**Assignment 2-3 Activity:**

**Data Protection Case Study**

Matthew A Keaton

Southern New Hampshire University

CYB 200: Cybersecurity Foundations

Professor Linda Hamons

March 17, 2024

# CYB 200 Module Two Case Study Template

After reviewing the scenario in the Module Two Case Study Activity Guidelines and Rubric document, fill in the table below by completing the following steps for each control recommendation:

1. Specify which Fundamental Security Design Principle best applies by marking all appropriate cells with an *X*.
2. Indicate which security objective (confidentiality, availability, or integrity) best reflects your selected control recommendation.
3. Explain your choices in one to two sentences, providing a selection-specific justification to support your decision.

| **Control Recommendations** | **Least Privilege** | **Layering (Defense in Depth)** | **Fail-Safe Defaults / Fail Secure** | **Modularity** | **Usability** | **Security Objective Alignment (CIA)** | **Explain your Choices (1-2 sentences)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Automatically lock workstation sessions after a standard period of inactivity. (Completed as an example) |  | X |  |  |  | C | I chose layering because it adds another layer of protection for the confidentiality of our data. |
| If possible, close and lock your office door when leaving your computer. |  | X | X |  |  | C  A | I chose Fail-Safe Defaults because unless given access it should be denied and Layering because having multiple forms of security for hardware. |
| Use technology to make sure that only authorized software executes, and unauthorized software is blocked from executing on assets. | X | X |  |  |  | I | I chose Least Privilege because only authorized software should execute and Layering because extra security to block unauthorized software from executing. |
| Use automated tools to inventory all administrative accounts to ensure that only authorized individuals have elevated privileges. | X |  |  |  |  | I | I chose Least Privilege because only authorized users should have minimal amount of privileges to perform their duties. |
| Use system configuration management tools to automatically reapply configuration settings to systems at regularly scheduled intervals. |  | X |  |  |  | I | I chose Layering because using system configuration management tools is an extra layer of security. |
| Maintain an inventory of all sensitive information stored or transmitted by the organization's technology systems, including those located on site or at a remote location. |  |  |  | X |  | C  I  A | I chose Modularity because maintaining and organizing sensitive information can be broken down into smaller tasks making it easier to secure. |
| Use approved whole-disk encryption software to encrypt the hard drive of all mobile devices. |  | X |  |  |  | C  I | I chose Layering because adding encryption adds extra layer of security. |
| If USB storage devices are required, software should be used that can configure systems to allow the use of specific devices. | X |  |  |  |  | C  I | I chose Least Privilege because access should be given to only those authorized to use USB devices. |
| Configure systems not to write data to external removable media, if there is no business need for supporting such devices. | X |  |  |  |  | C  I | I chose Least Privilege because only minimal amount of privilege should be given. If there is no need then don’t do it. |
| If USB storage devices are required, all data stored on such devices must be encrypted. |  | X | X |  |  | C  I | I chose Fail-safe Defaults because unless given access in should be denied and Layer because encryption adds a layer of security. |
| Protect all information stored on systems through the use of access control lists. These access control lists enforce the principle that only authorized individuals should have access to the information based on approved business need. | X | X |  |  |  | C  I  A | I chose Least Privilege because only authorized users should have minimal access to perform duties and Layering because this adds an extra layer of security. |
| Require multifactor authentication for all user accounts, on all systems, whether managed on site or by a third-party provider. |  | X |  |  |  | C  I | I chose Layering because adding an MFA adds an extra layer of security. |

After you have completed the table above, respond to the following short questions:

1. How might you work with someone like Dr. Beard to cultivate a security mind-set that is more in line with the organization’s ethical norms? Hint: Consider his attitude, his past behaviors, and his opinion about organizational policies.

Working with someone like Dr. Beard to cultivate a security mindset we can start by educating Dr. Beard about the importance of cybersecurity and the potential consequences of security breaches, specifically in a healthcare environment where patient confidentiality is extremely important. Helping them become more aware and understanding of the importance of protecting patient data will allow Dr. Beard to be more considerate of their actions. Also, adding leadership from the organization in the loop will help reinforce the importance of security policies and promote a security mindset across a broader workspace. Encouraging open communication and collaboration of all staff members will help address security concerns effectively in the organization.

1. How would you help the hospital better secure its patient files? Make sure to incorporate at least one data state (data-at-rest, data-in-use, or data-in-motion) and one of the control recommendations from your completed table in your response.

To help the hospital better secure its patient files I would focus on data-at-rest security. Data-at-rest is “data in a stable state, not currently being transmitted across a network or actively being read or being used by any application” (Saltzer & Schroeder, 1975). Since patient files are typically sitting around until accessed, data-in-rest would be the best data state to incorporate. Also, incorporating the control recommendation of “Protect all information stored on systems through the use of access control lists. These access control lists enforce the principle that only authorized individuals should have access to the information based on approved business need” would be best for this scenario with Dr. Beard. This control recommendation would allow Dr. Beard access to patient information if approved and for business purposes only, otherwise access will be denied. This also adds a layer of security that would deny Dr. Beard from accessing any patient files that aren’t for business should he try to access any files while working remotely or away from the office.

**Reference**

Saltzer, J., & Schroeder, M. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), 1278-1308. doi:10.1109/proc.1975.9939