**Assignment 3-3 Activity:**

**Privacy Protection Case Study**

Matthew A Keaton

Southern New Hampshire University

CYB 200: Cybersecurity Foundations

Professor Linda Hamons

March 24, 2024

# CYB 200 Module Three Case Study Template

| **Control Recommendations** | **Isolation** | **Encapsulation** | **Complete Mediation** | **Minimize Trust Surface (Reluctance to Trust)** | **Trust Relationships** | **Security Objective Alignment (CIA)** | **Explain Your Choices**  **(1–2 sentences)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals. |  | X | X |  |  | C  I | I chose Encapsulation because this would keep equipment from being used maliciously and complete mediation because this would check if access and transfers are allowed |
| Monitor all traffic leaving the organization to detect any unauthorized use. |  | X |  |  |  | I | I chose encapsulation because this would keep equipment from being used maliciously |
| Use an automated tool, such as host-based data loss prevention, to enforce access controls to data even when data is copied off a system. |  |  | X |  |  | C  I | I chose complete mediation because this would check all access and ensure they’re allowed. |
| Physically or logically segregated systems should be used to isolate higher-risk software that is required for business operations. | X |  |  | X |  | C | I chose isolation because this will keep resources from interfering with other processes and minimize trust surface because this reduces the degree which components rely on other components |
| Make sure that only the resources necessary to perform daily business tasks are assigned to the end users performing such tasks. | X |  |  |  |  | A | I chose isolation because this allows processes to have enough resources to run |
| Install application firewalls on critical servers to validate all traffic going in and out of the server. |  | X |  |  |  | C  I | I chose encapsulation because this would keep equipment from being used maliciously |
| Require all remote login access and remote workers to authenticate to the network using multifactor authentication. |  |  | X |  | X | C  I  A | I chose complete mediation because this would check all access and ensure they’re allowed and trust relationships because the rights and privileges are shared among all remote workers. |
| Restrict cloud storage access to only the users authorized to have access, and include authentication verification through the use of multi-factor authentication. |  | X | X |  |  | C  I | I chose encapsulation because this would keep equipment from being used maliciously and complete mediation to ensure and check that access is allowed |
| Make sure all data-in-motion is encrypted. |  | X |  |  |  | C  I | I chose encapsulation because this would keep equipment from being used maliciously |
| Set alerts for the security team when users log into the network after normal business hours, or when users access areas of the network that are unauthorized to them. |  | X | X |  | X | C  I | I chose encapsulation because this would keep equipment from being used maliciously and complete mediation to ensure and check that access is allowed and trust relationships because the rights and privileges are shared among all workers. |

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

1. Is it possible to use DataStore and maintain an **isolated environment**? Explain your reasoning.

No, it is not possible to use DataStore and maintain an isolated environment. An isolated environment would have “individual processes or tasks running in their own space” (Tjaden, 2015). This would not be able to be achieved within a shared cloud storage service like DataStore where a cloud-based data service operates on a shared infrastructure.

1. How could the organization have more effectively applied the principle of **minimizing trust surface** with DataStore to protect its confidential data? Explain your reasoning.

The organization could have more effectively applied the principle of minimizing trust surface with DataStore to protect its confidential data by adding access controls, encryption, and monitoring. By applying the principle of minimizing trust surface, helps an organization to reduce the degree of where their components wouldn’t have to rely on other components (Bishop, 2003). Adding access controls, encryption, and monitoring would help the organization to not rely on the components of DataStore as much.

1. How can the organization build a more **security-aware culture** from the top down to prevent mistakes before they happen? Explain your reasoning.

Building a security-aware culture from the top down is crucial for preventing mistakes before they happen in an organization. Senior leaders should prioritize security measures and have clear communication of security policies and procedures. Security professional leaders should define security baseline goals of confidentiality, integrity, and availability while implementing the fundamental security design principles. Implementing fundamental security design principles will help protect assets, mitigate risks, ensure compliance, maintain customer trust, and help achieve business objectives. Doing this will help create a framework in an organization that promotes a more security-aware culture to prevent mistakes from happening before they happen.

**References**

Bishop, M. (2003). Computer security: Art and science. Boston, MA: Addison-Wesley Professional.

Tjaden, B. C. (2015). Appendix 1: Cybersecurity first principles. Retrieved from <https://users.cs.jmu.edu/tjadenbc/Bootcamp/0> GenCyber First-Principles.pdf