Southern New Hampshire University

Module 3 Case Study

Samuel Davidson

CYB-200 Cybersecurity Foundations

Jillian Seabrook

January 21, 2023

Southern New Hampshire University

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			I	As the automated tool checks for sensitive data transfers and blocks unauthorized transfers this is a form of complete mediation, allowing only authorized actions to occur. This in turn helps protect the integrity of the stored data.
Monitor all traffic leaving the organization to detect any unauthorized use.		X				C	Monitoring outbound traffic helps the security team ensure only authorized activities are occurring on the network. This ensures protected data is not being sent outside of the network, thus protecting confidentiality.

Southern New Hampshire University

Control Recommendations	Isolation	Encapsulation	Complete Mediation	Minimize Trust Surface (Reluctance to Trust)	Trust Relationships	Security Objective Alignment (CIA)	Explain Your Choices (1–2 sentences)
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	I	A host-based DLP allows for the administrator to set specific blocks and monitor system details via a direct link of the installed software. This ensures that devices connected to this system are not able to remove or steal data off a connected device.
Physically or logically segregated systems should be used to isolate higher-risk software that is required for business operations.	X					I	The segregated system is an example of isolation, or separating a high risk software from potentially harming other data. This in turn protects the integrity of data stored within the organization's systems.
Make sure that only the resources necessary to perform daily business				X		A	Ensuring only necessary users have access to certain

Control Recommendations	Isolation	Encapsulation	Complete Mediation	Minimize Trust Surface (Reluctance to Trust)	Trust Relationships	Security Objective Alignment (CIA)	Explain Your Choices (1–2 sentences)
tasks are assigned to the end users performing such tasks.							resources allows those resources from becoming slowed down with heavy concurrent use and ensures the availability of the resources when necessary.
Install application firewalls on critical servers to validate all traffic going in and out of the server.			X			C	A strong application firewall allows for the administrator to ensure only authorized access in and out of the network is occurring. This keeps necessary data confidential from unauthorized use.
Require all remote login access and remote workers to authenticate to the network using multifactor authentication.					X	A	The multifactor authentication and login access allows for ensuring the proper privileges are assigned to authorized users. This keeps work-necessary data

Control Recommendations	Isolation	Encapsulation	Complete Mediation	Minimize Trust Surface (Reluctance to Trust)	Trust Relationships	Security Objective Alignment (CIA)	Explain Your Choices (1–2 sentences)
							available even when not in the office.
Restrict cloud storage access to only the users authorized to have access, and include authentication verification through the use of multi-factor authentication.		X				I	Restricting cloud storage prevents an excessive number of users from accessing the stored data, and protects the integrity of cloud-based data.
Make sure all data-in-motion is encrypted.			X			C	Encryption ensures that even if a device is lost or stolen, it will be extremely difficult for a 3rd party to view any stored data. These keeps that data confidential and accessed only by authorized users.
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				C	The security alerts are an example of encapsulation as the security team is able to protect the network for any unauthorized access. This keeps the data

Southern New Hampshire University

Control Recommendations	Isolation	Encapsulation	Complete Mediation	Minimize Trust Surface (Reluctance to Trust)	Trust Relationships	Security Objective Alignment (CIA)	Explain Your Choices (1–2 sentences)
							stored in the organization's systems confidential.

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.
    a. Yes, it is possible to use DataStore and maintain an isolated environment given the data used for DataStore is a separate entity. As stated in the brief, DataStore was used for public based information, thus does not have the need for isolation that the secure customer data will. Holding the customer data in a separate isolated system, and allowing only trained and authorized users access to this secure system allows you to hold a DataStore for the associated public data, and a isolated system for the private data.

2. How could the organization have more effectively applied the principle of **minimizing trust surface** with DataStore to protect its confidential data? Explain your reasoning.
    a. One major consideration for applying the principle of minimizing trust surface would be to ensure someone that was not properly trained in the use of handling secured data did not have access to the data. This ensures that the security of the data does not rely on the action of an individual not taught to handle it. Strong training programs and proper user access policies would be a strong move towards better ensuring the integrity of each system individually.

3. How can the organization build a more **security-aware culture** from the top down to prevent mistakes before they happen? Explain your reasoning.
    a. The best way to ensure a more security-aware culture in the organization is to focus first on training. Strong guidelines on how data should be handled is the best way to ensure the confidentiality of sensitive data, and integrity of highly important information. Further, setting policies on acceptable use, and incorporating monitoring into data transfers and attachments will add additional layers of security for the organization to better protect its systems.