environment:
    - Protect individual privacy
    - Simplify compliance process
    - Minimize exposure

- **Challenges:**
  - Conflicts between different country and regional privacy laws
  - Burdensome compliance process
  - Tool development
  - Scope of each project (e.g. de-identified versus use of all data)
Current environment

- **Explosion of virtual and mobile devices:**
  - Information is not always limited to a specific location or device
  - Ownership of the devices and legal/privacy implications

- **Openness:**
  - Social networks
  - Data leakage
  - Lack of guidance

- **Collaboration:**
  - Both internally & externally
  - Data ownership/Intellectual Property
Sensitive Data Identification and Classification

- **Challenges:**
  - Lack of formal data identification processes/framework
  - Data inventories not kept up-to-date or non-existent
  - Mandated compliance to external regulatory laws (PHI-HIPAA, ITAR, Exports, Privacy, etc.)
  - Time-based sensitivity
  - Openness and flexibility
  - Cloud versus physical servers hosting

- **Best Practices:**
  - Finding the right balance between what is sensitive/confidential in each organization to avoid over- or under-classification that can lead to inappropriate protection levels.
    - Define a subset of classification categories (labels).
    - It’s easier to begin simple and then add additional categories based on your organizations needs. For example:
      - Most sensitive
      - Sensitive
      - Non-sensitive
Sensitive Data Identification and Classification

- Need Senior Management Sponsorship:
  - Senior Management sponsorship and mandate for the overall organization
  - Sets the common policy (instruction, standard, guidance) that needs to be followed to consistently protect information across the organization

- Assignment of Data Stewards across the organization to:
  - Oversee/perform the discovery and inventory management of sensitive information
  - Define additional discretionary security controls
  - Determine revalidation process frequency to assess if information still needs this level of control or is no longer sensitive (de-classification)
  - Ensure governance & compliance, and data retention

  - Guidance example: University North Carolina - Chapel Hill
    - [http://help.unc.edu/6446](http://help.unc.edu/6446)
Best Practices

- **Proactive access monitoring management:**
  - Who is accessing information?
  - Requires real-time analysis of system, application, and network logs to analyze and alert when unusual access behavior/pattern is detected

- **Security breaches/leakages:**
  - Proactive identification of Security breaches/incidents (e.g. malware, phishing)
  - Implement controls at each layer (network, server, endpoint, application, and data)
  - Implement a formal process for end-to-end management of security incidents

- **Education:**
  - Implement a program to periodically educate individuals how they need to secure sensitive information organization.
    - It can be part of the annual certification program
    - Useful to highlight changes to both internal and external policies
  - Begin by targeting your most critical individuals working with this sensitive information
Best Practices

- **Compartmentalization:**
  - Who has a need to access what information?
  - Common problem today is that individuals are granted unrestricted access to data
  - Partition information repository or enable application controls to restrict what individuals can access per their need to know (including physical and logical location)
    - Firewalls, VLANs, private networks, etc.

- **Hosting of Information:**
  - Risk increases as information is hosted outside the organization domain
  - Need to identify which information can be hosted in each zone
  - Assess what additional security controls and frequency of supporting processes execution are needed
Best Practices

- **Access Controls:**
  - Perform need to know revalidations on a continuous basis (based on your risk tolerance level)
  - Expedite access deletion of individuals no longer involved with projects
  - Revoke external/remote access for individuals no longer employ with your organization
  - For your most sensitive information, assess how frequently you need to perform these access revalidation and revocation.
  - Other technical controls:
    - Time tokens

- **De-identification & Anonymization of data:**
  - For some types of data, compliance and risks are minimized through de-identification or anonymization of the data.
    - Examples: PHI/HIPAA data
  - In our experience, individuals like to work with real data for cases where they just need to do number crunching/data analytics.
    - Establish a review board team to assess when there is a valid need to actually work with real data and share accountability for the risk taken among all teams involved.
Best Practices

- **Server, Application, Endpoint Security:**
  - Where and how information is being accessed?
  - Some organization allow individuals to store business/enterprise/university data onto personally-owned devices.
    - Is that the right policy for your organization?
  - Security Controls:
    - Technical controls to wipe or have information expire, if asset is compromised
    - Assign who access and check out information (for data leakage)
    - File-level, full hard drive, and data repository encryption enablement
  - Comprehensive Security Policy
    - Define mandatory security controls. For example, what products or tools have been approved:
      - Encryption
      - Antivirus
      - Firewall
      - Passwords (e.g. harddrive, account, power-on)
      - Secure transmission and protection of information (SSL, ssh, sftp)
    - For specific types of sensitive information, for example, not all devices can be used
    - Data retention and disposal
Questions:

- ?’s