DMBoK Data Security Framework Exploration & Implementation

Objective: To help you understand and implement the Data Security Framework from DMBoK using real-world examples and interactive tools.

Duration: 1 hour and 30 minutes

Requirements:

1. Access to the internet
2. Laptops or computers for each group
3. DMBoK Data Security Framework (provided to you)
4. Access to the following websites:
    - https://haveibeenpwned.com/
    - https://www.sha1-online.com/
    - https://crackstation.net/
    - https://www.browserling.com/tools/random-password
    - https://www.playgroundai.com/

Activity Breakdown:

Part 1: Hands-on Exploration of Data Security (45 minutes)

1. Form groups of 2-3 students.
2. Each group should choose one data breach case from the following list:
    - Equifax: https://en.wikipedia.org/wiki/Equifax#2017_data_breach
    - Target: https://en.wikipedia.org/wiki/2013_Target_data_breach
    - Yahoo: https://en.wikipedia.org/wiki/Yahoo!_data_breaches
3. Research your chosen data breach case and identify the main causes and consequences. Take notes for a brief presentation later.
4. Visit the following websites and complete the tasks listed below:

a) HaveIBeenPwned (https://haveibeenpwned.com/):

- Check if any of your personal email addresses have been compromised in a data breach.
- Identify which breaches the email addresses have been involved in and the types of data compromised.

b) SHA1-Online (https://www.sha1-online.com/):

- Create a simple text password and generate its SHA1 hash.

- Discuss the importance of hashing and why it's crucial for password storage.

c) CrackStation (https://crackstation.net/):

- Attempt to crack the previously generated SHA1 hash to recover the original password.
- Discuss the limitations of hashing and how to improve security (e.g., using stronger hashing algorithms, adding salt).

d) Browserling's Random Password Generator (https://www.browserling.com/tools/random-password):

- Generate a random, strong password.
- Discuss the characteristics of a strong password and why it's essential for data security.

5. Compile your findings and prepare a brief presentation on the data breach case and the hands-on tasks you completed.

Part 2: DMBoK Data Security Framework Implementation (45 minutes)

As a group, study the DMBoK Data Security Framework provided to you. Familiarize yourself with the key components and principles.

Use the knowledge gained from Part 1 and the DMBoK Data Security Framework to analyze your chosen data breach case. Identify which aspects of the framework were inadequately addressed or missing in the case.

Create a revised data security plan for the breached organization, incorporating the DMBoK Data Security Framework. Your plan should include the following:

a) Risk assessment and mitigation strategies

b) Data classification and protection

c) Access controls and identity management

d) Encryption and secure data storage

e) Monitoring and incident response

Use Mermaid.js (https://mermaid-js.github.io/mermaid/#/) to create a visual representation (flowchart or diagram) of your revised data security plan, highlighting the key components and their relationships.

As a group, present your findings from Part 1 and your revised data security plan from Part 2. Discuss how the DMBoK Data Security Framework can help prevent similar data breaches in the future.

After all group presentations, engage in a class-wide discussion about the challenges organizations face in implementing the DMBoK Data Security Framework and potential solutions.

Conclusion:

This hands-on, interactive group activity aims to provide you with a practical understanding of data security and the DMBoK Data Security Framework. By analyzing real-world data breach cases and applying the framework to create a revised data security plan, you'll gain valuable insights into the importance of data security and how to implement it effectively.