

## **Project Two Scenario**

William Pascoe

CYB-200: Cybersecurity Foundations

Robert Brickan

August 9, 2025

## **Project Two Scenario**

Last week we had an incident in the payroll department. While the payroll administrator was on a coffee break someone entered her office and managed to gain access to her computer. Upon returning from her break, she witnessed the person rushing out of the office with a backpack full of items and an electronic device that was probably used in the attack. We know that several manila folders with unknown contents were taken, the remote logs show that the administrator's computer was accessed and that the payroll report contained some inaccuracies. Because of this event I think we need to reexamine the company's security protocols to ensure data integrity. We also look at security principles that involve fail safe / fail secure and least privilege.

### **Data Integrity**

As part of the CIA triad, integrity is ensuring data is accurate and trustworthy throughout its lifecycle. This includes preventing unauthorized modification or deletion of data, often achieved through checksums, version control, and digital signatures (Hashemi-Pour, 2023). This is relevant to what happened here because the latest payroll report after the breach had some inaccuracies that are currently being investigated by the human resources department. This not only erodes the trust of fellow employees that everything is accurate but also our customers and their data as well. As a financial organization we do not want our clients to be unsure that their financial records are or could possibly be inaccurate.

### **The Fundamental Security Design Principles**

There are two fundamental security principles that I think should be a necessary measure to make sure they are implemented properly and maintained at all levels. These are Fail-safe

defaults / Fail-secure and principle of least privilege. With the Fail-safe /fail secure design we ensure things like computers are locked if not used in a relatively timely manner as well as doors to offices that maintain sensitive information also are locked behind people. The principle of least privilege is used to ensure that only people who need to access sensitive data are to access the information and only at the levels to which they require it.

To implement these principles, we need to first look at access control to make sure that we are giving staff access to information but not to things outside their department or above and below their job description unless it is absolutely needed. This may require a look at roles in which people do for the company to define a standard. To implement the fail safe / fail secure we need to examine computers to make sure they are self-locking if idle for a short amount of time. For people in higher or more secure roles we should look at making offices lock when the door closes and having access control badges to gain access to the office. This will help to keep records of who enters the office at any given time of the day.

### **Balance of impacts**

We do need to find balance in what we do. We don't want to take away everyone's access to all information and lock the building down like a prison. That would help keep data the most secure but would cause frustration for everyone. I think having standardized roles and access creates a level security that isn't impeding people's jobs but shows them that we importance of keeping data secure for the company as well as themselves.

### **Most Critical**

Implementing this whole process will take some time. Often roles tend to get blurred together and creating a standard may be hard or in some cases impossible to do. The fail safe / fail secure procedure should be the easiest and most critical thing we can accomplish. Having the IT dept setup computers to lock out would be something we could do in a relatively short amount of time. Placing access controls on doors and making them self-locking could also be accomplished soon and these two things would allow us to be more secure than we are now and help to start creating a culture of data security. I think we also need to make sure we keep the staff apprised of the situation and the plan we are making to rectify it. This will also help to foster a level of trust and disdain among the employees because they will look at our new security features as a necessary inconvenience rather than company distrust.

### References:

Hashemi-Pour, C. (2023, December 21). *What is the CIA triad (confidentiality, integrity and availability)?* TechTarget. <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>

A, B. (2023, February 18). *Two Concepts To Reason About Safety In System Design Reviews*. Medium. <https://basila.medium.com/fail-safe-versus-fail-secure-584201a7bada>

CyberArk. (n.d.). *What is Least Privilege Access? PoLP Explained*. CyberArk. <https://www.cyberark.com/what-is/least-privilege/>