Conducting a Risk Assessment of an Access Control System (3e)

Access Control and Identity Management, Third Edition - Lab 02

Student: Jacob Jeffers	Email: jjeffers6151@ucumberlands.edu
Time on Task:	Progress: 100%

Report Generated: Friday, May 14, 2021 at 6:40 PM

Guided Exercises

Part 1: Research Risk Assessment Standards

4. **Compare** the requirements for access control systems in the PCI DSS to those in the HIPAA Security Rule. **Describe** the level of detail found in each standard and how each standard might be easier and more challenging to meet compared with the other.

The PCI DSS requirements are much more detailed than the HIPAA requirements. For example, PCI DSS requires the use of firewalls and encrypted data. On the other hand, HIPAA's approach is more broad and doesn't require the use of encrypted data. Meeting both compliance standards would be difficult because being compliant in one doesn't mean being compliant with the other.

Part 2: Conduct a Risk Assessment

1. Conduct a risk analysis of this environment using the version of PCI DSS that you downloaded in Part 1 of this lab. **Document** at least five control gaps that exist in the environment. You may make assumptions about information not provided in this scenario, if necessary.

Control Gap 1 - Managers and Cashiers shouldn't be able to access POS and backend servers from other stores. Assume that store managers receive compensation if their store is the most profitable when compared to competing restaurants. This provides managers an incentive for falsifying data for another store to push their own. This doesn't follow the least privileges concept. Control Gap 2 - The usernames for cashiers is too generic and doesn't provide accountability in the event that the POS was messed up. How do we define who cashier1 is on the machine the counts are off at the end of the evening. This breaks PCI DSS 8.1.1. Control Gap 3 - The limit for PCI DSS compliance is 6 failed password attempts according to 8.1.6. The store is noncompliant with this issue. Control Gap 4 - They are also not in compliance with 8.1.7 which states that user accounts should be locked out for a minimum of 30 minutes or until an administrator can unlock the account. Control Gap 5 - The organization is also out of compliance with 8.2.4 because their passwords are to be changed 180 days when it should be 90 days.

2. Identify controls that will mitigate each of the five deficiencies you identified in the previous step. **Create** a prioritized list of these actions.

Control Gap 1 - Managers and Cashiers shouldn't be able to access POS and backend servers from other stores. Assume that store managers receive compensation if their store is the most profitable when compared to competing restaurants. This provides managers an incentive for falsifying data for another store to push their own. This doesn't follow the least privileges concept. To mitigate this, the administrators should implement the least privileges principle and restrict access to other stores. This should be priority number one. Control Gap 2 - The usernames for cashiers is too generic and doesn't provide accountability in the event that the POS was messed up. How do we define who cashier1 is on the machine the counts are off at the end of the evening. This breaks PCI DSS 8.1.1. Each cashier should be created a unique username and strong passphrase. This is priority number 2. Control Gap 3 - The limit for PCI DSS compliance is 6 failed password attempts according to 8.1.6. The store is noncompliant with this issue. Their current passcode lockout is 10 which is 4 too many. Administrators should implement this control with priority number 3. Control Gap 4 - They are also not in compliance with 8.1.7 which states that user accounts should be locked out for a minimum of 30 minutes or until an administrator can unlock the account. Their current policy covers the minimum lockout phase, but because the lab doesn't explicitly say this, I am going to assume that the accounts will become automatically unlocked after an hour, An administrative control should be set in place to allow the accounts to be unlocked by an administrator. This should priority four. Control Gap 5 - The organization is also out of compliance with 8.2.4 because their passwords are to be changed 180 days when it should be 90 days. This is an easier fix. Passwords should be changed every 90 days to ensure compliance. This is priority number 5.

Challenge Exercise

1. What risk assessment standard would be the best approach for evaluating this system? Depending on the system, you may use one of the standards already discussed in this lab or identify an alternative standard more appropriate for your environment. **Provide** a brief description of the system, **identify** the standard that you used and **describe** why it is appropriate for the system.

In my younger years, I worked at one job that required the storage of credit card information. The best standard for this would the PCI DSS standard.

2. Conduct a risk assessment of the system against those standards to the best of your ability. If you are not familiar with the detailed workings of the systems, you may make assumptions to facilitate your risk assessment. **Create a list** of the gaps that exist between the system and the standard you used.

I don't remember much about the way things worked, but I do remember a glaringly obvious mistake. At our location, the application stayed open all day as we constantly received orders by phone. This broke 9.9. In addition, the application was viewable by someone standing outside the window. It was on ground floor which broke 9.4.

3. **Develop a prioritized list** of risk mitigation activities which, if followed, would address the issues raised in your gap analysis from step 2.

To fix 9.4, I would move the computer to a locked room with no windows and secure access. To fix 9.9, I would close the application when not in use. Both are critical risks and should be fixed immediately.